ПОСІБНИК

Посібник з європейського права у сфері захисту персональних даних

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Спільна програма Європейського Союзу та Ради Європи
«Зміцнення інформаційного суспільства в Україні»

Фінансується Європейським Союзом та Радою Європи

EUROPEAN UNION

COUNCIL OF EUROPE
CONCEIL DE L'EUROPE

Впроваджується Радою Європи

This publication was translated and produced under the Joint Programme between the European Union and the Council of Europe "Strengthening information society in Ukraine". The content of the publication can in no way be taken to reflect the views of the European Union and the Council of Europe.

Видання цієї публікації та переклад на українську мову здійснено у рамках спільної програми Європейського Союзу та Ради Європи «Зміцнення інформаційного суспільства в Україні». Зміст публікації не повинен тлумачитися як такий, що відображає офіційні погляди Європейського Союзу та Ради Європи.

Роботу над цим матеріалом завершено в 2014 році.

У майбутньому оновлену версію можна буде знайти на сайті Агентства ЄС із основоположних прав (FRA): fra.europa.eu, на сайті Ради Європи coe.int/dataprotection, та Європейського суду з прав людини у розділі «судова практика»: echr.coe.int.

Більш детальну інформацію про Європейський Союз можна знайти в мережі Інтернет за адресою: (http://europa.eu).

Каталожні дані знаходяться в кінці публікації.

ISBN 978-617-684-103-6 (Укр.)

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Посібник з європейського права у сфері захисту персональних даних

Передмова

Цей посібник з європейського права у сфері захисту персональних даних підготовлено Агентством Європейського Союзу із основоположних прав (FRA) та Радою Європи спільно з Секретаріатом Європейського суду з прав людини. Це – третій випуск із серії посібників з права, які підготовлено Агентством ЄС із захисту основоположних прав та Радою Європи. У березні 2011 року було опубліковано перший посібник – з проблематики європейського антидискримінаційного права, у червні 2013 року опублікований другий – з європейського права стосовно питань притулку, кордонів та імміграції.

Ми вирішили продовжити нашу співпрацю, звернувшись до такого надзвичайно актуального питання, що зачіпає кожного з нас в повсякденному житті, яким є захист персональних даних. У цій сфері Європа має одну з кращих за рівнем захисту систему, в основу якої покладено Конвенцію Ради Європи № 108, правові документи Європейського Союзу (ЄС), а також прецедентну практику Європейського суду з прав людини (ЄСПЛ) і Суду Європейського Союзу (СЄС).

Метою даного посібника є підвищення обізнаності та розширення знань про правила захисту персональних даних у державах – членах Європейського Союзу та Ради Європи, до яких читачі могли би звертатися як до основного орієнтира. Його підготовлено для правників широкого профілю, суддів, працівників національних органів з питань захисту персональних даних та інших осіб, які працюють у цій сфері.

Після набуття чинності Лісабонським договором у грудні 2009 року Хартія основних прав ЄС стала юридично обов'язковим документом, а разом з цим статусу окремого основоположного права набуло право на захист персональних даних. Для забезпечення цього основоположного права надзвичайно важливим є добра обізнаність з Конвенцією Ради Європи № 108 та правовими документами ЄС, які відкрили шлях до захисту персональних даних у Європі, а також з прецедентною практикою Суду ЄС та ЄСПЛ.

Хочемо подякувати Інституту прав людини ім. Людвіга Больцмана за його внесок у підготовку цього посібника. Також висловлюємо подяку Європейському наглядовому бюро з захисту персональних даних за допомогу на стадії підготовки посібника. Особливу вдячність висловлюємо відділу з питань захисту персональних даних Європейської комісії за надану допомогу під час підготовки цього посібника.

Філіпп Буайа,

Генеральний директор директорату з прав людини та верховенства права Ради Європи

Мортен К'ярум,

директор Агенції Європейського Союзу з питань основоположних прав

Зміст

Список скорочень

BCR	Обов'язкове корпоративне правило
CCTV	Замкнута система ТВ-спостереження
CETS	Серія договорів Ради Європи
Charter	Хартія основних прав Європейського Союзу
CIS	Митна інформаційна система
CJEU	Суд Європейського Союзу (СЄС) (до грудня 2009 року – Суд першої інстанції Європейських співтовариств)
CoE	Рада Європи
Convention 108	Конвенція про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних
CRM	Система управління зв'язками з клієнтами (CRM–система)
C-SIS	Центральна Шенгенська інформаційна система
EAW	Європейський ордер на арешт (ЄОА)
EC	Європейське співтовариство (ЄС)
ECHR	Конвенція про захист прав людини і основоположних свобод (ЄКПЛ)
ECtHR	Європейський суд з прав людини (ЄСПЛ)
EDPS	Європейський інспектор із захисту даних
EEA	Європейська економічна зона (ЄЕЗ)
EFTA	Європейська асоціація вільної торгівлі (ЄАВТ)
ENISA	Європейське агентство з мережевої та інформаційної безпеки (ЄАМІБ)
ENU	Національний відділ Європейського поліцейського управління
ESMA	Європейський орган з цінних паперів та фінансових ринків
eTEN	Транс-європейські телекомунікаційні мережі
EU	Європейський Союз (ЄС)

EuroPriSe	Європейський знак конфіденційності
eu-LISA	Агентство Європейського Союзу для великомасштабних IT систем
FRA	Агентство Європейського Союзу із основоположних прав
GPS	Система встановлення місцезнаходження GPS
JSB	Спільний наглядовий орган
NGO	Неурядова організація
N-SIS	Національна Шенгенська інформаційна система
OECD	Організація економічного співробітництва та розвитку (ОЕСР)
PIN	Персональний ідентифікаційний код
PNR	Реєстраційні дані авіапасажирів
SEPA	Єдина зона платежів у євро
SIS	Шенгенська інформаційна система
SWIFT	Спільнота всесвітніх міжбанківських фінансових телекомунікацій (SWIFT)
TEU	Договір про Європейський Союз (ДЄС)
TFEU	Договір про функціонування Європейського Союзу (ДфЄС)
UDHR	Загальна декларація прав людини
UN	Організація Об’єднаних Націй (ООН)
VIS	Візова інформаційна система (ВІС)

Як користуватися посібником

У цьому посібнику представлено огляд права Європейського Союзу (ЄС) та Ради Європи (РЄ) в питаннях захисту персональних даних.

Посібник підготовлено з метою надання допомоги юристам-практикам, які не спеціалізуються у сфері захисту персональних даних; він рекомендований для використання адвокатами, суддями або іншими фахівцями, а також працівниками інших органів, в тому числі й неурядових організацій (НУО), перед якими можуть постати правові питання, пов'язані з захистом персональних даних.

Це – перше звернення до права ЄС і Конвенції про захист прав людини і основоположних свобод (ЄСПЛ) у частині захисту персональних даних та роз'яснення процесу регулювання цієї сфери у праві ЄС, ЄКПЛ та Конвенції про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108), а також інших документах Ради Європи. Кожна глава розпочинається таблицею застосовних правових норм, а також прикладами вибраної судової практики двох окремих європейських правових систем. Далі за тематикою один за одним наводяться приклади застосовування правових актів двох європейських систем. Це дозволяє читачеві з'ясувати їх спільні та відмінні риси.

У таблицях на початку кожної глави окреслено теми, які у ній розглядатимуться, вказано застосовні правові норми та інші відповідні матеріали, зокрема, судові рішення. Порядок питань може дещо відхилятися від структури тексту глави там, де це необхідно для лаконічності викладення змісту. У таблицях наведено правові акти і РЄ, і ЄС. Це допоможе користувачам знайти ключову інформацію у контексті їхньої ситуації, особливо коли вони є суб'єктами виключно права РЄ.

Ті, хто опікуються цими питаннями в державах, які не входять до ЄС, але є членами РЄ, Сторонами ЄКПЛ та Конвенції 108, можуть отримати інформацію щодо їхньої країни безпосередньо із розділів, присвячених РЄ. Читачам із держав – членів ЄС потрібно буде звертатися до обох розділів, оскільки держави – члени ЄС мають юридичні зобов'язання в обох правових системах. Ті, кому потрібна детальніша інформація з певного питання, можуть звернутись до переліку посилань спеціальних матеріалів у розділі «Додаткові матеріали».

Право РЄ представлено скороченими посиланнями на вибрані рішення Європейського суду з прав людини (ЄСПЛ). Їх було обрано з великої кількості існуючих рішень ЄСПЛ, пов'язаних із захистом персональних даних.

Право ЄС представлено ухваленими правовими актами, відповідними договорами, Хартією основних прав Європейського Союзу у тлумаченні Суду Європейського Союзу (СЄС, який до 2009 року називався Судом першої інстанції Європейських співтовариств (ЕСJ)).

Приклади із судової практики, які наведено або на які даються посилання в цьому посібнику, належать до основних прецедентів, ухвалених ЄСПЛ та СЄС. Вказівники в кінці посібника допоможуть читачеві знайти потрібне рішення у мережі Інтернет.

На додаток до цього у текстових вікнах на блакитному фоні наведено приклади з вигаданим сюжетом, які пояснюють практичне застосування європейських норм захисту персональних даних, особливо з тематики, з якої немає рішень ЄСПЛ або СЄС. У текстових вікнах на сірому фоні наведено приклади із законодавства, а не з прецедентної судової практики.

На початку посібника поміщено короткий огляд ролі двох правових систем, створених правом ЄКПЛ та ЄС (глава 1). У главах 2–8 розглядаються такі питання:

- термінологія у сфері захисту персональних даних;
- основні принципи захисту персональних даних у європейському праві;
- норми європейського права про захист персональних даних;
- права суб'єктів персональних даних та їх реалізація;
- транскордонний обмін персональними даними;
- захист персональних даних у контексті діяльності поліції та кримінального судочинства;
- інші спеціальні європейські правові акти про захист персональних даних.

1 Контекст та історія європейського права про захист персональних даних

ЄС	питання, що висвітлюються	РЄ
Право на захист даних		
Директива 95/46/ЄК «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» (Директива про захист персональних даних), OJ 1995 L 281		ЄКПЛ, ст.8 (право на повагу до приватного та сімейного життя, житла і кореспонденції) Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108)
Баланс прав		
СЄС, Об'єднані справи, C-92/09 та C-93/09 «Товариство громадського права «Фолькер і Маркус Шеке» і Хартмут Айферт проти землі Гессен» (Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen), 2010р.	**загальні**	

ЄС	питання, що висвітлюються	РЄ
СЄС, C-73/07, «Уповноважений із захисту персональних даних Фінляндії проти компаній «Satakunnan Markkinapörssi Oy» і «Satamedia Oy» (Tietosuojavaltuutettu v. Satakunnan Markkinaporssi Oy and Satamedia Oy), 2008р.	**свобода вираження поглядів**	Рішення ЄСПЛ у справі «Аксель Шпрінгер проти Німеччини», 2012 р. Рішення ЄСПЛ у справі «Мослі проти Сполученого Королівства», 2011 р.
	свобода художньої творчості та науково-дослідницької діяльності	Рішення у справі ЄСПЛ «Ферайнігунг Більдендер Кюнстлер проти Австрії», 2007
СЄС, C-275/06 «Музичне виробництво в Іспанії (організація «Promusicae») проти АТ «Telefonica de Espana» (Productores de Musica de Espana (Promusicae) v. Telefonica de Espana SAU), 2008 р.	**захист власності**	
СЄС, C-28/08 P, «Європейська комісія проти компанії «Баваріан Лагер» (European Commission v. The Bavarian Lager Co. Ltd), 2010	**доступ до документів**	Рішення у справі ЄСПЛ «Таршашаг о Собадшагйогокерт проти Угорщини», 2009

1.1. Право на захист персональних даних

Ключові моменти

- Згідно зі статтею 8 ЄКПЛ право на захист проти збору та використання персональних даних складає частину права на повагу до приватного та сімейного життя, до житла та кореспонденції.
- Конвенція 108 РЄ – це перший міжнародний юридично зобов'язальний документ, який стосується виключно питань захисту персональних даних.
- Директива про захист персональних даних була першим документом, який регулює захист персональних даних у праві ЄС.
- У праві ЄС право на захист персональних даних визнано як основоположне право.

Вперше право особи на захист від втручання інших у приватне життя, зокрема, з боку держави, було закріплено у статті 12 (повага до приватного та сімейного життя) такого міжнародно-правового документу, як Загальна декларація прав людини Організації Об'єднаних Націй (ООН) 1948 року.[1] Загальна декларація прав людини мала вплив на розвиток інших правових документів (інструментів) захисту прав людини у Європі.

1.1.1. Конвенція про захист прав людини і основоположних свобод

Раду Європи було засновано після Другої світової війни з метою єднання європейських держав задля ствердження принципів верховенства права, демократії, прав людини і соціального розвитку. З цією метою у 1950 році РЄ прийняла Конвенцію про захист прав людини і основоположних свобод (ЄСПЛ), яка набула чинності у 1953 році.

Держави мають міжнародні зобов'язання щодо дотримання ЄКПЛ. Усі держави – члени РЄ уже включили норми ЄКПЛ до свого національного законодавства або ввели їх в дію, що вимагає від них дотримуватися її положень.

З метою забезпечення виконання Договірними Сторонами їхніх зобов'язань за ЄКПЛ у 1959 році у Страсбурзі (Франція) було засновано Європейський суд з

1 Організація Об'єднаних Націй (ООН), Загальна декларація прав людини (ЗДПЛ), 10 грудня 1948 р.

прав людини (ЄСПЛ). Європейський суд з прав людини забезпечує виконання державами їхніх зобов'язань за Конвенцією шляхом розгляду заяв від будь-яких осіб, груп осіб, недержавних організацій або юридичних осіб, які заявляють про порушення Конвенції. У 2013 році до складу Ради Європи входило 47 держав-членів, 28 з яких були одночасно і державами-членами ЄС. Для того, щоб подати заяву до ЄСПЛ, не потрібно бути громадянином однієї з держав-членів. ЄСПЛ може також розглядати міждержавні справи, порушені однією або декількома державами – членами РЄ проти іншої держави-члена.

Право на захист персональних даних є частиною прав, що захищаються статтею 8 ЄКПЛ, яка гарантує право на повагу до приватного і сімейного життя, житла та кореспонденції, а також визначає умови, за яких дозволяється обмежувати це право.[2]

За час свого існування ЄСПЛ розглядав велику кількість ситуацій, коли поставало питання про захист персональних даних, передовсім тоді, коли йшлось про перехоплення інформації[3], різні форми спостереження[4] та захист від зберігання персональних даних державними органами[5]. ЄСПЛ роз'яснював, що стаття 8 ЄКПЛ не тільки зобов'язує держави утримуватися від будь-яких дій, які могли б порушити гарантоване Конвенцією право, але й за певних обставин передбачає позитивні зобов'язання держав активно забезпечувати ефективне дотримання права на приватне і сімейне життя[6]. Значна кількість цих справ детально розглядатиметься у відповідних розділах.

1.1.2. Конвенція 108 Ради Європи

Із появою у 1960-их роках інформаційних технологій з'явилася потреба у розробленні більш детальних правил забезпечення захисту осіб через охорону їхніх (персональних) даних. До середини 1970-х років Комітет міністрів Ради Єв-

2 РЄ, Конвенція про захист прав людини і основоположних свобод, CETS No. 005, 1950 р.

3 Див., наприклад: рішення ЄСПЛ у справі *«Малоун проти Сполученого Королівства» (Malone v. the United Kingdom)*, № 8691/79 від 2 серпня 1984 р.; *«Копланд проти Сполученого Королівства» (Copland v. the United Kingdom)*, № 62617/00 від 3 квітня 2007 р.

4 Див., наприклад: рішення ЄСПЛ у справі *«Класс та інші проти Німеччини» (Klass and Others v. Germany)*, № 5029/71 від 6 вересня 1978 р.; *«Уцун проти Німеччини» (Uzun v.Germany)*, № 35623/05 від 2 вересня 2010 р.

5 Див., наприклад: рішення ЄСПЛ у справі *«Леандер проти Швеції» (Leander v. Sweden)*, № 9248/81 від 26 березня 1987 р.; *«С. і Марпер проти Сполученого Королівства» (S. and Marper v. The United Kingdom)*,, №№. 30562/04 та 30566/04 від 4 грудня 2008 р.

6 Див., наприклад: рішення ЄСПЛ у справі *«І. проти Фінляндії» (I. v. Finland)*, № 20511/03 від 17 липня 2008 р.; *«K.U. проти Фінляндії» (K.U. v. Finland)*, № 2872/02 від 2 грудня 2008 р.

ропи прийняв ряд резолюцій про захист персональних даних з посиланням на статтю 8 ЄКПЛ.[7] У 1981 році була відкрита для підписання Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108)[8]. Конвенція 108 була і залишається єдиним юридично зобов'язуючим міжнародним документом у сфері захисту персональних даних.

Конвенція 108 застосовується до будь-якого процесу обробки даних, що здійснюється як у приватному, так і у державному секторах, зокрема, до обробки персональних даних судовими і правоохоронними органами. Вона захищає особу від зловживань, які можуть виникати при збиранні та обробці персональних даних, її другим завданням є регулювання транскордонної передачі персональних даних. Що стосується збирання та обробки персональних даних, визначені в Конвенції принципи стосуються, зокрема, відкритого і законного збирання та автоматизованої обробки персональних даних, які зберігаються для визначених і законних цілей та не використовуються у спосіб, не сумісний із цими цілями, а також не зберігаються довше, ніж це необхідно. Вони також стосуються якості даних, зокрема, передбачають, що такі дані повинні бути адекватними, відповідними та не надмірними (пропорційними), а також точними.

На додаток до гарантій, що стосуються збору та обробки персональних даних, конвенція забороняє за відсутності відповідних правових гарантій здійснювати обробку чутливих даних, які стосуються расової належності, політичних переконань, здоров'я, релігії, статевого життя або засудження в кримінальному порядку.

Також у Конвенції закріплено за особою право знати про факт збереження про нього/неї інформації і про можливість, за необхідності, її корегування. Дія закладених у Конвенції обмежень щодо здійснення прав можлива лише за умови існування загрози для інтересів, які переважають (наприклад, інтереси безпеки та захисту держави).

Незважаючи на те, що Конвенція передбачає вільний обмін персональними даними між державами, які є сторонами Конвенції, вона водночас накладає

7 РЄ, Комітет міністрів (1973 р.), Резолюція (73) 22 «Про захист недоторканості приватного життя осіб стосовно електронних банків персональних даних у приватному секторі» від 26 вересня 1973 р.; РЄ, Комітет міністрів (1974 р.), Резолюція (74) 29 «Про захист недоторканості приватного життя осіб стосовно електронних банків персональних даних у публічному секторі» від 20 вересня 1974 р.

8 РЄ, Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних, Рада Європи, CETS № 108, 1981 р.

деякі обмеження на ті потоки, які направлено у країни, де правове регулювання не передбачає відповідний рівень захисту даних.

З метою подальшого розвитку викладених у Конвенції 108 загальних принципів і правил Комітет міністрів РЄ ухвалив декілька рекомендацій, які не мають сили юридичного зобов'язання (див. глави 7 і 8).

Усі держави – члени ЄС ратифікували Конвенцію 108. У 1999 році до Конвенції 108 було внесено зміни, які дозволили ЄС стати стороною Конвенції.[9] У 2001 році було прийнято Додатковий протокол до Конвенції 108, який містить положення про транскордонні потоки даних до так званих третіх країн, які не є сторонами, та про обов'язкове створення національних наглядових органів з питань захисту персональних даних.[10]

Огляд

У 2011 році після прийняття рішення про необхідність оновлення Конвенції 108 було проведено громадські обговорення, за результатами яких було підтверджено дві основні цілі модернізації: посилення захисту приватного життя у сфері використання цифрових технологій та зміцнення механізму виконання Конвенції.

Конвенція 108 відкрита для приєднання для держав, які не є членами РЄ, в тому числі для неєвропейських країн. Здатність Конвенції формувати універсальні норми та її відкритий характер можуть бути основою для розвитку захисту персональних даних на світовому рівні.

Станом на сьогодні 45 із 46 Договірних Сторін Конвенції 108 є державами – членами Ради Європи. Уругвай, перша неєвропейська країна, приєдналася у серпні 2013 року, а Марокко, якому Комітет Міністрів запропонував приєднатися до Конвенції 108, знаходиться у процесі оформлення приєднання.

9 РЄ, зміни до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних (порядковий номер у серії Європейських договорів – 108), які дозволили Європейським співтовариствам приєднатися до неї, ухвалені Комітетом Міністрів у Страсбурзі 15 червня 1999 р.; ст. 23 (2) Конвенції зі змінами.

10 РЄ, Додатковий протокол до Конвенції про захист осіб у зв'язку з обробкою персональних даних та вільне переміщення таких даних, CETS № 181, 2001 р.

1.1.3. Законодавство Європейського Союзу про захист персональних даних

В основі законодавства ЄС лежать договори ЄС та акти вторинного законодавства ЄС. Договори, а саме Договір про Європейський Союз (ДЄС) та Договір про функціонування Європейського Союзу (ДфЄС), ухвалено всіма державами – членами ЄС, їх також називають «первинним законодавством ЄС». Регламенти, директиви та рішення ЄС ухвалюються уповноваженими дією договорів інститутами ЄС; їх часто називають «вторинним або похідним законодавством ЄС».

Основним правовим інструментом ЄС у сфері захисту персональних даних є Директива 95/46/ЄС Європейського парламенту та Ради Європи від 24 жовтня 1995 року «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» (Директива про захист персональних даних).[11] Її було прийнято в 1995 році вже після того, як декілька держав-членів прийняли національні закони про захист персональних даних. Вільне переміщення товарів, капіталів, послуг і осіб на внутрішньому ринку вимагало вільного потоку даних, який не можна було б здійснити, якби держави-члени не могли розраховувати на однаково високий рівень захисту персональних даних.

Оскільки прийняття Директиви про захист персональних даних передбачало гармонізацію[12] національного законодавства у сфері захисту персональних даних, у ній пропонувався більш точний рівень визначень у порівнянні з існуючими на той час національними законами про захист персональних даних. За визначенням СЄС «Призначенням Директиви 95/46 [...] є забезпечення однакового рівня захисту прав і свобод особи при обробці персональних даних в усіх державах-членах. [...] Процес адаптації національного законодавства, яке діє у цій сфері, не повинен призводити до зменшення передбачуваного ним захисту, а навпаки, повинен намагатися гарантувати високий рівень захисту в ЄС. Тому [...] гармонізація національного законодавства не повинна обмежуватися мінімальними заходами, а повинна бути повною.»[13] Відповідно,

11 Директива про захист персональних даних, OJ 1995 L 281, стор. 31.

12 Див., наприклад, Директиву про персональних захист даних, частини 1, 4, 7 та 8 преамбули.

13 СЄС, об'єднані справи C-468/10 та C-469/10, *«Національна асоціація кредитних фінансових установ (ASNEF) і Федерація* електронної комерції і прямого маркетингу (FECEMD) проти Державної адміністрації» *(Asociacion Nacional de Establecimientos Financieros de Credito (ASNEF) and Federacion de Comercio Electronico y Marketing Directo (FECEMD) v. Administracion del Estado)* від 24 листопада 2011 р., пункти 28–29.

держави – члени ЄС мають тільки обмежену свободу для маневрування у процесі реалізації директиви.

Директиву про захист персональних даних підготовлено з метою наповнення реальним змістом та розширення викладених у Конвенції 108 принципів права на приватність. Той факт, що всі 15 держав, які були членами ЄС у 1995 році, також були Договірними Сторонами Конвенції 108, виключає можливість прийняття суперечливих норм у цих двох правових інструментах. Окрім того, у Директиві про захист персональних даних зафіксовано передбачену у статті 11 Конвенції 108 можливість додавати інструменти захисту. Зокрема, введення незалежного контролю як інструменту, що вдосконалював дотримання правил захисту персональних даних, стало важливим внеском в ефективне функціонування європейського законодавства про захист персональних даних. (Згодом у 2001 році цю норму було внесено до права Ради Європи Додатковим протоколом до Конвенції 108).

Територія, на якій застосовується Директива про захист персональних даних, виходить за межі 28 держав – членів ЄС, охоплюючи ті держави, які не є членами ЄС, але входять до єдиної економічної зони ЄС (ЕЕА)[14], наприклад, Ісландія, Ліхтенштейн та Норвегія.

СЄС в Люксембурзі має юрисдикцію встановлювати факт виконання державою-членом своїх зобов'язань за Директивою про захист персональних даних і надавати попередні рішення щодо законності та тлумачення Директиви в цілях забезпечення її ефективного та однакового застосування у державах-членах. Важливим винятком із застосування Директиви є так звані побутові винятки, а саме обробка персональних даних фізичними особами для особистих чи побутових потреб.[15] Така обробка, зазвичай, розглядається як елемент свобод фізичної особи.

У відповідності до первинного права ЄС, чинного на момент прийняття Директиви про захист персональних захист даних, матеріальну сферу її застосування обмежено питаннями внутрішнього ринку. Крім того, і це є найбільш важливим, питання співробітництва з поліцією та органами кримінального судочинства не належать до сфери її застосування. Захист персональних даних у подібних справах визначається різними правовими документами, які детальніше розглядаються в главі 7.

14 Угода про Європейську економічну зону, OJ 1994 L 1, яка набрала чинності 1 січня 1994 р.

15 Директива про захист персональних даних, ст. 3 (2) друга частина.

Через той факт, що Директива про захист персональних даних стосувалася лише держав – членів ЄС, виникла необхідність у створенні додаткового правового інструменту з метою захисту персональних даних під час їх обробки інститутами та органами ЄС. Таким інструментом став Регламент (ЄС) № 45/2001 про захист фізичних осіб при обробці персональних даних інститутами і органами Співтовариства і про вільне переміщення таких даних (*Регламент інститутів ЄС щодо захисту персональних даних)*.[16]

Окрім цього, навіть для того, щоб регулювати сфери, які охоплюються дією Директиви про захист персональних даних, часто необхідні більш детальні положення для досягнення необхідної ясності стосовно балансу інших законних інтересів. Як приклад можна навести дві директиви: Директиву 2002/58/ЄС «Про обробку персональних даних та захист таємниці у секторі електронних комунікацій (*Директива про секретність та електронні комунікації*)[17] і Директиву 2006/24/ЄС «Про збереження даних, створених або оброблених при наданні загальнодоступних послуг електронних повідомлень або громадських мереж зв'язку та про внесення змін до Директиви 2002/58/ЄС (*Директива про збереження даних),* яка втратила чинність 8 квітня 2014 р.)[18] Інші приклади розглядатимуться у главі 8. Положення цих документів повинні відповідати Директиві про захист персональних даних.

Хартія основних прав Європейського Союзу

У перших договорах Європейських співтовариств немає посилань на права людини або їх захист. З огляду на те, що до тодішнього Суду першої інстанції Європейських співтовариств надходили заяви про порушення прав людини у сферах дії права ЄС, він розробив новий підхід. Для забезпечення захисту фізичних осіб він включив основоположні права до так званих загальних принципів європейського права. Згідно СЄС ці загальні принципи відображають зміст захисту прав людини, який закріплений в національних конституці-

16 Регламент (ЄС) № 45/2001 Європейського парламенту та Ради від 18 грудня 2000 р. «Про захист фізичних осіб при обробці персональних даних інститутами і органами Співтовариства і про вільне переміщення таких даних», OJ 2001 L 8.

17 Директива 2002/58/ЄС Європейського парламенту та Ради від 12 липня 2002 р. «Про обробку персональних даних та захист таємниці у секторі електронних комунікацій (*Директива про секретність та електронні комунікації), OJ 2002 L 201.*

18 Директива 2006/24/ЄС Європейського парламенту та Ради від 15 березня 2006 р. «Про збереження даних, створених або оброблених при наданні загальнодоступних послуг електронних повідомлень або громадських мереж зв'язку та про внесення змін до Директиви 2002/58/ЄС» *(Директива про збереження даних),* OJ 2006 L 105, яка втратила чинність 8 квітня 2014 р.

ях і договорах з прав людини, зокрема в ЄКПЛ. СЄС заявив, що забезпечуватиме відповідність права ЄС цим принципам.

Визнаючи, що його політика може мати вплив на права людини, та намагаючись «наблизити» громадян до ЄС, у 2000 році ЄС ухвалив Хартію основних прав Європейського Союзу (Хартія). Ця Хартія включає весь спектр громадянських, політичних, економічних і соціальних прав європейських громадян у поєднанні з конституційними традиціями та міжнародними зобов'язаннями, які є спільними для держав-членів. Описані в Хартії права класифіковано у шістьох розділах: гідність, свобода, рівність, солідарність, права громадян та правосуддя.

Спочатку Хартія була лише політичним документом, але після набрання чинності Лісабонською угодою 1 грудня 2009 року[19] вона стала юридично зобов'язальною[20] на зразок усього первинного права ЄС (див. статтю 6 (1) Договору про Європейський Союз).

У первинному праві ЄС також є положення про загальні законодавчі повноваження ЄС у сфері захисту персональних даних (стаття 16 Договору про ЄС).

Хартія не тільки гарантує повагу до приватного і сімейного життя (стаття 7), але й передбачає право на захист персональних даних (стаття 8), відкрито піднімаючи рівень його захисту до рівня захисту основного права ЄС. Інститути ЄС та держави-члени повинні дотримуватися і гарантувати це право, що також повинні робити держави-члени, реалізуючи право Союзу (стаття 51 Хартії). Статтю 8 Хартії, яку було сформульовано через кілька років після прийняття Директиви про захист персональних даних, слід вважати такою, у якій втілено право ЄС про захист персональних даних, що існувало до того часу. Таким чином, у статті 8 (1) Хартії не тільки відкрито визнається право на захист персональних даних, але й основні принципи захисту персональних даних (стаття 8 (2)). І нарешті, положення статті 8 (3) Хартії гарантують здійснення незалежним органом контролю за реалізацією цих принципів.

19 ЄС (2012), Хартія основних прав Європейського Союзу, OJ 2012 C 326.

20 Див. консолідовані версії Договору про Європейські співтовариства (2012), Договору про Європейський Союз, OJ 2012 C 326; та Договору про Європейські співтовариства (2012), ДфЄС, OJ 2012 C 326.

Огляд

У січні 2012 року Європейська комісія, заявивши про необхідність модернізації існуючих норм захисту персональних даних у світлі стрімких технологічних змін та глобалізації, запропонувала пакет реформ у сфері захисту персональних даних. До пакету реформ включено пропозиції щодо заміни Директиви про захист персональних даних Генеральним регламентом про захист персональних даних[21], а також підготовки нової Генеральної директиви про захист персональних даних[22], у якій би передбачалось забезпечення захисту даних у таких сферах, як поліцейське та судове співробітництво, спрямоване на подолання злочинності. На час публікації цього посібника обговорення пакету реформ все ще тривали.

1.2. Баланс прав

Ключові моменти

- Право на захист персональних даних не є абсолютним, воно має бути приведене у відповідність з іншими правами.

Основне право на захист персональних даних за статтею 8 Хартії «не є абсолютним правом і повинно розглядатися у зв'язку з його функцією у суспільстві».[23] Тому у статті 52 (1) Хартії визнається, що на здійснення таких прав можуть бути накладені обмеження, наприклад, такі, які викладені в статтях 7 і 8 Хартії, на період, передбачений законом, які мають поважати суть цих прав і свобод, спиратися на принцип пропорційності і застосовуватися лише в тому випадку, якщо є необхідними і по-справжньому відповідають загаль-

21 Європейська комісія (2012), пропозиції щодо Регламенту Європейського парламенту та Ради *«Про захист осіб при обробці персональних даних та про вільне переміщення таких даних» (Генеральний Регламент про захист персональних даних), COM(2012) 11 остат., Брюссель, 25 січня 2012 р.*

22 Європейська комісія (2012), пропозиції до Директиви Європейського парламенту та Ради *«Про захист фізичних осіб при обробці персональних даних уповноваженими органами з метою попередження, розслідування, виявлення та переслідування за скоєння кримінального злочину або виконання кримінального покарання та про вільне переміщення таких даних» (Генеральна Директива про захист даних), COM(2012) 10 остат., Брюссель, 25 січня 2012 р .*

23 Див., наприклад, СЄС, об'єднані справи C-92/09 та C-93/09, *«Національна асоціація кредитних фінансових установ (ASNEF) і Федерація електронної комерції і прямого маркетингу (FECEMD) проти Державної адміністрації» (Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen)* від 9 листопада 2010 р., п. 48.

ним цілям, визнаним Європейським Союзом, або необхідні для захисту прав і свобод інших людей.[24]

У системі ЄКПЛ право на захист персональних даних гарантується статтею 8 (право на повагу до приватного і сімейного життя), а в системі Хартії це право має застосовуватися за умови, якщо дотримуються всі інші конкурентні права. Відповідно до статті 8 (2) ЄКПЛ «органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві [...] для захисту прав і свобод інших осіб».

У зв'язку з цим і ЄСПЛ, і СЄС неодноразово заявляли, що при застосовуванні й тлумаченні статті 8 ЄКПЛ та статті 8 Хартії її необхідно узгоджувати з іншими правами.[25] Декілька важливих прикладів продемонструють, як досягати цього балансу.

1.2.1. Свобода вираження поглядів

Одним із прав, яке може вступати у конфронтацію з правом на захист персональних даних, є право на свободу вираження поглядів.

Право на свободу вираження поглядів закріплено у статті 11 Хартії («Свобода вираження поглядів та свобода інформації»). Це право включає «свободу дотримуватись своїх поглядів, отримувати і розповсюджувати інформацію та ідеї без втручання органів державної влади та незалежно від державних кордонів». Стаття 11 відповідає статті 10 ЄКПЛ. За статтею 52 (3) Хартії у тій мірі, у якій Хартія містить права, що відповідають правам, гарантованим ЄКПЛ, «їх зміст та сфера застосування збігаються зі змістом та сферою застосування, що встановлені вказаною Конвенцією». Отже обмеження, які можуть встановлюватися законом на здійснення гарантованого у статті 11 Хартії права, не можуть перевищувати ті обмеження, які передбачено у статті 10 (2) ЄКПЛ, тобто вони повинні бути передбачені законом і бути необхідними в демократич-

24 Там само, пункт 50.

25 Рішення у справі ЄСПЛ *«Фон Ганновер проти Німеччини» (Von Hannover v. Germany)(№ 2)* [ВП], №№ 40660/08 та 60641/08 від 7 лютого 2012 р.; Об'єднані справи СЄС, C-468/10 та C-469/10, *«Національна асоціація кредитних фінансових установ (ASNEF) і Федерація електронної комерції і прямого маркетингу (FECEMD) проти Державної адміністрації»* від 24 листопада 2011р., п. 48; СЄС, C-275/06, *«Музичне виробництво в Іспанії (організація «Promusicae») проти АТ «Telefonica de Espana»* від 29 січня 2008р., п. 68. Див. також РЄ (2013 р.), Судова практика Європейського суду з прав людини щодо захисту персональних даних, DP (2013р.) Судову практику можна знайти на сайті: www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/DP 2013 Case Law_Eng_FINAL.pdf.

ному суспільстві «для захисту [...] репутації чи прав інших осіб». Це поняття включає право на захист персональних даних.

Взаємозв'язок між захистом персональних даних та свободою поглядів регулюється у статті 9 Директиви про захист персональних даних, яка називається «Обробка персональних даних і свобода самовираження».[26] Згідно із положеннями цієї статті від держав-членів вимагається надання ряду відступів чи обмежень щодо захисту персональних даних а отже, стосовно основоположного права на недоторканність приватного життя, про що йдеться у главах II, IV і VI директиви. Ці відступи мають здійснюватися виключно для цілей журналістики або художньої чи літературної творчості, що підпадає під дію основоположного права на свободу вираження поглядів, за умови, що вони необхідні для узгодження права на приватне життя з нормами, які регулюють свободу вираження поглядів.

Приклад: У справі *«Уповноважений із захисту персональних даних Фінляндії проти компаній «Satakunnan Markkinapörssi Oy» і «Satamedia Oy»*[27] СЄС повинен був надати тлумачення статті 9 Директиви про захист персональних даних та визначити взаємозв'язок між захистом даних та свободою преси. Суд мав розглянути питання про поширення Markkinaporssi та Satamedia законно отриманої від фінських податкових органів інформації про податки 1.2 млн фізичних осіб. Зокрема, Суд мав встановити, чи повинна обробка персональних даних, які були оприлюднені податковими органами з метою надання користувачам мобільних телефонів доступу до отримання ними даних про податки інших фізичних осіб, розглядатися як діяльність, що здійснюється виключно для цілей журналістики. Встановивши, що діяльність Satakunnan це – «обробка персональних даних у значенні статті 3 (1) Директиви про захист персональних даних, Суд продовжив роз'ясненням статті 9 Директиви. Насамперед Суд наголосив на важливості права на свободу вираження поглядів у будь-якому демократичному суспільстві і постановив, що поняття, які стосуються цієї свободи, наприклад, журналістику, слід тлумачити широко. Потім він зазначив, що задля досягнення балансу між двома основоположними правами відступи та обмеження у здійсненні права на захист персональних даних повинні застосовуватися тільки з переконливою не-

26 Директива про захист персональних даних, ст. 9.

27 СЄС, C-73/07, *«Уповноважений із захисту (персональних) даних Фінляндії проти компаній «Satakunnan Markkinapörssi Oy» і «Satamedia Oy» (Tietosuojavaltuutettu v. Satakunnan Markkinaporssi Oy and Satamedia Oy)* від 16 грудня 2008, пункти 56, 61 та 62.

обхідністю. За таких обставин Суд визнав, що діяльність, яку здійснювали Markkinaporssi і Satamedia з даними документами, які відповідно до національного законодавства перебувають у державному володінні, може бути визнано «журналістською діяльністю», якщо її метою є розкриття громадськості інформації, поглядів та ідей, незалежно від способу, який використовується для їх передачі. Суд також постановив, що ця діяльність не обмежується зобов'язаннями ЗМІ і може здійснюватися з метою отримання прибутку. Проте право визначити, чи справді це так у даному випадку, СЄС залишив за національним судом.

Що стосується узгодження права на захист персональних даних з правом на свободу вираження поглядів, ЄСПЛ прийняв декілька знакових рішень.

У справі *«Аксель Шпрінгер AG. проти Німеччини»*[28] ЄСПЛ постановив, що накладення національним судом заборони на власника газети, який хотів опублікувати статтю про арешт і засудження відомого актора, порушувало статтю 10 ЄКПЛ. ЄСПЛ повторив визначені у своїх рішеннях критерії балансу права на свободу вираження поглядів та права на повагу до приватного життя:

- по-перше, якщо подія, яку опубліковано у статті, викликає суспільний інтерес: арешт і засудження особи – це публічний судовий факт і тому викликає суспільний інтерес;
- по-друге, якщо ця особа є публічною особою: особа, про яку йшлось, була актором настільки відомим, що могла вважатися публічною особою;
- по-третє, спосіб отримання інформації та визначення того, чи є він надійним: інформацію було надано Генеральною прокуратурою, достовірність інформації в обох публікаціях не викликала сумнівів у сторін. Тому ЄСПЛ визнав, що накладені на компанію обмеження не були переконливо пропорційними законній меті захисту приватного життя заявника. Суд дійшов висновку, що мало місце порушення статті 10 ЄКПЛ.

28 ЄСПЛ, рішення у справі «*Аксель Шпрінгер проти Німеччини*» (*Axel Springer AG v. Germany*) [ВП], № 39954/08 від 7 лютого 2012 р., пункти 90 та 91.

Приклад: у справі «*Фон Ганновер проти Німеччини» (№ 2)*[29] ЄСПЛ не визнав факту порушення права на повагу до приватного життя за ст.8 ЄКПЛ, коли принцесі Монако Кароліні було відмовлено у накладенні судової заборони на публікацію фотографії з її зображенням та зображенням її чоловіка, яку було зроблено під час відпочинку на лижах. Фотографія супроводжувалась статтею, у якій, між іншим, також повідомлялося про поганий стан здоров'я князя Реньє. ЄСПЛ дійшов висновку, що національними судами було точно дотримано балансу права видавничих компаній на свободу вираження поглядів та права заявників на повагу до їхнього приватного життя. Характеристика національними судами хвороби князя Реньє як події у сучасному суспільстві не може вважатися необґрунтованою і ЄСПЛ визнав можливим прийняти той факт, що фотографія, яка розглядалася у контексті статті, принаймні, деякою мірою сприяла дискусіям у суспільстві. Суд дійшов висновку про відсутність порушення статті 8 ЄКПЛ.

У прецедентних рішеннях ЄСПЛ одним із найважливіших критеріїв дотримання балансу цих прав є критерій сприяння обговорюваного питання дискусіям у суспільстві.

Приклад: у справі «*Мослі проти Сполученого Королівства*»[30] національна щотижнева газета надрукувала інтимні фотографії заявника. П. Мослі заявив про порушення статті 8 ЄКПЛ у зв'язку з тим, що через відсутність вимоги, яка б зобов'язувала газету заздалегідь сповіщати про заплановані публікації матеріалу, що здатен порушити право особи на приватне життя, він не зміг отримати судову заборону на публікацію цих фотографій. Незважаючи на те, що такий матеріал поширювався загалом в розважальних, а не освітніх цілях, це питання, звичайно ж, підпадає під захист статті 10 ЄКПЛ, яка може поступатися вимогам статті 8 ЄКПЛ у випадку, якщо ця інформація носить приватний та інтимний характер, а також не викликає суспільного інтересу при її поширенні. Проте особливу обережність слід виявляти під час розгляду обмежень, які можуть мати ефект цензури щодо публікації. Що стосується стримуючого ефекту, до якого мав би призвести факт попереднього повідомлення про плани, ма-

29 ЄСПЛ, рішення у справі «*Фон Ганновер проти Німеччини*» (*Von Hannover v. Germany)* (№ 2) [ВП], №№ 40660/08 та 60641/08 від 7 лютого 2012р., пункти 118 та 124.

30 ЄСПЛ, рішення у справі «*Мослі проти Сполученого Королівства*» *(Mosley v. the United Kingdom),* № 48009/08 від 10 травня 2011 р., пункти. 129 та 130

ючи сумніви щодо його ефективності та з широкою свободою розсуду у цій сфері, ЄСПЛ дійшов висновку, що існування юридично зобов'язуючої вимоги щодо попереднього повідомлення не передбачено в статті 8. Відповідно, Суд дійшов висновку, що не було порушено статтю 8.

Приклад: у справі *«Бірюк проти Литви»*[31] заявниця вимагала від щоденної газети відшкодування збитків за публікацію у статті інформації про те, що вона було ВІЛ-позитивною. Цю інформацію нібито підтверджували лікарі місцевої лікарні. ЄСПЛ не вважає цю статтю такою, яка сприяє будь-яким публічним дискусіям, і підтвердив, що захист персональних даних, медичних зокрема, має принципове значення для задоволення прав особи на повагу до його або її приватного і сімейного життя, які гарантовані у статті 8 ЄКПЛ. Суд надає особливого значення тому факту, що згідно з повідомленням у газеті медичний персонал лікарні надав інформацію про ВІЛ-інфіковану заявницю, відкрито порушуючи обов'язок зберігати лікарську таємницю. Отже, держава не забезпечила право заявниці на повагу до її приватного життя. Суд дійшов висновку, що було порушено статтю 8.

1.2.2. Доступ до документів

Свобода інформації відповідно до статті 11 Хартії та статті 10 ЄКПЛ гарантує право не тільки розповсюджувати, але й *отримувати* інформацію. Усвідомлення важливості прозорості у діяльності уряду для функціонування демократичного суспільства постійно зростає. Як результат, за останні два десятиліття право на доступ до документів, які знаходяться у розпорядженні державних органів, було визнано важливим правом кожного громадянина ЄС і будь-якої фізичної або юридичної особи, яка проживає або офіційно зареєстрована в державі-члені.

У праві РЄ можна послатися на принципи, закріплені в Рекомендації про доступ до офіційних документів, які сприяли процесу розробки Конвенції про доступ до офіційних документів *(Конвенція 205)*.[32] У **праві ЄС** право на доступ

31 ЄСПЛ, рішення у справі *«Бірюк проти Литви» (Biriuk v. Lithuania),* № 23373/03 від 25 листопада 2008 р.

32 Рада Європи, Комітет міністрів (2002), Рекомендація (2002)2 державам-членам щодо доступу до офіційних документів від 21 лютого 2002 р.; Рада Європи, Конвенція про доступ до офіційних документів, CETS № 205 від 18 червня 2009 р. Конвенція ще не набрала чинності.

до документів гарантується Регламентом 1049/2001 щодо доступу громадськості до документів Європейського парламенту, Ради та документів Комісії *(Регламент щодо доступу до документів)*.[33] Положеннями статті 42 Хартії та статті 15(3) ДфЄС дію цього права було поширено на доступ «до документів інститутів, органів, служб та агентств Союзу, незалежно від їхньої форми». Відповідно до статті (52) 2 Хартії право доступу до документів також здійснюється на умовах і в межах положень статті 15 (3) ДфЄС. Це право може вступати у конфронтацію з правом на захист персональних даних, якщо у результаті доступу до документа буде розкрито персональні дані інших осіб. Тому запити на отримання доступу до документів або інформації, які перебувають у розпорядженні державних органів, мають бути збалансовані з правом на захист осіб, персональні дані яких містяться в запитуваних документах.

Приклад: у справі *«Європейська комісія проти компанії «Баваріан Лагер»*[34] Суд ЄС визначив межі захисту персональних даних у контексті доступу до документів інститутів ЄС та взаємозв'язку між Регламентом № 1049/2001 (*Регламент щодо доступу до документів*) та Регламентом № 45/2001 (*Регламент щодо захисту даних*). Створена в 1992 році компанія «Баваріан Лагер» імпортує до Сполученого Королівства німецьке пиво в пляшках, здебільшого для пабів та барів. У компанії виникли труднощі, пов'язані з тим, що британське законодавство де-факто підтримує національного виробника. У відповідь на скаргу компанії «Баваріан Лагер» Європейська комісія прийняла рішення про порушення справи проти Сполученого Королівства за невиконання зобов'язань, у результаті чого було внесено зміни до спірних положень та узгоджено їх із правом ЄС. «Баваріан Лагер» звернулась до Комісії з проханням надати документи, серед яких вимагалась копія протоколу засідання за участі представників Комісії, органів державної влади Сполученого Королівства і Конфедерації загального ринку пивоварів. Комісія надала дозвіл на розкриття деяких документів, які стосуються засідання, але затерла у протоколі імена п'яти учасників: дві особи чітко заявили, що заперечують проти розкриття їхніх імен, а з іншими трьома у Комісії не було можливості встановити зв'язок. Рішенням від 18 березня 2004 р. Комісія відхилила нову заяву «Баваріан Лагер» щодо отримання повного протоколу засідання, посилаючись,

33 Регламент (ЄС) № 1049/2001 Європейського парламенту та Ради від 30 травня 2001 р. щодо загального доступу до документів Європейського парламенту, Ради та Комісії, OJ 2001 L 145.

34 CEC, C-28/08 P, «*Європейська комісія проти компанії «Баваріан Лагер лтд*» (*European Commission v. The Bavarian Lager Co. Ltd.)* від 29 червня 2010 р., пункти 60, 63, 76,78 та 79.

зокрема, на право захисту приватного життя цих осіб, яке гарантовано Регламентом щодо захисту даних. Оскільки така позиція Комісії не задовольняла компанію «Баваріан Лагер», вона подала позов до суду першої інстанції, який своїм рішенням від 8 листопада 2007 року (справа T-194/04, «Баваріан Лагер» проти Комісії) скасував рішення Комісії, вважаючи, зокрема, що навряд чи поява імен цих осіб у списку учасників засідання від імені органа, який вони представляють, становитиме втручання в їхнє приватне життя або загрожуватиме йому.

У відповідь на апеляцію Комісії Суд ЄС відмінив рішення суду першої інстанції. СЄС постановив, що Регламентом щодо доступу до документів встановлено «конкретну і посилену систему захисту осіб, персональні дані яких у деяких випадках можуть бути оприлюднені». Згідно СЄС, якщо запит підготовлено відповідно до Регламенту про доступ до документів і його метою є отримання доступу до документів, включаючи й персональні дані, положення Регламенту застосовуються в повному обсязі. Далі СЄС дійшов висновку, що Комісія справедливо відхилила заяву про надання доступу до повного протоколу засідання від жовтня 1996 р. З огляду на відсутність згоди п'ятьох учасників засідання Комісія належним чином виконала свій обов'язок щодо дотримання відкритості, коли надала запитуваний документ із затертими іменами.

Окрім того, відповідно до Суду ЄС «з огляду на те, що компанія «Баваріан Лагер» не надала прямих і правомірних підстав або будь-яких переконливих аргументів, які могли би довести факт необхідності передачі цих персональних даних, Комісія не змогла узгодити розбіжні інтереси сторін у цій справі. Також не було можливості перевірити наявність підстав вважати, що «законним інтересам суб'єктів персональних даних може бути завдано шкоди», що вимагається Регламентом щодо захисту персональних даних.

Згідно з цим судовим рішенням для втручання у право на захист персональних даних у зв'язку з доступом до документів потрібна конкретна і обґрунтована причина. Право доступу до документів не може автоматично відмінити право на захист персональних даних.[35]

35 Проте див. детальні консультації Європейського інспектора з охорони персональних даних (2011), *Доступ громадськості до документів, які містять персональні дані після рішення у справі «Баваріан Лагер»*, Брюссель, 24 March 2011, за адресою: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11–03–24_Bavarian_Lager_EN.pdf.

Особливий аспект доступу до документів було розглянуто в наступному рішенні ЄСПЛ.

Приклад: у справі «*Таршашаг о Собадшагйогокерт проти Угорщини*»[36] заявник, правозахисна недержавна організація, вимагала від Конституційного Суду доступу до інформації про справу, яка знаходилась на стадії розгляду. Без проведення консультації з членом парламенту, який подав заяву, Конституційний Суд відмовив у доступі на підставі того, що інформація про справи, які до нього надходять, може бути розкрита стороннім особам лише за умови згоди позивача. Національні суди підтримали цю відмову, обґрунтовуючи це тим, що право на захист персональних даних не може підмінятися іншими законними інтересами, в тому числі й правом на доступ громадськості до інформації. Заявник виступав як «сторожовий пес суспільства», діяльність якого вимагала такого самого захисту, як і діяльність преси. Відносно свободи преси ЄСПЛ постійно заявляє про те, що громадськість має право отримувати інформацію загального характеру. Запитувана заявником інформація була «готова і доступна» і не вимагала збирання даних. За таких обставин обов'язком держави є не перешкоджати поширенню інформації, про яку запитував заявник. Загалом ЄСПЛ визнав, що перешкоди, які ставлять для того, щоб унеможливити доступ до інформації, яка має суспільний інтерес, можуть відбити бажання у тих, хто працює в ЗМІ або в суміжних сферах, виконувати життєво важливу функцію «сторожового пса суспільства». Суд дійшов висновку, що мало місце порушення статті 10.

У **праві ЄС** чітко визначено важливість принципу прозорості. Цей принцип закріплено в статтях 1 і 10 ДЄС, та в статті 15 (1) в ДфЄС.[37] Як передбачено у частині 2 преамбули Регламенту (ЄС) №1049/2001, він наближає громадян до участі у процесі прийняття рішень і є гарантією того, що уряд має більшу легітимність і є більш ефективним і більш підзвітним громадянам у демократичній системі.[38]

36 ЄСПЛ, рішення у справі «*Таршашаг о Сабадшагйогокерт проти Угорщини*» *(Tarsasag a Szabadsagjogokert v. Hungary),* № 37374/05 від 14 квітня 2009 р.; див. пункти 27, 36–38.

37 ЄС (2012), консолідовані версії Договору про Європейський Союз та ДфЄС, OJ 2012 C 326.

38 CJEU, C-41/00 P, *ТОВ «Interporc Im- und Export» проти Комісії Європейських Співтовариств» (Interporc Im- und Export GmbH v. Commission of the European Communities)* від 6 березня 2003 р, пункт 39; та СЄС, C-28/08 P, *«Європейська комісія проти Баваріан Лагер лтд»* від 29 червня 2010 р., пункт 54.

Тому у положеннях Регламенту Ради (ЄС) № 1290/2005 щодо фінансування спільної сільськогосподарської політики та Регламенту Комісії (ЄС) № 259/2008, який деталізує положення застосування Регламенту Ради, закріплено вимогу щодо необхідності оприлюднювати інформацію про отримувачів певних фондів ЄС у аграрному секторі, а також про отримання коштів кожним отримувачем.[39] Оприлюднення має сприяти здійсненню громадського контролю за належним використанням урядом державних коштів. Пропорційність такого оприлюднення була оскаржена декількома отримувачами.

Приклад: у справі *«Товариство громадського права «Фолькер і Маркус Шеке» і Харттмут Айферт проти землі Гессен»*[40] СЄС повинен був винести рішення про пропорційність оприлюднення інформації (вимога права ЄС), про імена отримувачів сільськогосподарських субсидій ЄС і отримані ними кошти.

Суд, зазначаючи, що право на захист персональних даних не є абсолютним, висловив сумнів, що оприлюднення даних про отримувачів двох фондів сільськогосподарської допомоги ЄС і отримані ними точні суми на сайті, є втручанням у їхнє приватне життя загалом, а також порушенням права на захист їхніх персональних даних, зокрема.

Суд вважає, що таке втручання у гарантовані статтями 7 та 8 Хартії права передбачено законом і відповідає загальній меті, яка визнається ЄС, а саме: зміцнення прозорості використання суспільних коштів. Попри це СЄС постановив, що оприлюднення імен фізичних осіб, які є отримувачами сільськогосподарської допомоги цих двох фондів ЄС, і отриманих ними точних сум, не відповідає вимогам статті 52 (1) Хартії щодо пропорційності та виправданості. Таким чином Суд визнав закони ЄС щодо оприлюднення інформації про отримувачів європейських сільськогосподарських фондів частково необґрунтованими.

39 Регламент Ради (ЄС) № 1290/2005 від 21 червня 2005 р. щодо фінансування спільної сільськогосподарської політики, OJ 2005 L 209; та Регламент Комісії (ЄС) № 259/2008 від 18 березня 2008 р., який деталізує положення застосування Регламенту Ради (ЄС) № 1290/2005 щодо оприлюднення інформації про отримувачів, які отримують кошти від Європейського сільськогосподарського гарантійного фонду (EAGF) та Європейського сільськогосподарського фонду розвитку сільських територій (EAFRD), OJ 2008 L 76.

40 СЄС, об'єднані справи C-92/09 та C-93/09, *«Товариство громадського права «Фолькер і Маркус Шеке» (C-92/09) та Харттмут Айферт (C-93/09) проти землі Гессен» (Volker and Markus Schecke GbR (C-92/09) and Hartmut Eifert(C-93/09) v. Land Hessen)* від 9 листопада 2010 р., пункти 47–52, 58, 66–67, 75, 86 та 92.

1.2.3. Свобода художньої творчості і науково-дослідницької діяльності

Ще одним правом, яке потебує встановлення балансу з правом на повагу до приватного життя і правом на захист персональних даних, є право на художню творчість і науково-дослідницьку діяльність, яке відкрито гарантується у статті 13 Хартії. Воно, в основному, виводиться із права на свободу думки і вираження поглядів і має здійснюватися з урахуванням статті 1 Хартії (людська гідність). ЄСПЛ вважає, що право на свободу творчості охороняється статтею 10 ЄКПЛ.[41] Здійснення гарантованого статтею 13 Хартії права також може підлягати обмеженням, визначеним у статті 10 ЄКПЛ.[42]

Приклад: У справі «*Об'єднання працівників образотворчого мистецтва проти Австрії*»[43] австрійські суди заборонили заявникові (об'єднанню) продовжувати виставку картини з фотографіями голів громадських діячів, тіла яких були зображені у позах, які мали сексуальний зміст. Австрійський парламентар, фото якого було використано в полотні, подав позов до суду проти заявника, намагаючись отримати судову заборону на експонування картини. У відповідь на це національний суд видав судову заборону. ЄСПЛ нагадав, що стаття 10 ЄКПЛ застосовується до поширення ідей, які ображають, шокують або викликають стурбованість у держави або частини населення.

Ті, хто створив, виконав, розповсюдив або виставив твори мистецтва, сприяють обміну ідеями та думками, а держава зобов'язана не втручатися у їхнє право на свободу вираження поглядів. Враховуючи, що картина – це колаж, у якому було використано лише фотокартки голів людей, і що зображення їх тіл було нереалістичним і перебільшеним, що навряд чи могло би не тільки відобразити, але й натякнути на реальність, ЄСПЛ також зазначив, що «картину навряд чи можна розуміти як таку, що спрямована на деталі [відображеного] приватного життя, а радше можна пов'язати з його репутацією політика», і що «в цій ролі [зображений на

41 ЄСПЛ, рішення у справі «*Мюллер та інші проти Швейцарії*» *(Muller and Others v. Switzerland)*, № 10737/84 від 24 травня 1988 р.

42 Пояснення до Хартії основних прав, OJ 2007 C 303.

43 ЄСПЛ, рішення у справі «*Об'єднання працівників образотворчого мистецтва проти Австрії*» (*Vereinigung bildender Kunstler v. Austria)*, № 68345/01 від 25 січня 2007; див. особливо пункти 26 та 34.

картині] мав би бути більш толерантним до критики». Зважуючи різні інтереси, ЄСПЛ встановив, що необмежена заборона на подальшу експозицію картини була непропорційною. Суд дійшов висновку, що було порушено статтю 10 ЄКПЛ.

Що стосується науково-дослідницької діяльності, європейське право про захист персональних даних враховує те особливе значення, яке наука має в суспільстві. Тому загальні обмеження щодо використання персональних тут є меншими. І Директива про захист персональних даних, і Конвенція 108 дозволяють зберігати персональні дані для наукових досліджень, якщо вони більше не потрібні для цілей, для яких їх спочатку збирали. Крім того, подальше використання персональних даних для наукових досліджень не вважається таким, що не відповідає меті. Перед національним законодавством стоїть завдання розробити більш детальні положення, які б включали необхідні гарантії щодо узгодження мети наукових досліджень з правом на захист персональних даних (див. також розділи 3.3.3 і 8.4).

1.2.4. Захист власності

Право на захист власності закріплено у статті 1 Першого протоколу до ЄКПЛ, а також у статті 17 (1) Хартії. Одним із важливих аспектів права власності є захист інтелектуальної власності, на що відкрито вказується у статті 17 (2) Хартії. У правовій системі ЄС можна знайти ряд директив, у яких передбачено ефективний захист інтелектуальної власності, зокрема авторського права. Інтелектуальна власність охоплює не тільки питання прав на літературні та художні твори, але також патентні права, право на торгову марку і суміжні права.

Як роз'яснено у прецедентних рішеннях СЄС, захист основоположного права на володіння майном має бути узгоджений із захистом інших основоположних прав, зокрема, з правом на захист персональних даних.[44] Траплялися справи, коли установи захисту авторських прав вимагали від Інтернет-провайдерів розкрити особи користувачів файлообмінних Інтернет-платформ. Такі платформи часто дозволяють інтернет-користувачам безкоштовно завантажувати музичні твори навіть попри те, що ті захищені авторським правом.

44 ЄСПЛ, рішення у справі «Ешбі Дональд та інші проти Франції» (Ashby Donald and others v. France), № 36769/08 від 10 січня 2013 р.

Приклад: справа *«Музичне виробництво в Іспанії (організація «Promusicae») проти AT «Telefonica de Espana»*[45] стосувалася відмови іспанського Інтернет провайдера (Telefonica) розкрити некомерційній організації музичних продюсерів і видавців музичних та аудіовізуальних записів «Promusicae» персональні дані про деяких осіб, яким надавалися послуги з доступу до Інтернет. «Promusicae» добивалася розкриття інформації з метою подання цивільного позову проти тих осіб, які, як вона зазначала, використовували файлообмінну програму доступу до фонограм, права на експлуатацію яких належали членам «Promusicae».

Суд Іспанії передав справу на розгляд до СЄС із запитом про те, чи потрібно в рамках права Співтовариств повідомляти персональні дані в контексті цивільного позову щодо забезпечення ефективного захисту авторських прав. Він посилався на Директиви 2000/31, 2001/29 і 2004/48, розтлумачені у контексті статті 17 і 47 Хартії. СЄС дійшов висновку, що ці три директиви, а також Директива про секретність та електронні комунікації (2002/58/ЄС) не перешкоджає здійсненню державою-членом зобов'язання щодо розкриття персональних даних у контексті цивільного позову щодо забезпечення ефективного захисту авторських прав.

СЄС зазначив, що у справі піднімаються питання про необхідність узгодження вимог захисту різних основоположних прав, а саме права на повагу до приватного життя, з правом на захист власності і ефективний засіб правового захисту.

Суд дійшов висновку, що «держави-члени повинні звертати увагу на необхідність брати до уваги тлумачення вказаних директив під час їх транспозиції, що надасть можливість досягати справедливого балансу між різними основоположними правами, які гарантує правова система Співтовариств. Окрім того, здійснюючи заходи щодо транспозиції цих директив, державні органи і суди держав-членів повинні не тільки тлумачити свої національні закони у спосіб, який відповідає цим директивам, але й бути впевненими, що вони не залежатимуть від їхнього тлумачення, що суперечило б тим основоположним правам або іншим загальним принципам права Співтовариств, як, наприклад, принципу пропорційності».[46]

45 СЄС, C-275/06, *«Музичне виробництво в Іспанії (організація «Promusicae») проти AT «Telefonica de Espana»* (*Productores de Musica de Espana (Promusicae) v. Telefonica de Espana SAU*) від 29 січня 2008 р., пункти 54 і 60.

46 Там само, пункти 65 і 68; див. також СЄС, C-360/10, *«Компанія «SABAM» проти AT «Netlog»* (*SABAM v. Netlog N.V.)* від 16 лютого 2012 р.

2 Терміни у сфері захисту персональних даних

ЄС	питання, що висвітлюються	РЄ
Персональні дані		
Директива про захист персональних даних, стаття 2 (а) СЄС, об'єднані справи C-92/09 та C-93/09 *«Товариство громадського права «Фолькер і Маркус Шеке» (C-92/09) та Гартмут Айферт (C-93/09 проти землі Гессен»*, 29 листопада 2010 р. СЄС, C-275/06, *«Музичне виробництво в Іспанії (організація «Promusicae») проти АТ «Telefonica de Espana»*, 29 січня 2008 р.	**правове визначення**	Конвенція 108, стаття 2 (а) рішення ЄСПЛ у справі *«Бернх Ларсен Холдинг АС» та інші проти Норвегії»*, № 24117/08 від 14 березня 2013 р.
Директива про захист персональних даних, стаття 8 (1) СЄС, C-101/01 «*Боділ Ліндквіст»*, 6 листопада 2003 р.	**Спеціальні категорії персональних даних (чутливі дані)**	Конвенція 108, стаття 6

ЄС	питання, що висвітлюються	РЄ
Директива про захист персональних даних 6 (1) (e)	**анонімні дані та псевдоніми**	Конвенція 108, стаття 5 (e) Конвенція 108, Пояснювальна доповідь, стаття 42
Обробка даних		
Директива про захист персональних даних, стаття 2 (b) СЄС, C-101/01 «*Боділ Ліндквіст*», 6 листопада 2003 р.	**дефініції**	Конвенція 108, стаття 2 (c)
Користувачі даних		
Директива про захист персональних даних, стаття 2 (d)	**володілець**	Конвенція 108, стаття 2 (d) *Профайлінг Рекомендація*, стаття 1 (g) *
Директива про захист персональних даних, стаття 2 (e) СЄС, C-101/01 «*Боділ Ліндквіст*», 6 листопада 2003 р.	**розпорядник**	*Профайлінг Рекомендація* стаття 1 (h)
Директива про захист персональних даних, стаття 2 (g)	**одержувач**	Конвенція 108, Додатковий протокол, стаття 2 (1)
Директива про захист персональних даних, стаття 2 (f)	**третя особа**	
Згода		
Директива про захист персональних даних, стаття 2 (h) Суд ЄС, C-543/09 «*Компанія «Deutsche Telekom» проти Федеративної Республіки Німеччина*», 5 травня 2011р.	**визначення і вимоги щодо незаперечної згоди**	Рекомендація щодо захисту медичних даних, стаття 6, та ряд наступних рекомендацій

*Примітка: *Рада Європи, Комітет Міністрів (2010), Рекомендація (2010)13 державам-*членам щодо захисту фізичних осіб у зв'язку з автоматизованою обробкою персональних даних у контексті використання таких даних (профайлінг) *(Профайлінг рекомендація), 23 листопада 2010 р.*

2.1. Персональні дані

Ключові моменти

- Дані набувають характеру персональних даних в разі, коли в них йдеться про встановлену особу чи, принаймні, особу, яку можна встановити,
- Особою, яку можна встановити, є така, додаткову інформацію про яку можна встановити без необґрунтованих зусиль, і яка дозволяє ідентифікувати відповідну особу.
- Аутентифікація означає підтвердження того факту, що певна особа має певну ідентичність та/або має право здійснювати певні види діяльності.
- Існують особливі категорії даних, так звані чутливі дані, перелік яких наводиться у Конвенції 108 і в Директиві про захист персональних даних, і які потребують посиленого захисту а, отже, є предметом особливого правового режиму.
- Анонімні дані – це ті, які не мають жодних ідентифікаторів; псевдоніми – ті, у яких ідентифікатори зашифровано.
- На відміну від анонімних даних, псевдоніми є персональними даними.

2.1.1. Основні аспекти поняття персональних даних

І у **праві ЄС,** і у **праві РЄ** «персональні дані» визначаються як інформація, що пов'язана з ідентифікацією або можливою ідентифікацією фізичної особи[47], тобто інформація про особу, ідентичність якої відкрито встановлена або ж може бути встановлена за допомогою отримання додаткової інформації. Особа, персональні дані якої обробляються, визначається як «суб'єкт персональних даних».

Особа

Право на захист персональних даних бере початок із права на повагу до приватного життя. Поняття «приватне життя» стосується людей. Отже, фізичні особи – це головні вигодонабувачі від захисту персональних даних. До того ж відповідно до висновку робочої групи «Стаття 29» тільки *жива особа* може пе-

47 Директива про захист персональних даних, ст. 2 (a); Конвенція 108, ст. 2 (a).

ребувати під захистом європейського законодавства про захист персональних даних.[48]

Судова практика ЄСПЛ в питаннях застосування статті 8 ЄКПЛ свідчить про те, що повністю відокремити окремі питання приватного та професійного життя може бути складно.[49]

Приклад: У справі *«Аманн проти Швейцарії»*[50] державні органи влади перехопили телефонну розмову заявника, яка стосувалася питань його бізнесу. На підставі цього дзвінка державні органи влади провели розслідування діяльності заявника і завели на нього картку для зберігання у картотеці національної служби безпеки.

Незважаючи на той факт, що перехоплений телефонний дзвінок стосувався бізнесу, ЄСПЛ розглянув питання зберігання персональних даних про цей дзвінок у зв'язку з приватним життям заявника. Він зазначив, що термін «приватне життя» не повинен тлумачитися вузько, оскільки повага до приватного життя включає право встановлювати і розвивати відносини з іншими людьми. Окрім того, жодних підстав для відокремлення діяльності професійного і ділового характеру від поняття «приватне життя» не було. Таке широке тлумачення відповідає Конвенції 108. ЄСПЛ також встановив, що у справі заявника втручання було незаконним, оскільки у національному законодавстві не було передбачено спеціальних чи конкретних положень про збирання, реєстрацію та зберігання інформації. Таким чином Суд дійшов висновку, що було порушено статтю 8 ЄКПЛ.

Більше того, якщо питання професійного життя також може бути предметом захисту персональних даних, то виникає запитання, чому лише фізичним особам має бути забезпечено захист. Згідно ЄСПЛ права гарантуються всім особам, а не лише фізичним.

48 Робоча група «Стаття 29» (2007), *Висновок 4/2007 щодо концепції персональних даних*, РГ 136, 20 червня 2007, с. 22.

49 Див., наприклад: рішення ЄСПЛ у справі *«Ротару проти Румунії» (Rotaru v. Romania)* [ВП], № 28341/95 від 4 травня 2000 р., п. 43; рішення ЄСПЛ у справі *«Німітц проти Німеччини» (Niemietz v. Germany)*, № 13710/88 від 16 грудня 1992 р., п. 29.

50 Рішення ЄСПЛ у справі *«Аманн проти Швейцарії» (Amann v. Switzerland)* [ВП], № 27798/95 від 16 лютого 2000 р., п. 65.

У судовій практиці ЄСПЛ є рішення у справах про порушення права на захист від використання даних, визначеного у статті 8 ЄКПЛ, заявниками в яких є юридичні особи. Проте Суд розглянув справу у контексті права на повагу до житла і кореспонденції, а не у контексті приватного життя:

Приклад: справа «*Бернх Ларсен Холдінг АС та інші проти Норвегії*»[51] стосувалася оскарження трьома норвезькими компаніями наказу податкового органу надати податковим аудиторам копії усіх даних з комп'ютерного серверу, яким усі три компанії спільно користувалися.

ЄСПЛ визнав, що факт вимагання такої інформації від заявника (компанії) є втручанням у його право на повагу до «житла» і «кореспонденції» у значенні статті 8 ЄКПЛ. Проте Суд визнав, що у податкових органів були ефективні та адекватні гарантії проти зловживань: заявника (компанії) було завчасно повідомлено; компанії були на місці і могли відразу подати заперечення проти втручання; матеріал міг бути знищеним після завершення аудиту. За таких обставин було дотримано справедливий баланс між правом заявника (компаній) на повагу до «житла» та «кореспонденції», інтересом заявника щодо захисту приватності осіб, які на нього працюють, з одного боку, та інтересами суспільства щодо забезпечення ефективного аудиту в цілях податкової оцінки, з іншого. Суд постановив, що за цих причин не було порушено статтю 8.

Згідно Конвенції 108 захист персональних даних стосується, насамперед, захисту фізичних осіб; попри це Договірні Сторони можуть розширювати у своєму національному законодавстві дію захисту персональних даних на юридичних осіб, таких, як бізнес-компанії та об'єднання.

Загалом у праві ЄС про захист персональних даних не охоплюються питання захисту юридичних осіб у зв'язку з обробкою персональних даних, які їх стосуються. Національні регулятивні органи є вільними щодо регулювання цього питання.[52]

51 Рішення ЄСПЛ у справі «*Бернх Ларсен Холдинг АС» та інші проти Норвегії*» (*Bernh Larsen Holding AS and Others v. Norway*), № 24117/08 від 14 березня 2013 р. Проте див. також рішення ЄСПЛ у справі «*Лібертi» та інші проти Сполученого Королівства*» (*Liberty and Others v. the United Kingdom*), № 58243/00 від 1 липня 2008 р.

52 Директива про захист персональних даних, п. 24 преамбули.

Приклад: у справі *«Товариство громадського права «Фолькер і Маркус Шеке» і Хартмут Айферт проти землі Гессен»*[53] щодо оприлюднення персональних даних про отримувачів сільськогосподарської допомоги СЄС постановив, що «юридичні особи у зв'язку з таким розкриттям можуть заявляти про свої права у світлі статей 7 та 8 Хартії лише за умови, якщо з офіційної назви юридичної особи можна встановити одну або декілька фізичних осіб. [... П]раво на повагу до приватного життя у зв'язку з обробкою персональних даних, передбачене у статтях 7 і 8 Хартії, стосується будь-якої інформації про встановлену особу або особу, яку можна встановити. [...]».[54]

Можливість встановлення особи

І в праві ЄС, і в праві РЄ інформація є такою, що містить персональні дані, якщо:

- з неї можна встановити особу; або
- якщо особу не встановлено, але дано опис у такий спосіб, який шляхом подальшого розслідування робить можливим з'ясування, хто є суб'єктом персональних даних.

Захист обох видів інформації гарантується у європейському законодавстві про захист персональних даних однаково. ЄСПЛ неодноразово заявляв, що і у ЄКПЛ, і у Конвенції 108 поняття «персональні дані» визначається однаково, особливо у зв'язку з умовою, що дані повинні стосуватися встановлених осіб або таких, яких можна встановити. [55]

У визначенні поняття «персональні дані» не наведено більше роз'яснень, коли особа вважається такою, що може бути встановленою.[56] Вочевидь процес встановлення повинен складатися із елементів, які описують особу у такий спосіб, який має відрізняти його або її від усіх інших осіб та робити його

53 СЄС, об'єднані справи C-92/09 та C-93/09 «Товариство громадського права «*Фолькер і Маркус* Шеке» *і Хартмут* Айферт *проти землі Гессен» (Volker and Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v. Land Hessen)* від 9 листопада 2010, п. 53.

54 Там само, п. 52.

55 Див. рішення у справі ЄСПЛ «*Аманн проти Швейцарії» (Amann v. Switzerland)* [ВП], №. 27798/95 від 16 лютого 2000 р., п. 65 та ін.

56 Див. рішення ЄСПЛ у справі «*Одієвр проти Франції» (Odievre v. France)* [ВП], №. 42326/98 від 13 лютого 2003 р.; та рішення ЄСПЛ у справі «*Годеллі проти Італії*» (*Godelli v. Italy)*, №. 33783/09 від 25 вересня 2012 р.

або її пізнаваним. Ім'я особи є яскравим прикладом таких елементів опису. У виняткових випадках такий самий ефект, як ім'я, можуть мати інші ідентифікатори. Наприклад, у ситуації з громадськими діячами може бути достатньо посилання на їх посаду, приміром: Голова Європейської Комісії.

> Приклад: у справі «*Музичне виробництво в Іспанії (організація «Promusicae») проти AT «Telefonica de Espana»*[57] СЄС заявив, що «не викликає питань той факт, що процедура повідомлення імен та адрес певних користувачів [однієї файлообмінної платформи інтернет], якого домагалась «Promusicae», передбачає розкриття персональних даних, тобто інформації, яка стосується встановлених осіб або осіб, яких можна встановити, відповідно до визначення, даного у статті 2 (а) Директиви 95/46 [...]. Така передача інформації (якщо «Promusicae» надасть, а «Telefonica» не оскаржуватиме), яка зберігається у «Telefonica», є процесом обробки персональних даних у розумінні першого пункту статті 2 Директиви 2002/58, яка читається разом зі статтею 2 (б) Директиви 95/46».

Беручи до уваги той факт, що більшість імен не є неповторними, у процесі встановлення особи може виникнути необхідність у додаткових ідентифікаторах для того, щоб не сплутати особу з іншою особою. Зазвичай використовується дата і місце народження. Окрім того, в деяких країнах, щоб краще розрізняти осіб, було введено персональні індивідуальні номери. У вік технологій зростаючої важливості для встановлення осіб набувають біометричні дані, такі, як відбитки пальців, цифрові фотокартки або сканування райдужної оболонки ока.

Для того, щоб європейське право про захист персональних даних стало застосовуватися, зовсім не потребується якісна ідентифікація відповідної особи; достатньо того, щоб цю особу можна було ідентифікувати. Особа вважається такою, яку можна ідентифікувати, якщо інформація містить ідентифікатори, за допомогою яких особу можна ідентифікувати прямо чи опосередковано.[58] Згідно пункту 26 преамбули Директиви про захист персональних даних відправною точкою є імовірність існування розумних засобів для встановлен-

57 СЄС, C-275/06, *«Музичне виробництво в Іспанії (організація «Promusicae») проти AT «Telefonica de Espana»* (*Productores de Musica de Espana (Promusicae) v. Telefonica de Espana SAU)* від 29 січня 2008 р., п. 45.

58 Директива про захист персональних даних, ст. 2 (а).

ня особи, а також їх здійснення передбачуваними користувачами інформації; включаючи одержувачів – третіх осіб (див. розділ 2.3.2).

Приклад: місцева влада вирішує зібрати інформацію про перевищення швидкості на місцевих вулицях. Вона фотографує автомобілі, автоматично реєструючи час і місце, для того, щоб передати дані компетентному органу для накладення штрафу на тих, хто порушив вимоги щодо обмеження швидкості. Суб'єкт персональних даних подає скаргу на дії місцевої влади, яка за законом про захист персональних даних не має на це права. Місцева влада стверджує, що не збирає персональні дані. Номерні знаки, як вона заявляє, це анонімна інформація. У місцевої влади немає юридичних прав на доступ до реєстру загальних транспортних засобів, інформація з якого допомогла би з'ясувати особу власника автомобіля або водія.

Таке пояснення не відповідає пункту 26 преамбули Директиви про захист персональних даних. Беручи до уваги мету збирання даних, як-то: чітко встановити та накласти штраф на любителів швидкості, можна передбачити, що будуть здійснені спроби щодо їх ідентифікації. Незважаючи на те, що у місцевої влади немає наявних засобів ідентифікації особи, вона передасть інформацію компетентному органу, поліції, у якої вони є. У пункті 26 преамбули також чітко передбачено умови, за яких майбутні одержувачі даних, які не є прямим користувачем даних, можуть спробувати встановити особу. У світлі пункту 26 преамбули дії місцевого органу влади прирівнюються до збирання даних про осіб, яких можна ідентифікувати, а тому для їх здійснення мали би бути правові підстави у законодавстві про захист персональних даних.

У праві РЄ можливість ідентифікації особи розуміється так само. Наприклад, у статті 1 (2) Рекомендації щодо захисту персональних даних, які використовуються для сплати та інших споріднених операцій[59], йдеться про те, що особу не вважають такою, яку можна ідентифікувати, якщо процес ідентифікації потребує необґрунтовано багато часу, коштів або робочої сили.

59 РЄ, Комітет міністрів (1990), Рекомендація щодо захисту персональних даних, які використовуються для сплати та інших споріднених операцій, 13 вересня 1990 р.

Аутентифікація

Це процедура, за допомогою якої особа здатна довести, що вона володіє певною ідентичністю і/або має право вчиняти певні дії, такі, як входити до охоронюваної зони або знімати гроші з банківського рахунку. Аутентифікація здійснюється шляхом порівняння біометричних даних як-то: фотокартка або відбитки пальців у паспорті з даними, які особа представляє власноруч, приміром, у пункті імміграційного контролю; або шляхом надання відомої тільки особі інформації про ідентичність або авторизацію, наприклад, персональний ідентифікаційний номер (PIN) або пароль; або ж шляхом пред'явлення певного знаку, який має знаходитись виключно у володінні особи, про її ідентичність або авторизацію як, наприклад, спеціальної чіп-карти або ключа до банківського сейфу. Окремо від паролів або чіп-карт, а іноді і PIN-кодів, інструментом, який власне здатен ідентифікувати та аутентифікувати особу у контексті електронної комунікації є електронний підпис.

Характер персональних даних

Будь-яка інформація може бути даними персонального характеру за умови, що вона стосується якоїсь особи.

> Приклад: оцінка інспектора про виконання роботи працівником, що зберігається в особовій справі працівника, є персональними даними про нього, навіть якщо просто частково або повністю відображає особисту думку керівництва, наприклад, таку: «працівник не присвячує себе роботі», або не дуже сувору: «працівник за останні шість місяців був відсутній на роботі протягом п'яти тижнів».

Персональні дані стосуються як інформації про приватне життя особи, так і її професійного чи громадського життя.

У справі «Аманн»[60] ЄСПЛ визначив термін «персональні дані» як такий, що не обмежується питаннями приватної сфери особи (див. розділ 2.1.1.). Таке саме визначення міститься і у Директиві про захист персональних даних:

60 Див. рішення ЄСПЛ у справі *«Аманн проти Швейцарії» (Amann v. Switzerland)*, № 27798/95 від 16 лютого 2000 р., п. 65.

Приклад: у справі *«Товариство громадського права «Фолькер і Маркус Шеке» і Хартмут Айферт проти землі Гессен»*[61] СЄС постановив, що «у зв'язку з цим не має значення, чи стосуються оприлюднені дані діяльності професійного характеру [...]. У цьому питанні Європейський суд з прав людини з посиланням на тлумачення статті 8 Конвенції постановив, що термін «приватне життя» не слід тлумачити обмежено і що немає жодної принципової причини для того, щоби виправдати виключення діяльності [...] професійного характеру з поняття «приватне життя».

Дані також стосуються осіб, якщо зміст інформації опосередковано розкриває дані про особу. У деяких випадках, коли існує тісний зв'язок між об'єктом або подією, наприклад, мобільний телефон, автомобіль, нещасний випадок, з одного боку, і особа, наприклад, його власник, користувач, жертва, з іншого боку, інформацію про об'єкт або про подію також слід розглядати як таку, що містить персональні дані.

Приклад: у справі *«Уцун проти Німеччини»*[62] за заявником і ще за одним чоловіком через підозру в причетності до вибухів було встановлено стеження за допомогою пристрою системи глобального позиціонування (GPS), який було встановлено в автомобілі чоловіка. У цій справі ЄСПЛ постановив, що стеження за заявником через GPS було втручанням у його право на приватне життя, яке гарантується статтею 8 ЄКПЛ. Проте GPS стеження здійснювалося у відповідності до закону, а також було пропорційним законній меті здійснення розслідування декількох епізодів замаху на вбивство і тому було необхідним у демократичному суспільстві. Суд постановив, що в цьому випадку не було порушено статтю 8 ЄКПЛ.

Форма представлення персональних даних

Форма, в якій персональні дані зберігаються або використовуються, не має відношення до застосовності законодавства про захист персональних даних. Письмовий або усний формат передачі даних може містити персональ-

61 Рішення ЄСПЛ у справі *«Леандер проти Швеції» (Leander v. Sweden)*, № 9248/81 від 26 березня 1987 р., п. п. 59.

62 Рішення ЄСПЛ у справі *«Узун проти Німеччини» (Uzun v.Germany)*, № 35623/05 від 2 вересня 2010 р.

ну інформацію та зображення,[63] включаючи дані, записані за допомогою замкнутої системи ТВ-спостереження (CCTV)[64] або звукові дані.[65] Персональними даними може бути інформація як з електронного, так і з паперового носія; навіть зразки клітин тканини людини можуть бути персональними даними, оскільки містять ДНК людини.

2.1.2. Особливі категорії персональних даних

У **праві ЄС та РЄ** існують особливі категорії персональних даних, які за своєю природою можуть становити загрозу для суб'єктів, персональні дані яких обробляються, і потребують посиленого захисту. Тому дозвіл на обробку цих особливих категорій даних («чутливих») повинен надаватися лише з особливими гарантіями.

І у Конвенції 108 (стаття 6), і у Директиві про захист персональних даних (стаття 8) визначаються такі категорії чутливих даних:

- персональні дані, які розкривають расове чи етнічне походження;
- персональні дані, які розкривають політичні, релігійні чи інші переконання; та
- персональні дані, які стосуються здоров'я або статевого життя.

Приклад: у справі «*Боділ Ліндквіст*»[66] СЄС заявив, що «посилання на те, що особа травмувала ногу і працює на півставки за медичними показаннями, становить персональні дані, які стосуються здоров'я у розумінні статті 8 (1) Директиви 95/46».

63 Рішення ЄСПЛ у справі «*Фон Ганновер проти Німеччини*» *(Von Hannover v. Germany)*, № 59320/00 від 24 червня 2004 р.; рішення ЄСПЛ у справі «*Шіакка проти Італії*» *(Sciacca v. Italy)*, № 50774/99 від 11 січня 2005 р.

64 Рішення ЄСПЛ у справі «*Пек проти Сполученого Королівства*» *(Peck v. the United Kingdom)*, № 44647/98 від 28 січня 2003 р.; рішення ЄСПЛ у справі «*Кьопке проти Німеччини*» *(Kopke v. Germany)*, № 420/07 від 5 жовтня 2010 р.

65 Директива про захист персональних даних, пп. 16 і 17 преамбули; рішення ЄСПЛ у справі «*П.Г. і Дж.Х. проти Сполученого Королівства*» *(P.G. and J.H. v. the United Kingdom)*, № 44787/98 від 25 вересня 2001 р., пп. 59 та 60; рішення ЄСПЛ у справі «*Віссе проти Франції*» *(Wisse v. France)*, № 71611/01 від 20 грудня 2005 р.

66 СЄС, C-101/01, «*Боділ Ліндквіст*» *(Bodil Lindqvist)* від 6 листопада 2003 р., п. 51.

Директива про захист персональних даних додає до списку чутливих даних «членство в профспілці», оскільки ця інформація може бути суттєвим ідентифікатором політичних переконань або членства у партії.

У Конвенції 108 персональні дані, які стосуються кримінального засудження, також віднесено до чутливих даних.

Стаття 8 (7) Директиви про захист персональних даних зобов'язує держави – члени ЄС «визначати умови, за яких можна здійснювати обробку національного ідентифікаційного коду чи будь-якого іншого ідентифікатора загального застосування.»

2.1.3. Анонімні дані та псевдоніми

Відповідно до принципу збереження персональних даних протягом обмеженого періоду, який передбачено в Директиві про захист персональних даних та у Конвенції 108 (і більш детально розглядається у розділі 3), дані повинні зберігатись «у формі, що дозволяє встановлювати особу суб'єктів персональних даних не довше, ніж це необхідно для мети, заради якої дані були зібрані чи заради якої вони надалі обробляються.» [67] Отже, якщо володілець хоче зберігати вже неактуальні персональні дані, які більше не відповідають своїй початковій меті, вони мають бути знеособлені.

Анонімні дані

Дані є анонімними, якщо з персональних даних виключено всі ідентифікатори. Жоден ідентифікуючий елемент не може бути залишений в інформації, яка шляхом здійснення розумних зусиль може сприяти повторному встановленню визначеної(их) особи(осіб). [68] Якщо дані успішно знеособлено, вони більше не є персональними.

Якщо персональні дані більше не слугують своїй початковій меті, але повинні зберігатися в персональній формі з метою історичного, статистичного чи наукового використання, Директива про захист персональних даних і Конвенція 108 надають таку можливість за умови встановлення відповідних гарантій проти зловживань. [69]

67 Директива про захист персональних даних, ст. 6 (1) (e); та Конвенція 108, ст. 5 (e).

68 Там само, п. 26 преамбули.

69 Там само, ст. 6 (1) (e); та Конвенція 108, ст. 5 (e).

Псевдоніми

У персональній інформації є такі ідентифікатори, як ім'я, дата народження, стать і адреса. Якщо персональні дані вигадуються, ідентифікатори замінюються псевдонімами. Псевдонімізація здійснюється, наприклад, за допомогою кодування ідентифікаторів в персональних даних.

У Конвенції 108 або у Директиві про захист персональних даних немає відкритого визначення для псевдонімів. Проте у статті 42 Пояснювальної доповіді до Конвенції 108 зазначається, що «[в]имога [...] щодо термінів зберігання іменних даних не означає, що через деякий час їх потрібно буде раз і назавжди відокремити від імені особи, якої вони стосуються, а означає відсутність можливості швидко встановити зв'язок між даними і ідентифікаторами». Цього можна досягти шляхом псевдонімізації даних. Тим, хто не володіє дешифрувальним ключем, важко буде ідентифікувати псевдоніми. Власне у самій формі псевдоніма є зв'язок з особою, до якої додається дешифрувальний ключ. Ті, хто має право використовувати дешифрувальний ключ, можуть із легкістю здійснити повторну ідентифікацію. Проти використання дешифрувальних ключів не уповноваженими на це особами мають вживатися запобіжні заходи.

У випадку, якщо не існує можливості повністю відмовитися від використання персональних даних, псевдонімізація, за великим рахунком, є одним з найбільш важливих засобів забезпечення захисту персональних даних, але логіку і результат цього процесу необхідно детально пояснювати.

Приклад: речення «Charles Spencer (Чарльз Спенсер), народився 3 квітня 1967 року, батько чотирьох дітей: двох хлопчиків і двох дівчаток» може бути псевдонімізовано таким чином:

«C. S. 1967, батько чотирьох дітей: двох хлопчиків і двох дівчаток»; або

«324 батько чотирьох дітей: двох хлопчиків і двох дівчаток»; або

«YESz320l батько чотирьох дітей: двох хлопчиків і двох дівчаток».

Користувачі, у яких є доступ до цих псевдонімізованих даних, не зможуть відтворити речення «Чарльз Спенсер, народився 3 квітня 1967 року» із формату «324» або «YESz3201». Найвірогідніше, що такі дані будуть захищені від неналежного використання.

Проте у цьому випадку існує ризик. Якщо речення «C.S. 1967, батько чотирьох дітей: двох хлопчиків і двох дівчаток» використовується у контексті маленького села, у якому живе Чарльз Спенсер, можна легко зрозуміти, що це саме він. Метод псевдонімізації впливає на ефективність процедури захисту персональних даних.

Персональні дані з шифрувальними ідентифікаторами як засіб збереження ідентичності осіб використовуються у різних контекстах. Це особливо важливо у ситуації, коли володільцям персональних даних потрібна впевненість у тому, що вони мають справу з одними і тими самими суб'єктами персональних даних, але водночас, коли вони не можуть вимагати або їм не слід мати реальні відомості про суб'єктів даних. Це, приміром, той випадок, коли дослідник вивчає історію хвороби пацієнтів, особи яких відомі тільки лікарні, у якій вони лікуються, і від якої він отримує ці історії з псевдонімами. Тому псевдонімізація – це ефективний засіб в арсеналі технологій зі зміцнення конфіденційності, важливий елемент планового забезпечення конфіденційності. Це означає, що захист персональних даних вбудовано в сучасну структуру системи обробки персональних даних.

2.2. Обробка персональних даних

Ключові моменти

- термін «обробка» стосується, здебільшого, автоматизованого процесу.
- Відповідно до **права ЄС** «обробка» здійснюється додатково до ручної обробки структурованих картотек даних.
- Відповідно до **права РЄ** значення «обробка» може поширюватися національним законодавством на процес ручної обробки.

Процес захисту персональних даних відповідно до Конвенції 108 і Директиви про захист персональних даних зосереджується, насамперед, на процесі автоматизованої обробки персональних даних.

Проте у визначенні, даному поняттю «автоматизована обробка» у **праві РЄ,** передбачається, що між автоматизованими операціями може виникати потреба у застосуванні ручної обробки персональних даних. Так само, у **праві ЄС** автоматизована обробка персональних даних визначається як «операція,

що здійснюється з персональними даними за допомогою повного чи часткового використання автоматизованих засобів.»[70]

> Приклад: у справі *«Боділ Ліндквіст»*[71] СЄС постановив, що «посилання на Інтернет-сторінці на різних осіб та їх ідентифікація за іменем або за допомогою інших засобів, наприклад, за телефонним номером або інформацією про умови праці чи хобі, становить процес «обробки персональних даних за допомогою повного чи часткового використання автоматизованих засобів» у розумінні статті 3 (1) Директиви 95/46».

Процедура ручної обробки даних також потребує захисту персональних даних.

Відповідно до **права ЄС** захист персональних даних відбувається не лише під час автоматизованої обробки. Тому у **праві ЄС** захист даних застосовується до обробки персональних даних, які зберігаються у неавтоматизованій картотеці, тобто у спеціально структурованій паперовій картотеці.[72] Причиною такого розширення сфери дії захисту даних є те, що:

- паперові картотеки структуровано у такий спосіб, який пришвидшує і полегшує пошук інформації; та
- зберігання персональних даних у структурованих паперових картотеках допомагає обійти обмеження, які стосуються процесу автоматизованої обробки даних.[73]

У **праві РЄ,** а саме у Конвенції 108, головним чином регулюється процес обробки даних, які зберігаються у файлах для автоматизованої обробки.[74] У ній також передбачено можливість поширення у національному законодавстві процедури захисту на процес ручної обробки. Багато держав, які є Сторонами Конвенції 108, скористалися цією можливістю і повідомили про це у своїх заявах на ім'я Генерального Секретаря РЄ.[75] Розширення дії захисту персональних даних в рамках такої заяви має стосуватися усього процесу ручної

70 Конвенція 108, ст. 2 (c); та Директива про захист персональних даних, ст. 2 (b) та ст. 3 (1).

71 СЄС, C-101/01, *«Боділ Ліндквіст» (Bodil Lindqvist)* від 6 листопада 2003 р., п. 27

72 Директива про захист персональних даних, ст. 3 (1).

73 Там само, п. 27 преамбули.

74 Конвенція 108, ст. 2 (b).

75 Див. заяви, зроблені в рамках Конвенції 108, ст. 3 (2) (c).

обробки персональних даних і не може обмежуватися обробкою даних неавтоматизованих картотек. [76]

Що стосується характеру охоплених процесом обробки операцій, поняття обробки є загальним як у **праві ЄС, так і у праві РЄ**: «обробка персональних даних» [...] означає будь-яку операцію, здійснювану з персональними даними [...] таку, як збір, реєстрація, організація, зберігання, адаптація чи зміна, пошук, консультація, використання, розкриття за допомогою передачі, поширення чи іншого надання, упорядкування чи комбінування, блокування, стирання чи знищення.» [77] Термін «обробка» також охоплює дії, в результаті яких дані виходять з-під відповідальності одного володільця і передаються під відповідальність іншого.

Приклад: роботодавці збирають та обробляють інформацію про своїх співробітників, включаючи й ту, яка стосується їхньої заробітної плати. Правовою підставою таких дій є трудовий договір.

Роботодавцям потрібно буде відправити інформацію про зарплату своїх співробітників до податкових органів. Такий процес передачі даних також означатиме «обробку» у розумінні цього терміна Конвенцією 108 та Директивою. Проте для цього розкриття трудовий договір не може бути правовою підставою. Для здійснення операцій з обробки персональних даних мають існувати додаткові правові підстави, які б узаконили передачу роботодавцем інформації про заробітну плату податковим органам. Зазвичай, такою правовою базою є національне податкове законодавство. В іншому випадку процес передачі даних вважатиметься незаконною обробкою.

76 Див. текст Конвенції 108, ст. 3 (2).

77 Директива про захист персональних даних, ст. 2 (b). Також див. Конвенцію 108, ст. 2 (c).

2.3. Користувачі персональних даних

Ключові моменти

- Той, хто вирішує обробляти персональні дані інших осіб є «володільцем» відповідно до законодавства про захист персональних даних; якщо таке рішення приймається декількома особами, вони можуть бути «спільними володільцями».
- «Розпорядник» є юридично самостійним суб'єктом, який/яка на підставі закону обробляє персональні дані від імені володільця.
- Розпорядник стає володільцем, якщо він або вона використовують персональні дані у власних цілях і не дотримуються вказівок володільця.
- Будь-хто, хто отримує дані від володільця, є «розпорядником».
- «третя особа» – це фізична або юридична особа, яка не виконує вказівки володільця (і не є суб'єктом персональних даних).
- «Розпорядник – третя особа» – це фізична або юридична особа, яка юридично відокремлена від володільця, але отримує персональні дані від володільця.

2.3.1. Володільці та розпорядники

Найбільш важливим у роботі володільця або розпорядника є правова відповідальність за дотримання передбачених у законодавстві про захист персональних даних відповідних зобов'язань. Лише ті, кого може бути притягнуто до відповідальності за чинним законодавством, можуть зайняти ці посади. У приватному секторі це, зазвичай, фізична або юридична особа; в державному – орган державної влади. Інші суб'єкти, наприклад, органи або установи, які не мають правосуб'єктності, можуть бути володільцями або розпорядниками, якщо це передбачено спеціальним законодавством.

Приклад: Якщо відділ маркетингу компанії «Саншайн» запланує здійснити обробку даних з метою дослідження ринку, компанія «Саншайн», а не відділ маркетингу, буде володільцем такої обробки. Відділ маркетингу не може бути володільцем, оскільки не має окремої правосуб'єктності.

Якщо компанії входять до складу групи, компанія-засновник і кожна філія, які є самостійними юридичними особами, вважаються окремими володільцями або

розпорядниками. Такий самостійний правовий статус кожного члена групи виливається у необхідність існування спеціальної правової бази, яка б дозволила взаємну передачу персональних даних. Привілеїв, які б уможливили обмін персональними даними між окремими юридичними особами в рамках групи, не існує.

У цьому контексті варто згадати про роль фізичних осіб. Відповідно до **права ЄС** фізичні особи, здійснюючи обробку персональних даних інших осіб під час діяльності виключно особистого чи побутового характеру, не підпадають під дію норм Директиви про захист персональних даних; вони не вважаються володільцями.[78]

Проте судовою практикою встановлено, що право з питань захисту персональних даних застосовується до фізичної особи тоді, коли вона викладає в Інтернет персональну інформацію про інших осіб.

Приклад: у справі «*Боділ Ліндквіст*»[79] СЄС підтвердив, що: «згадування на інтернет-сторінці різних осіб та їх ідентифікація за іменем або за допомогою інших засобів є процесом «обробки персональних даних за допомогою повного чи часткового використання автоматизованих засобів» у розумінні статті 3 (1) Директиви 95/46».[80]

Така обробка персональних даних не підпадає під значення діяльності виняткового особистого чи побутового характеру, яка не охоплюється дією Директиви про захист персональних даних, оскільки цей виняток «повинен [...] тлумачитися як такий, що стосується лише діяльності, що здійснюється у приватному або сімейному житті осіб, яке, ясна річ, не має відношення до процедури обробки персональних даних, які містяться в інтернет-публікації і є доступними для невизначеного кола осіб.»[81]

Володілець

У праві ЄС «володілець» – це той, «хто окремо чи разом з іншими визначає мету і процедури обробки персональних даних.[82] Володілець вирішує, чому і як персональні дані оброблятимуться. У **праві РЄ** визначення «володілець»

78 Директива про захист персональних даних, п. 12 преамбули та ст. 3 (2) останній абзац.

79 СЄС, C-101/01, справа «*Боділ Ліндквіст*» *(Bodil Lindqvist)* від 6 листопада 2003 р.

80 Там само, п. 27.

81 Там само, п. 47.

82 Директива про захист персональних даних, ст. 2 (d).

також містить положення про те, що володілець вирішує, які категорії персональних даних повинні зберігатися. [83]

У даному Конвенцією 108 визначенні «володільця» є посилання на додатковий аспект здійснення контролю, який слід розглянути. Це визначення стосується питання про те, хто саме на законних підставах може обробляти певні персональні дані для певної мети. Однак, якщо здійснюються начебто незаконні операції обробки і має бути знайдено відповідального володільця, це має бути фізична чи юридична особа, як-то компанія чи державний орган, які незалежно від наявності у них для цього законних підстав, прийняли рішення щодо обробки персональних даних[84]. Тому запит на видалення має завжди направлятися на ім'я «фактичного» володільця.

Спільне володіння

У визначенні «володілець», яке дається у Директиві про захист персональних даних, зазначено, що володільцями можуть бути декілька окремих юридичних осіб, які діють разом або солідарно з іншими. Це означає, що вони разом приймають рішення щодо здійснення обробки для спільної мети.[85] З правової точки зору це можливо за умови, якщо для процедури спільної обробки даних для спільної мети передбачено спеціальні правові підстави.

Приклад: спільне використання бази даних некредитоспроможних клієнтів декількома кредитними установами є поширеним прикладом спільного володіння. Коли будь-хто звертається за кредитом із того банку, який є одним із спільних володільців, банки перевіряють базу даних, щоб допомогти прийняти обґрунтовані рішення щодо кредитоспроможності заявника.

У документах прямо не зазначено, чи потребує спільне володіння наявності загальної мети для всіх володільців, чи досить того, що їхня мета лише частково співпадає. На жаль, на європейському рівні поки немає відповідної судової практики з цього питання, а також ясності щодо наслідків такої відповідальності. Робоча група «Стаття 29» виступає за більш широке тлумачення поняття «спільне володіння», яке б додало деякої гнучкості у реагування на

83 Конвенція 108, ст. 2 (d).

84 Див. також робоча група 29 статті (2010), *Висновок 1/2010 щодо понять «володілець» та «розпорядник»*, РГ 169, Брюссель від 16 лютого 2010р., с. 15.

85 Директива про захист персональних даних, ст. 2 (d).

зростаючі потреби процесу обробки персональних даних.[86] Справа Спільноти всесвітніх міжбанківських фінансових телекомунікацій (SWIFT) доводить позицію робочої групи.

Приклад: у так званій справі СВІФТ європейські банківські установи користувалися системою СВІФТ (спочатку у статусі розпорядника) для управління передачею даних у ході банківських операцій. Не маючи прямої вказівки європейських банківських установ, які користувалися цією системою, СВІФТ розкрив Міністерству фінансів США інформацію про банківську транзакцію, яка зберігалась в обчислювальному сервісному центрі в Сполучених Штатах Америки (США). Робоча група «Стаття 29», оцінюючи законність цієї ситуації, дійшла висновку, що європейські банківські установи, які користувались системою СВІФТ, а також саму систему СВІФТ слід було б вважати спільними володільцями, які б несли відповідальність перед європейськими клієнтами за розкриття органам влади США їхніх персональних даних.[87] Система СВІФТ, вирішуючи питання про розкриття, незаконно взяла на себе роль володільця; банківські установи, вочевидь, не справилися з функцією нагляду за своїм розпорядником і, отже, не могли бути повністю звільнені від відповідальності володільців. Результат такої ситуації – спільне володіння.

Розпорядник

Як визначено у **праві ЄС,** розпорядник персональних даних – це той, хто обробляє персональні дані від імені володільця.[88] Доручена розпоряднику діяльність може бути обмежена дуже конкретним завданням чи контекстом або може бути досить загальною і широкою.

У праві РЄ визначення «розпорядник персональних даних» має те ж саме значення, що й у **праві ЄС.**

Окрім обробки персональних даних для третіх осіб розпорядники також мають право бути володільцями персональних даних у зв'язку з обробкою, яку

86 Робоча група «Стаття 29» (2010), *Висновок 1/2010 щодо понять «володілець» та «розпорядник»*, РГ 169, Брюссель від 16 лютого 2010р., с. 15.

87 Робоча група «Стаття 29» (2006), *Висновок 10/2006 щодо обробки персональних даних Спільнотою всесвітніх міжбанківських фінансових телекомунікацій (SWIFT),* РГ 128, Брюссель, 22 листопада 2006 р.

88 Директива про захист персональних даних, ст. 2 (e).

вони здійснюють для власних цілей, наприклад для управління своїм персоналом, заробітними платами та рахунками.

Приклади: компанія «Евереді» спеціалізується на обробці даних у сфері управління людськими ресурсам для інших компаній. У цій функції «Евереді» є розпорядником обробки.

Якщо ж «Евереді» обробляє дані своїх співробітників, тоді вона – володілець персональних даних для здійснення своїх зобов'язань як роботодавця.

Зв'язок між володільцем та розпорядником обробки персональних даних

Ми вже з`ясували, що володілець – це той, хто визначає мету і процедури обробки персональних даних.

Приклад: директор компанії «Саншайн» вирішує, що компанії «Мунлайт», яка є спеціалістом з питань аналізу ринку, слід провести аналіз ринку даних клієнтів «Саншайн». Незважаючи на те, що завдання щодо визначення засобів обробки має делегуватися «Мунлайт», компанія «Саншайн» залишається володільцем, а «Мунлайт» – лише розпорядником, оскільки у відповідності до договору «Мунлайт» може використовувати дані про клієнтів компанії «Саншайн» тільки для цілей, які визначить «Саншайн».

Незважаючи на те, що право визначати засоби обробки делеговано розпоряднику, володілець повинен мати можливість втручатися у рішення розпорядника щодо засобів обробки. Загальну відповідальність також покладено на володільця, який повинен контролювати відповідність рішень розпорядника законодавству про захист персональних даних. Договір, який забороняє володільцю втручатися у рішення розпорядника, ймовірно, може бути розтлумачено як такий, що витікає зі спільного здійснення контролю, до того ж, коли обидві сторони поділяють однакову відповідальність володільця.

Окрім того, якщо розпорядник не дотримується встановлених володільцем обмежень щодо використання даних, розпорядник стає володільцем, принаймні, настільки, наскільки серйозно порушено інструкції володільця. Це, най-

імовірніше, зробить розпорядника володільцем, який діє незаконно. У свою чергу, першому володільцю доведеться пояснити факт порушення розпорядником своїх функцій. Насправді робоча група «Стаття 29» схиляється до спільного здійснення контролю у таких випадках, оскільки результатом є кращий захист інтересів суб'єктів персональних даних.[89] Важливим наслідком спільного здійснення контролю має бути солідарна відповідальність за збитки з наданням суб'єктам персональних даних більш широкого діапазону захисту.

У випадку, якщо володілець – це мале підприємство, а розпорядник – велика корпоративна компанія, яка має право диктувати умови щодо надання своїх послуг, має бути поставлено питання про розподіл відповідальності, незважаючи на те, що робоча група «Стаття 29» вважає, що рівень відповідальності не повинен знижуватися через економічний дисбаланс і що витлумачення поняття «володілець» має залишатись незмінним. [90]

Задля ясності і прозорості деталі взаємовідносин між володільцем і розпорядником слід виписувати у письмовому договорі.[91] Відсутність такого договору є порушенням зобов'язання володільця щодо надання письмової документації про взаємні обов'язки і може призвести до накладення санкцій. [92]

Може статись, що розпорядники вважатимуть за необхідне делегувати певні завдання додатковим допоміжним розпорядникам. Із точки зору закону це допускається і залежатиме від деталей умов договору між володільцем і розпорядником, включаючи питання про те, чи необхідно щоразу отримувати дозвіл володільця, чи достатньо одноразового повідомлення.

У **праві РЄ,** як пояснювалося вище, визначення понять «володілець» і «розпорядник» є повністю застосовним, доказом чого є розроблені відповідно до Конвенції 108 рекомендації.[93]

89 Робоча група 29 статті (2010), *Висновок 1/2010 щодо понять «володілець» та «розпорядник»*, РГ 169, Брюссель від 16 лютого 2010р., с.25; Робоча група «Стаття 29» (2006), *Висновок 10/2006 щодо обробки персональних даних Спільнотою всесвітніх міжбанківських фінансових телекомунікацій* (СВІФТ), РГ 128, Брюссель, 22 листопада 2006 р.

90 Робоча група 29 статті (2010), *Висновок 1/2010 щодо понять «володілець» та «розпорядник»*, РГ 169, Брюссель від 16 лютого 2010р., с.26

91 Директива про захист персональних даних, ст. 17 (3) та (4).

92 Робоча група «Стаття 29» (2010), *Висновок 1/2010 щодо понять «володілець» та «розпорядник»*, РГ 169, Брюссель від 16 лютого 2010р., с.27.

93 Див., наприклад, Профайлінг Рекомендацію, ст. 1.

2.3.2. Одержувачі і треті особи

Різниця між цими двома категоріями фізичних або юридичних осіб, як визначено у Директиві про захист персональних даних, стосується, здебільшого, їх зв'язку з володільцем і, як результат, їхнього права на доступ до персональних даних володільця.

«Третя особа» – це той, хто на законних підставах відрізняється від володільця. Тому процедура розкриття даних третій особі має бути визначена спеціальним законом. Відповідно до статті 2 (f) Директиви про захист персональних даних, «третя особа» означає «будь-яку фізичну чи юридичну особу, державний орган, агентство чи будь-який інший орган, інший, ніж суб'єкт персональних даних, володільця, розпорядника персональних даних і осіб, що, будучи безпосередньо підпорядкованими володільцю чи розпоряднику персональних даних, уповноважені обробляти такі дані». Це означає, що особи, які працюють в організації, яка своїм правовим статусом відрізняється від володільця, навіть якщо належить до тієї ж групи або холдингової компанії, будуть «третьою особою» (або належатимуть «третій особі»). З іншого боку, філії того банку, який здійснює обробку рахунків своїх клієнтів з прямого дозволу своїх штаб-квартир, не будуть «третьою особою». [94]

Термін «одержувач» має ширше значення, ніж термін «третя особа». У значенні статті 2 (г) Директиви про захист персональних даних, «одержувач» це – «фізична або юридична особа, державний орган, установа чи будь-який інший орган, якому надаються дані, незалежно від того є він третьою особою, чи ні». Цей одержувач може бути особою, яка не входить до складу володільця або розпорядника, тоді це – третя особа; або особою, яка входить до складу володільця або розпорядника, наприклад співробітник або інший відділ у межах однієї компанії або державного органу.

Відмінність між одержувачами і третіми особами є важливою лише у зв'язку з умовами законного оприлюднення персональних даних. Співробітники володільця або розпорядника можуть без будь-яких законних вимог бути одержувачами персональних даних, якщо беруть участь у їхніх операціях з обробки. З іншого боку, третя особа, яка є юридично самостійною по відношенню до володільця або розпорядника, не має права використовувати оброблені володільцем персональні дані, за винятком, коли це передбачено спеціальним законом у кожному конкретному випадку. Тому для того, щоб отримати персо-

94 Робоча група «Стаття 29» (2010), *Висновок 1/2010 щодо понять «володілець» та «розпорядник»*, РГ 169, Брюссель від 16 лютого 2010р., с. 31.

нальні дані у законний спосіб, у «одержувачів-третьої особи» завжди повинні бути правові підстави.

Приклад: працівник розпорядника, який використовує персональні дані в межах доручених йому або їй роботодавцем завдань, є одержувачем даних, але не третьою особою, оскільки він чи вона використовують дані від імені та за дорученням розпорядника.

Проте якщо той самий працівник вирішує використовувати дані, до яких він або вона можуть отримати доступ з позиції співробітника розпорядника, для власних цілей і з метою продати їх іншій компанії, то він або вона діє як третя особа. У такому випадку він або вона більше не виконують доручення розпорядника (роботодавця). Як третій особі такому працівнику необхідно мати правові підстави для отримання та продажу даних. У цьому прикладі у працівника, звичайно ж, немає таких правових підстав, а тому його дії є незаконними.

2.4. Згода

Ключові моменти

- Згода як правова основа для обробки персональних даних має бути вільно вираженою, поінформованою та висловленою окремо.
- Згода має бути недвозначною. Згоду може бути надано прямо або шляхом дій, які не залишають сумнівів у тому, що суб'єкт персональних даних погоджується на обробку своїх даних.
- Для здійснення обробки чутливих даних необхідна чітко висловлена згода.
- Згоду може бути відкликано в будь-який момент.

Згода означає «будь-яке вільне, окреме та поінформоване висловлення бажання суб'єктом персональних даних.»[95] Згода у більшості випадків є правовою підставою для законної обробки персональних даних (розділ 4.1).

95 Директива про захист персональних даних, ст. 2 (h).

2.4.1. Складові елементи дійсної згоди

У **праві ЄС** визначено три складові, які роблять згоду дійсною, та гарантують, що суб'єкти персональних даних дійсно висловлювали свою згоду на використання їхніх персональних даних:

- під час надання згоди суб'єкт даних не повинен зазнавати тиску;
- суб'єкт персональних даних повинен бути належним чином поінформований про мету і наслідки надання згоди; і
- межі поширення згоди мають бути розумними та конкретними.

Лише за умови виконання усіх цих вимог згода буде дійсною відповідно до законодавства про захист персональних даних.

Конвенція 108 не дає визначення поняттю «згода»; це право залишено за національним законодавством. Проте у **праві РЄ** складові елементи незаперечної згоди відповідають вказаним вище, оскільки закладені у рекомендаціях, розроблених відповідно до Конвенції 108.[96] Вимоги щодо згоди є такими самими, що й для незаперечного волевиявлення, закріпленого у європейському цивільному праві.

Передбачені у цивільному праві додаткові вимоги щодо незаперечної згоди, наприклад, правоздатність, зазвичай застосовуються також у контексті захисту персональних даних, оскільки ці вимоги є основоположними правовими засадами. Відсутність незаперечної згоди осіб, які не є правоздатними, означатиме відсутність правових підстав для здійснення обробки їхніх персональних даних.

Згода може бути висловлена безпосередньо і відкрито[97] або ж опосередковано. Перша не залишає сумнівів щодо намірів суб'єкта персональних даних і може бути надана в усній або письмовій формі; щодо останньої можна зробити висновок, виходячи із обставин. Кожна згода має бути недвозначною.[98] Це означає, що не повинно бути жодних розумних сумнівів у тому, що суб'єкт персональних даних хотів(ла) повідомити про свою згоду, якою дозволяється обробка його або її персональних даних. Приміром, виведення згоди з простої відсутності дій не може тлумачитись як неоднозначна згода. У випадку, коли обробці підлягають чутливі дані, наявність безпосередньої недвозначної згоди є обов'язковою.

96 Див., наприклад, Конвенцію 108, Рекомендацію щодо статистичних даних, п. 6.

97 Директива про захист персональних даних, ст. 8 (2).

98 Там само, ст. 7 (a) та ст. 26 (1).

Вільно виражена згода

Вільно виражена згода є дійсною тільки тоді, коли «суб'єкт персональних даних здатен робити справжній вибір і немає жодних ризиків обману, залякування, примусу або істотних негативних наслідків, якщо він/вона не дає згоди».[99]

Приклад: у багатьох аеропортах пасажирам для того, щоб зайти у зону посадки, потрібно пройти крізь «сканери тіла».[100] Сканування передбачає обробку їхніх персональних даних, тому повинне здійснюватися з дотриманням одного з критеріїв статті 7 Директиви про захист персональних даних (див. розділ 4.1.1). Іноді проходження крізь «сканери тіла» представляють пасажирам як їх право вибору, маючи на увазі, що лише їхня згода уможливить його здійснення. Однак, пасажири можуть побоюватися, що своєю відмовою від проходження вони викличуть підозру або сприятимуть здійсненню додаткового контролю, наприклад, особистого огляду. Багато пасажирів погоджуються на сканування, намагаючись тим самим уникнути можливих проблем або затримок. Така згода, звісно, не є достатньо вільно вираженою.

Із цього слідує, що потужні правові підстави можуть бути лише в законодавчому документі, в основі якого лежать принципи статті 7 (e) Директиви про захист персональних даних, і які можуть зобов'язати пасажирів співпрацювати з огляду на існування переважаючого суспільного інтересу. У такому документі може бути передбачено можливість вибору між скануванням і обшуком, але тільки в рамках додаткових заходів прикордонного контролю, необхідних у конкретних умовах. Саме це було запропоновано Європейською комісією у 2011 р. у двох Регламентах щодо використання сканерів безпеки[101].

Вільному вираженню згоди можуть загрожувати ситуації підпорядкування, у яких існує значний економічний або інший дисбаланс між володільцем,

99 Див. також, Робоча група «Стаття 29» (2011), *Висновок щодо концепції «згода»*, РГ 187, Брюссель, 13 липня 2011р., с. 12.

100 Цей приклад взято звідти ж, с. 15.

101 Регламент Комісії (ЄС) № 1141/2011 від 10 листопада 2011 р., що вносить зміни до Регламенту (ЄС) № 272/2009, який доповнює загальні базові норми про безпеку цивільної авіації стосовно використання сканерів безпеки в аеропортах ЄС, OJ 2011 L 293, та Регламент Комісії щодо імплементації (ЄС) № 1147/2011 від 11 листопада 2011р., що вносить зміни до Регламенту (ЄС) № 185/2010, який доповнює загальні базові норми про безпеку цивільної авіації стосовно використання сканерів безпеки в аеропортах ЄС, OJ 2011 L 294.

який забезпечує безпеку згоди, і суб'єктом персональних даних, який надає згоду.[102]

Приклад: велика компанія виключно для цілей вдосконалення внутрішньої комунікації планує створити довідник з іменами всіх співробітників, їх функціями та адресами їхніх офісів. Керівник відділу кадрів пропонує додати в довідник фотокартки кожного співробітника, аби полегшити, приміром, процес впізнавання колег на засіданнях. Представники персоналу компанії наполягають на тому, що це повинно здійснюватися лише за згоди співробітників.

У такій ситуації згоду співробітників слід визнати правовою підставою процесу обробки фотокарток у довіднику, тому що зрозуміло, що, власне, сама наявність надрукованих у довіднику фото не матиме негативних наслідків, більше того, навряд чи працівники відчують негативні наслідки з боку роботодавця, якщо не зголосяться на друк своїх фото у довіднику.

Проте це не означає, що згода ніколи не може бути дійсною в умовах, коли її ненадання мало б негативні наслідки. Якщо, приміром, ненадання згоди на отримання картки клієнта у супермаркеті призведе до того, що клієнт не отримає знижки на окремі товари, то для тих клієнтів, які погодилися отримати цю картку, їхня згода є незаперечною правовою основою для обробки їхніх персональних даних. У цьому випадку немає підпорядкування між компанією і клієнтом, і наслідки ненадання згоди не є настільки серйозними для суб'єкта персональних даних, щоб не допускати вільного вибору.

З іншого боку, щоразу, коли достатньо важливі товари або послуги можуть бути отримані тільки і виключно за умов передачі певних персональних даних третім особам, згода суб'єкта даних на таке розкриття, зазвичай, не може вважатися вільним рішенням і тому не є дійсною, як того вимагає законодавство про захист персональних даних.

Приклад: висловлена згода пасажирів на передачу авіакомпанії так званих записів реєстрації пасажира (PNR), а саме інформації про себе, звички

102 Див. також Робоча група «Стаття 29» (2001), *Висновок 8/2001 щодо обробки персональних даних у контексті працевлаштування*, РГ 48, Брюссель, 13 вересня 2001 р.; та Робоча група «Стаття 29» (2005), *Робочий документ щодо спільного тлумачення статті 26 (1) Директиви 95/46/ЕС від 24 жовтня 1995 р.*, РГ 114, Брюссель, 25 листопада 2005 р.

у харчуванні чи проблеми зі здоров'ям до імміграційних органів конкретної іноземної держави не може розглядатися як дійсна згода в рамках даного законодавства про захист персональних даних, оскільки подорожуючі пасажири змушені це робити, якщо хочуть потрапити до цієї країни. Якщо такі дані потрібно передати на законних підставах, має існувати не просто згода, а інші правові підстави, наприклад, спеціальний закон.

Поінформована згода

Для того, щоб суб'єкт персональних даних міг прийняти рішення, у нього має бути достатньо інформації. Те, чи є надана інформація достатньою, чи ні, має вирішуватися окремо в кожному випадку. Зазвичай, поінформована згода включає точний і легко зрозумілий опис суті справи, у зв'язку з якою необхідне надання згоди, а також виклад наслідків надання або ненадання згоди. Викладена інформація має бути зрозумілою тим, кому вона адресується.

Окрім того, суб'єкту персональних даних має бути забезпечено легкий доступ до інформації. Доступність і наочність інформації є її важливими елементами. В умовах інтернет середовища хорошим рішенням можуть бути багаторівневі інформаційні повідомлення, оскільки суб'єкт персональних даних міг би отримувати не тільки стислу інформацію, але й більш повну.

Окрема згода

Щоби бути дійсною, згода також має бути окремою. Це узгоджується з якістю наданої інформації про мету згоди. У цьому контексті відповідними будуть розумні очікування звичайного суб'єкта персональних даних. Якщо необхідно доповнити операції з обробки або змінити їх у спосіб, який не можна було розумно передбачити, коли давалась початкова згода, суб'єкта персональних даних ще раз запитують про згоду.

Приклад: у справі *«Компанія «Deutsche Telekom» проти Федеративної Республіки Німеччина»*[103] СЄС розглядав питання про те, чи потрібно телекомунікаційному провайдеру, який передав персональні дані абонентів

103 СЄС, C-543/09, *«Компанія «Deutsche Telekom» проти Федеративної Республіки Німеччина» (Deutsche Telekom AG v. Germany)*, від 5 травня 2011 р.; особливо див. пп. 53 та 54.

відповідно до вимоги статті 12 Директиви про секретність та електронні комунікації,[104] отримувати нову згоду суб'єктів персональних даних через той факт, що одержувачі, коли надавалась згода, мали іншу назву.

СЄС постановив, що відповідно до вимог цієї статті не було необхідності в отриманні нової згоди для того, щоб передати дані, тому що суб'єкти персональних даних, як передбачено цією нормою, мали можливість надати згоду тільки для цілей здійснення обробки, які полягали в оприлюдненні їхніх даних, і не могли вибирати між різними адресними книгами, в яких могли бути надруковані ці дані.

Як підкреслив Суд, «із контекстного і систематичного тлумачення статті 12 Директиви про секретність та електронні комунікації слідує, що згода відповідно до статті 12 (2) відноситься до мети, з якою було надруковано персональні дані у публічній адресній книзі, а не до будь-якого конкретного постачальника адресної книги».[105]

Окрім того, «власне, саме оприлюднення персональних даних у публічній адресній книзі з певною метою може зашкодити не автору публікації, а абонентам».[106]

2.4.2. Право відкликати згоду у будь-який час

У Директиві про захист персональних даних не передбачено загальне право відкликати згоду в будь-який час. Проте вважається, що таке право існує і що у суб'єкта персональних даних повинна бути можливість скористатися ним на власний розсуд. Не може бути ані жодних вимог щодо обґрунтування свого відкликання, ані ризиків негативних наслідків від скасування будь-яких вигод, які могли би бути від раніше даної згоди на використання персональних даних.

104 Директива 2002/58/ЄС Європейського парламенту та Ради від 12 липня 2002 р. «Про обробку персональних даних та захист таємниці у секторі електронних комунікацій» (*Директива про секретність та електронні комунікації*), OJ 2002 L 201.

105 CJEU, C-543/09, *«Компанія «Deutsche Telekom» проти Федеративної Республіки Німеччина» (Deutsche Telekom AG v. Germany)* від 5 травня 2011 р.; особливо див. п. 61.

106 Там само, особливо див. п. 62.

Приклад: клієнт погоджується отримувати рекламну пошту на адресу, яку він або вона надає володільцю даних. Якщо клієнт відкликає свою згоду, володілець повинен відразу припинити відправку рекламної пошти. Жодних санкцій, як-то накладення штрафу, не повинно бути.

Якщо клієнт отримував 5% знижку вартості готельного номера в обмін на згоду використовувати його або її дані у рекламній пошті, наступне відкликання згоди на отримання рекламної пошти не повинно призвести до необхідності виплати суми наданої знижки.

3

Ключові принципи захисту персональних даних у європейському законодавстві

ЄС	питання, що висвітлюються	РЄ
Директива про захист персональних даних, стаття 6 (1) та (b) СЄС, C-524/06, *«Хубер проти Німеччини» (Huber v. Germany)* від 16 грудня 2008 р. СЄС, об'єднані справи C-92/09 та C-93/09 *«Товариство громадського права «Фолькер і Маркус Шеке» та Гарттмут Айферт проти землі Гессен»* від 9 листопада 2010 р.	**принцип законності обробки**	Конвенція 108, стаття 5 (a) та (b) ЄСПЛ, *«Ротару проти Румунії» (Rotaru v. Romania)* [ВП], № 28341/95, 4 травня 2000р. «ЄСПЛ, *«Тейлор-Себорі проти Сполученого Королівства» (Taylor-Sabori v.the United Kingdom)*, № 47114/99, 22 жовтня 2002 р. ЄСПЛ, *«Пек проти Сполученого Королівства» (Peck v. The United Kingdom)*, № 44647/98, 28 січня 2003 р. ЄСПЛ, *«Хелілі проти Швейцарії» (Khelili v. Switzerland)*, № 16188/07, 18 жовтня 2011 р. ЄСПЛ, *«Леандер проти Швеції» (Leander v.Sweden)*, № 9248/81, 26 березня 1987 р.
Директива про захист персональних даних, стаття 6 (1) (b)	**принцип конкретизації цілей та обмеження**	Конвенція 108, стаття 5(b)

ЄС	питання, що висвітлюються	РЄ
	принципи якості даних:	
Директива про захист персональних даних 6 (1) (c)	**принцип відповідності даних**	Конвенція 108, стаття 5 (c)
Директива про захист персональних даних 6 (1) (d)	**принцип точності даних**	Конвенція 108, стаття 5 (d)
Директива про захист персональних даних, стаття 6 (1) (e)	**принцип збереження даних протягом обмеженого періоду часу**	Конвенція 108, стаття 5 (e)
Директива про захист даних, стаття 6 (1) (e)	**виключення для наукових та статистичних досліджень**	Конвенція 108, стаття 9 (3)
Директива про захист персональних даних, стаття 6 (1) (a)	**принцип ретельної обробки**	Конвенція 108, стаття 5 (a) ЄСПЛ, «*Араламбіє проти Румунії*» (*Haralambie v. Romania*), № 21737/03, 27 жовтня 2009 р. ЄСПЛ, «*К.Х. та інші проти Словаччини*» (*K.H. and Others v.Slovakia*), № 32881/04, 28 квітня 2009 р.
Директива про захист даних, стаття 6 (2)	**принцип підзвітності**	

У викладених у статті 5 Конвенції 108 принципах закріплено суть європейського права про захист персональних даних. Вони також містяться у статті 6 Директиви про захист персональних даних і є відправною точкою для більш конкретних положень наступних статей цієї Директиви. Всі розроблені пізніше правові документи РЄ або ЄС про захист персональних даних повинні відповідати цим принципам, і ці принципи слід враховувати під час тлумачення таких правових документів. Будь-які винятки і обмеження щодо цих ключових принципів мають бути передбачені на національному рівні;[107] вони повинні

107 Конвенція 108, ст. 9 (2); Директива про захист персональних даних, ст. 13 (2).

бути визначені законом, переслідувати законну мету і бути необхідними у демократичному суспільстві. Всі три умови мають бути дотримані.

3.1. Принцип законності обробки

Ключові моменти

- Для того, щоб зрозуміти принцип законності обробки, потрібно звернутися до умов законного обмеження щодо здійснення права на захист персональних даних у світлі статті 52 (1) Хартії та виправданого втручання, яке визначене в пункті другому статті 8 ЄКПЛ.
- Відповідно, обробка персональних даних є законною, якщо тільки вона:
  - відповідає закону; та
  - переслідує законну мету; та
  - є необхідною у демократичному суспільстві для досягнення законної мети.

Відповідно до **права про захист персональних даних ЄС та РЄ** принцип законності обробки є першим із перерахованих принципів; він майже однаково визначається у статті 5 Конвенції 108 та у статті 6 Директиви про захист персональних даних.

Жодне з цих положень не містить визначення того, що наповнює поняття «законна обробка». Щоб зрозуміти цей юридичний термін, необхідно звернутися до визначеного у ЄКПЛ поняття виправданого втручання у тлумаченні судової практики ЄСПЛ та умов законного обмеження статті 52 Хартії.

3.1.1. Вимоги ЄКПЛ щодо виправданого втручання

Обробка персональних даних може бути втручанням у право на повагу до приватного життя суб'єкта персональних даних. Проте право на повагу до приватного життя не є абсолютним, воно має бути збалансоване і узгоджене з іншими законними інтересами, незалежно від того, чи це інтереси інших осіб (приватні інтереси), чи інтереси суспільства в цілому (суспільні інтереси).

Умови, за яких втручання держави є виправданим, є такими:

Відповідно до закону

Практика ЄСПЛ визнає втручання законним, якщо воно передбачено у положеннях національного законодавства, що має певні характеристики. Закони повинні бути «доступними для зацікавлених осіб і передбачуваними щодо наслідків їх дії».[108] Норма є «передбачуваною», якщо вона сформульована з достатньою чіткістю, що дає змогу кожному, хто потребує відповідної поради, вивіряти свою поведінку».[109] «Ступінь чіткості, що вимагається від закону» у зв'язку з цим залежатиме від конкретного питання.» [110]

Приклад: у справі «*Ротару проти Румунії*»[111] ЄСПЛ встановив порушення статті 8 ЄКПЛ через той факт, що румунське законодавство дозволяє право збирати, записувати та зберігати в секретних файлах інформацію, яка може зашкодити інтересам національної безпеки, і не передбачає обмежень щодо здійснення цих повноважень, які залишаються на розсуд влади. Наприклад, у національному законодавстві не визначено вид інформації, який можна обробляти, категорії людей, до яких застосовуються заходи стеження, обставини, за яких можуть бути прийняті такі заходи або процедури, яких необхідно дотримуватися. З огляду на ці недоліки Суд дійшов висновку, що національне законодавство не відповідає вимозі передбачуваності у контексті статті 8 ЄКПЛ і що цю статтю було порушено.

---

108 Рішення ЄСПЛ у справі «*Аманн проти Швейцарії*» (*Amann v. Switzerland)* [ВП], № 27798/95 від 16 лютого 2000 р., п. 50; див. також рішення ЄСПЛ у справі «*Копп проти Швейцарії*» *(Kopp v. Switzerland),* № 23224/94 від 25 березня 1998 р., п. 55 та рішення ЄСПЛ у справі «*Йордачі проти Молдови*» *(Iordachi and Others v. Moldova)*, № 25198/02 від 10 лютого 2009 р., п. 50.

109 Рішення ЄСПЛ у справі «*Аманн проти Швейцарії*» (*Amann v. Switzerland)* [ВП], № 27798/95 від 16 лютого 2000 р., п. 56; див. також рішення ЄСПЛ у справі «*Малоун проти Сполученого Королівства*» *(Malone v. the United Kingdom)*, № 8691/79 від 2 серпня 1984р., п. 66; рішення ЄСПЛ у справі «*Сільвер проти Сполученого Королівства*» *(Silver and Others v. the United Kingdom)*, №№ 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75 від 25 березня 1983 р., п. 88.

110 Рішення ЄСПЛ у справі «*Санді Таймс» проти Сполученого Королівства*» *(The Sunday Times v. the United Kingdom),* № 6538/74 від 26 квітня 1979 р., п. 49; див. також «*Сільвер проти Сполученого Королівства*» *(Silver and Others v. the United Kingdom)*, №№ 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75 від 25 березня 1983 р., п. 88.

111 Рішення ЄСПЛ у справі «*Ротару проти Румунії*» *(Rotaru v. Romania)* [ВП], № 28341/95 від 4 травня 2000 р., п. 57; див. також рішення ЄСПЛ у справі «*Асоціація за європейську інтеграцію і права людини*» і *Екімджієв проти Болгарії*» *(Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria)*, № 62540/00 від 28 червня 2007 р.; рішення ЄСПЛ у справі «*Шімоволос проти Росії*» *(Shimovolos v. Russia)*, № 30194/09 від 21 червня 2011 р.; та рішення ЄСПЛ у справі «*Веттер проти Франції*) *(Vetter v. France)*, № 59842/00 від 31 травня 2005р.

Приклад: у справі «*Тейлор-Себорі проти Сполученого Королівства*»[112] за заявником було встановлено поліцейське стеження. За допомогою пейджера–клона заявника поліція змогла перехопити надіслані йому повідомлення. Згодом заявника було заарештовано і йому були пред'явлені обвинувачення у змові щодо постачання наркотиків. Частину його обвинувальної справи складали записані сучасним способом повідомлення з пейджера, які поліція розшифрувала. Однак, на момент судового розгляду справи заявника у британському законодавстві не було жодного положення, яке б регулювало процес перехоплення повідомлень, які передаються приватною телекомунікаційною системою. Отже, втручання в його права не було здійснено у «відповідності до закону». ЄСПЛ дійшов висновку, що було порушено статтю 8 ЄКПЛ.

Переслідування законної мети

Законна мета може бути або одним із перерахованих суспільних інтересів, або ж якимсь із прав і свобод інших осіб.

Приклад: у справі «*Пек проти Сполученого Королівства*»,[113] заявник намагався скоїти самогубство, розрізавши собі вени на вулиці, не підозрюючи, що все це записується на камеру відеоспостереження. Після того як поліцейські, що стежили за записами замкнутої системи ТВ-спостереження, врятували його, їх керівництво передало відеоматеріал працівникам ЗМІ, які його оприлюднили, не замаскувавши обличчя заявника. ЄСПЛ встановив, що не було жодних відповідних чи достатніх підстав, які б могли виправдати пряме доведення відеоматеріалу до відома громадськості державними органами без отримання згоди заявника або маскування його особи. Суд дійшов висновку, що було порушено статтю 8 ЄКПЛ.

112 Рішення ЄСПЛ у *справі «Тейлор-Себорі проти Сполученого Королівства» (Taylor-Sabori v. the United Kingdom)*, № 47114/99 від 22 жовтня 2002 р.

113 Рішення ЄСПЛ у справі: *«Пек проти Сполученого Королівства» (Peck v. the United Kingdom)*, № 44647/98 від 28 січня 2003 р., особливо п. 85.

Необхідність у демократичному суспільстві

ЄСПЛ зазначив, що «поняття необхідності означає, що втручання відповідає нагальній суспільній потребі і, зокрема, є пропорційним переслідуваній законній меті»[114]

Приклад: у справі «*Хелілі проти Швейцарії*»[115] під час поліцейського рейду поліція виявила заявницю, у якої були візитівки з номером телефону і таким текстом: «Симпатична, гарна жінка, за тридцять, хотіла б зустріти чоловіка, щоб іноді разом випити або провести час. Номер тел. [...]». Заявниця стверджувала, що після цього поліцейські внесли в базу її ім'я як повії, якою вона ніколи не була. Заявниця вимагала видалити слово «повія» з комп'ютерної бази. ЄСПЛ визнав, що, в принципі, збереження персональних даних особи на тій підставі, що ця особа могла вчинити інший злочин, може за певних умов бути пропорційним. Проте у справі заявниці необґрунтоване обвинувачення у незаконній проституції виявилося занадто розпливчастим і загальним і не було обґрунтовано конкретними фактами, оскільки її ніколи не було засуджено за незаконне заняття проституцією, і тому не може розглядатися як таке, що відповідає «нагальній суспільній потребі» у розумінні статті 8 ЄКПЛ. Розглядаючи питання доказування достовірності збережених про заявницю даних як питання, що відноситься до повноважень органів влади, а також серйозності втручання в права заявниці, Суд постановив, що збереження слова «повія» в файлах поліції протягом багатьох років не було необхідним у демократичному суспільстві. Суд дійшов висновку, що було порушено статтю 8 ЄКПЛ.

Приклад: у справі «*Леандер проти Швеції*»[116] ЄСПЛ постановив, що власне сама секретна перевірка осіб, які подають документи для працевлаштування на посади, які є важливими з точки зору національної безпеки, не суперечить вимогам, які є необхідними у демократичному суспільстві. Існування спеціальних гарантій, які передбачені в національному законодавстві для захисту інтересів суб'єктів персональних даних, наприклад,

114 Рішення ЄСПЛ у справі «*Леандер проти Швеції*» (*Leander v. Sweden*), № 9248/81 від 26 березня 1987 р., п. 58.

115 Рішення ЄСПЛ у справі «*Хелілі проти Швейцарії*» (*Khelili v. Switzerland*), № 16188/07 від 18 жовтня 2011р.

116 Рішення ЄСПЛ у справі «*Леандер проти Швеції*» (*Leander v. Sweden*), № 9248/81 від 26 березня 1987 р., пп. 59 та 67.

здійснення контролю парламентом і Канцлером юстиції, призвело до висновку ЄСПЛ, що шведська система здійснення перевірки персоналу відповідає вимогам статті 8 (2) ЄКПЛ. Беручи до уваги наявне у неї широке поле розсуду, держава-відповідач мала право вважати, що у справі заявника інтереси національної безпеки переважали над особистими. Суд дійшов висновку, що не було порушено статтю 8 ЄКПЛ.

3.1.2. Умови законного обмеження відповідно до Хартії ЄС

Структура Хартії і її формулювання відрізняються від ЄКПЛ. У Хартії не йдеться про втручання у гарантовані нею права, але є положення про обмеження щодо здійснення визнаних у ній прав і свобод.

Відповідно до статті 52 (1) Хартії обмеження щодо здійснення гарантованих у ній прав і свобод і, відповідно, щодо здійснення права на захист персональних даних, як-то: обробку, допускаються тільки якщо вони:

- передбачені законом; та
- дотримуються основного змісту права на захист персональних даних; та
- є необхідними, відповідають принципу пропорційності; та
- відповідають загальній меті, яка визнана Європейським Союзом, або є необхідними для захисту прав і свобод інших осіб.

Приклади: у справі *«Фолькер і Маркус Шеке»*[117] СЄС дійшов висновку, що встановленням зобов'язання оприлюднити персональні дані стосовно кожної фізичної особи, що була отримувачем допомоги від [певних сільськогосподарських фондів], у ході якого їх не було розмежовано за відповідними критеріями, такими, як період, протягом якого ці особи отримували таку допомогу, частота її надання або характер та обсяг, Рада та Комісія перевищили межі, визначені принципом пропорційності.

117 СЄС, об'єднані справи C-92/09 та C-93/09, «*Товариство громадського права «Фолькер і Маркус Шеке» (C-92/09) та Хартмут Айферт (C-93/09) проти землі Гессен» (Volker and Markus Schecke GbR (C-92/09) and Hartmut Eifert(C-93/09) v. Land Hessen)* від 9 листопада 2010 пп. 89 та 86.

> Тому СЄС визнав за необхідне оголосити недійсними деякі положення Регламенту Ради (ЄС) № 1290/2005 і оголосити Регламент № 259/2008 таким, що повністю втратив силу.[118]

Незважаючи на відмінності у формулюваннях, вимоги щодо законності обробки, передбачені у статті 52 (1) Хартії, подібні до вимог положення статті 8 (2) ЄКПЛ. Справді, перелічені у статті 52 (1) Хартії вимоги слід розглядати як такі, що відповідають вимогам, переліченим у статті 8 (2) ЄКПЛ, з огляду на те, що у статті 52 (3) Хартії у першому реченні йдеться про таке: «оскільки у Хартії містяться права, які відповідають правам, що гарантуються Конвенцією про захист прав людини та основоположних свобод, суть і обсяг цих прав повинні бути такими самими як у тих, що встановлені у вказаній Конвенції.»

Проте, як йдеться в останньому реченні статті 52 (3), «це положення не є перешкодою більш широкому захисту у європейському праві». У контексті порівняння статті 8 (2) ЄКПЛ та першого речення статті 52 (3) це може означати тільки те, що вимоги статті 8 (2) ЄКПЛ щодо виправданого втручання є мінімальними умовами законного обмеження щодо здійснення права на захист персональних даних, передбачених у Хартії. Отже, у праві ЄС процедура законної обробки персональних даних вимагає, щоб передбачені статтею 8 (2) ЄКПЛ вимоги, щонайменше, виконувались; окрім того, право ЄС могло б зафіксувати додаткові вимоги у конкретних випадках.

Відповідність принципу законної обробки у праві ЄС відповідним положенням ЄКПЛ знаходить свій подальший розвиток у статті 6 (3) ДЄС за умови, що «основоположні права, гарантовані Конвенцією про захист прав людини та основоположних свобод [...], складають загальні принципи права Союзу».

118 Регламент Ради (ЄС) № 1290/2005 від 21 червня 2005 р. щодо фінансування спільної сільськогосподарської політики, OJ 2005 L 209; та Регламент Комісії (ЄС) № 259/2008 від 18 березня 2008 р., який деталізує положення застосування Регламенту Ради (ЄС) № 1290/2005 щодо оприлюднення інформації про користувачів, які отримують кошти від Європейського сільськогосподарського гарантійного фонду (EAGF) та Європейського сільськогосподарського фонду розвитку сільських територій (EAFRD), OJ 2008 L 76.

3.2. Принцип конкретизації цілей та обмеження

Ключові моменти

- Мета обробки персональних даних має бути чітко визначена до початку процесу обробки.
- У праві ЄС передбачено необхідність чіткого визначення мети обробки; у праві РЄ це питання залишено для регулювання національним законодавством.
- Обробка персональних даних з невизначеною метою не відповідає законодавству про захист персональних даних.
- Для того, щоб персональні дані можна було використовувати у подальшому для іншої мети, яка не узгоджується з першопочатковою метою, необхідні додаткові правові підстави.
- Передача даних третій особі є новою метою і вимагає додаткового правового обґрунтування.

По суті, принцип конкретизації і обмеження мети означає, що законність обробки персональних даних залежить від мети обробки.[119] Мета обробки персональних даних має бути чітко визначена та оприлюднена володільцем до початку процесу обробки.[120] **Відповідно до права ЄС** це здійснюється або в заявному порядку, інакше кажучи, шляхом надсилання повідомлення до відповідного наглядового органу або, як мінімум, шляхом розробки внутрішньої документації, яку слід надати для здійснення інспекції наглядовим органам та надати до неї доступ суб'єкту персональних даних.

Обробка персональних даних з невизначеною і/або необмеженою метою є незаконною.

Кожна нова мета обробки персональних даних повинна мати свої окремі правові підстави і не може опиратися на той факт, що дані були здобуті або оброблені з іншою законною метою. У свою чергу, законна обробка обмежується своєю першопочатковою визначеною метою і будь-яка нова мета потребує

119 Конвенція 108, ст. 5 (b); Директива про захист персональних даних, ст. 6 (1) (b).

120 Див. також Робоча групу «Стаття 29» (2013 р.), *Висновок 03/2013 щодо мети обмеження*, РГ 203, Брюссель, 2 квітня 2013 р.

окремого нового правового обґрунтування. Рішення про розкриття персональних даних третім особам має прийматися особливо ретельно, оскільки процедура розкриття, зазвичай, є новою метою, а тому вимагає правового обґрунтування, відмінного від того, на основі якого збиралися персональні дані.

Приклад: авіакомпанія збирає дані про своїх пасажирів, що бронюють квитки, з метою забезпечення належного здійснення польоту. Авіакомпанії необхідна інформація про номери місць пасажирів; спеціальні фізичні потреби, наприклад тих, хто перебуває в інвалідних візках; особливі вимоги в харчуванні, наприклад, про кошерну або халяльну їжу. Якщо до авіакомпаній звертаються з проханням передати ці дані, що містяться в записах реєстрації пасажирів (PNR), імміграційним органам влади у місці посадки, то потім вони використовуватимуться для цілей імміграційного контролю, які відрізняються від першої мети, для якої такі дані збиралися. Тому процедура передачі цих даних імміграційній владі вимагає нового окремого правового обґрунтування.

Розглядаючи обсяги і межі окремої мети, Конвенція 108 і Директива про захист персональних даних звертаються до поняття узгодженості: використання даних для узгоджених цілей допускається на основі першого правового обґрунтування. Однак, що означає «узгоджений» – не визначено, і це питання залишається відкритим для тлумачення у кожному окремому випадку.

Приклад: продаж компанією «І» даних про клієнтів компанії «Саншайн», отриманих через CRM–систему, компанії прямого маркетингу «Мунлайт», яка хоче використати ці дані для допомоги маркетинговим компаніям третіх компаній, є новою метою, яка несумісна з CRM–системою, першою метою збирання даних про клієнтів компанією «Саншайн». Тому продаж даних компанії «Мунлайт» потребує свого власного правового обґрунтування.

На противагу цьому, використання компанією «Саншайн» даних CRM для власних маркетингових цілей, якими є відправка маркетингових повідомлень власним клієнтам про власну продукцію, зазвичай, вважається узгодженою метою.

У Директиві про захист персональних даних прямо вказано, що «подальша обробка персональних даних з метою історичного, статистичного чи науко-

вого використання не повинна вважатися невідповідною за умови надання державами-членами відповідних гарантій». [121]

Приклад: компанія «Саншайн» зібрала і зберігає дані CRM–системи про своїх клієнтів. Подальше використання цих даних компанією «Саншайн» для статистичного аналізу купівельної поведінки своїх клієнтів допускається, оскільки статистика є відповідною метою. Додаткового правового обґрунтування, як-то згоди суб'єктів персональних даних, не потрібно.

Якщо ті самі дані потрібно передати третій особі, компанії «Старлайт», виключно для цілей статистики, це допускається без додаткового правового обґрунтування, але тільки за умови встановлення відповідних гарантій, наприклад, маскування особистих характеристик суб'єктів даних, оскільки, зазвичай, для статистичних цілей вони не потрібні.

3.3. Принципи якості персональних даних

Ключові моменти

- Принципи якості персональних даних повинні реалізовуватися володільцем в усіх операціях з обробки.
- Принцип обмеженого збереження персональних даних передбачає необхідність видалення даних, як тільки вони будуть не потрібні для мети, заради якої вони були зібрані.
- Винятки з принципу обмеженого збереження мають бути передбачені у законодавстві і потребують встановлення спеціальних гарантій для суб'єктів персональних даних.

121 Приклад таких національних положень у законі Австрії про захист персональних даних (Закон про конфіденційність), Федеральний вісник законів, № 165/1999, п. 46, можна знайти англійською мовою за адресою: www.dsk.gv.at/DocView.axd?CobId=41936.

3.3.1. Принцип відповідності даних

Тільки ті дані підлягають обробці, які є «адекватними, відповідними та ненадмірними стосовно мети, з якою вони збираються та/або обробляються» [122]. Категорії вибраних для обробки персональних даних мають бути необхідними для досягнення заявленої загальної мети здійснення операцій з обробки, а володілець повинен суворо обмежувати процес збирання персональних даних такою інформацією, що прямо відповідає конкретній меті, яку переслідує процедура обробки.

У сучасному суспільстві принцип відповідності персональних даних має додаткове значення: використання персональних даних можна взагалі уникнути, якщо використовувати технології підвищеної конфіденційності або псевдоніми, результатом чого може рішення, сприятливе для забезпечення приватності. Це особливо доречно в системах з великим обсягом даних, які оброблюються.

Приклад: постійним користувачам громадського транспорту міська рада пропонує придбати за певну плату чіп-картку. Ім'я користувача написано на самій картці, а також є в чіпі в електронному форматі. Щоразу перед використанням автобуса чи трамвая потрібно прикладати чіп-картку до зчитувальних пристроїв, які встановлено, приміром, в автобусах і трамваях. Зчитані електронними пристроями дані перевіряються по базі, яка містить імена людей, що купили картки для проїзду.

Ця система не дотримується принципу відповідності у найбільш оптимальний спосіб: перевірку наявності дозволу особи користуватися транспортними засобами можна забезпечити без порівняння персональних даних чіп–картки з базою даних. Достатньо було б, наприклад, мати спеціальне електронне зображення, приміром, у вигляді штрих-коду в чіп–картці, який під час прикладання до зчитувального пристрою, підтверджував би факт дійсності/недійсності картки. Така система не буде записувати, хто і коли користувався тим чи іншим транспортним засобом. Жодна інформація про персональні дані не збиратиметься, що є оптимальним рішенням у розумінні принципу відповідності, оскільки його дія призводить до зобов'язання мінімізувати збирання даних.

122 Конвенція 108, ст. 5 (c); та Директива про захист персональних даних, ст. 6 (1) (c).

3.3.2. Принцип точності даних

Володілець персональних даних не повинен використовувати надану інформацію, не пересвідчившись у тому, що вона точна і актуалізована.

Обов'язок щодо забезпечення точності даних слід розглядати в контексті мети обробки персональних даних.

Приклад: виписуючи рахунок клієнту, компанія з продажу меблів отримала його або її персональну інформацію та адресу. Шість місяців потому та сама компанія хоче розпочати маркетингову кампанію і має бажання звернутися до своїх колишніх клієнтів. Для цього компанії необхідно отримати доступ до національного реєстру населення, у якому, ймовірно, є оновлені адреси клієнтів, оскільки мешканці зобов'язані законом повідомляти до реєстру адреси, за якими проживають. Доступ до даних цього реєстру обмежено фізичними та юридичними особами, які можуть надати обґрунтовану причину доступу.

У цій ситуації компанія на підтримку свого права збирати нові адресні дані всіх своїх колишніх клієнтів з реєстру населення не може опиратись на аргумент, що дані повинні зберігатися точними і оновленими. Дані до неї надходили у результаті виписування рахунків; на момент продажу факт отримання інформації про адресу відповідає меті. Процедура збирання нових адресних даних з правової точки зору не є обґрунтованою, оскільки маркетингові інтереси не є тими, що заміщають право на захист даних, а тому не можуть виправдати право доступу до даних реєстру.

Також можуть бути випадки, коли збереження оновлених даних заборонено законом, тому що, здебільшого, метою, для якої дані зберігають, є документування подій.

Приклад: протокол медичної операції не можна змінювати, іншими словами, «оновлювати», навіть якщо вказані у ньому дані пізніше виявляться помилковими. За таких обставин до протоколу можуть бути внесені лише доповнення до зауважень за умови чіткого зазначення їх пізнішого внесення.

З іншого боку, бувають ситуації, коли регулярна перевірка точності даних, в тому числі їх оновлення, є цілковитою необхідністю через можливість заподіяння потенційної шкоди суб'єкту персональних даних, якщо дані залишаться неточними.

Приклад: якщо будь-який клієнт бажає укласти договір з банківською установою, установа, зазвичай, перевіряє його кредитоспроможність. Для цієї мети створено спеціальну базу даних, у якій міститься кредитна історія фізичних осіб. Якщо така база міститиме неправильну або застарілу інформацію, у особи можуть виникнути серйозні проблеми. Тому володільці таких баз даних повинні докладати особливих зусиль щодо дотримання принципу точності.

Окрім того, дані, які стосуються не фактів, а підозри, наприклад, кримінального розслідування, можуть збиратися і зберігатися доти, доки володілець має правові підстави для збирання такої інформації і обґрунтовані підозри.

3.3.3. Принцип збереження даних протягом обмеженого періоду

У статті 6 (1) (e) Директиви про захист персональних даних, а також у статті 5 (e) Конвенції 108 від держав-членів вимагається забезпечити збереження персональних даних «у формі, що дозволяє встановлювати особу суб'єктів персональних даних не довше, ніж це необхідно з метою, заради якої дані були зібрані чи заради якої вони надалі обробляються». Тому персональні дані повинні бути видалені, якщо цієї мети вже немає.

У справі *«С. і Марпер»* ЄСПЛ дійшов висновку, що основні принципи відповідних документів Ради Європи, законодавство і практика інших Договірних Сторін вимагають, щоб збереження даних було пропорційним меті збирання та обмежувалось у часі, особливо у секторі діяльності поліції.[123]

Проте збереження персональних даних протягом обмеженого періоду стосується тільки даних, які зберігаються у формі, що дозволяє встановити суб'єктів персональних даних. Законності процедури збереження персональних даних, які вже більше не потрібні, можна досягти шляхом їх знеособлення або псевдонімізації.

Збереження персональних даних з метою історичного, статистичного чи наукового використання є відкритим винятком з принципу обмеженого збе-

123 Рішення ЄСПЛ у справі «С. та Марпер проти Сполученого Королівства» (*S. and Marper v. the United Kingdom*), №№ 30562/04 та 30566/04 від 4 грудня 2008 р.; див. також, наприклад: рішення ЄСПЛ у справі «М.М. проти Сполученого Королівства» (*M.M. v. the United Kingdom*), № 24029/07 від 13 листопада 2012 р.

реження даних у Директиві про захист персональних даних.[124] Проте, таке подальше збереження та використання персональних даних має супроводжуватися встановленими законом спеціальними гарантіями.

3.4. Принцип ретельності обробки

Ключові моменти

- Ретельність обробки означає її прозорість, особливо, по відношенню до суб'єктів персональних даних.
- Володільці персональних даних повинні інформувати суб'єктів персональних даних до початку процедури обробки, принаймні, про мету, про особу володільця та про його адресу.
- Процедуру обробки персональних даних не може бути засекречено та утаємничено, якщо інше не встановлено законом.
- Суб'єкти персональних даних мають право на доступ до своїх даних, де б вони не оброблювалися.

Принцип ретельності обробки регулює, передусім, взаємовідносини між володільцем та суб'єктом персональних даних.

3.4.1. Прозорість

Цей принцип зобов'язує володільця персональних даних постійно інформувати суб'єктів персональних даних про те, як використовуються їхні персональні дані.

Приклад: у справі *«Хараламбі проти Румунії»*[125] заявник звернувся з проханням про надання йому доступу до досьє, яке було заведено на нього секретною службою, проте його прохання було задоволено лише через п'ять років. ЄСПЛ ще раз підтвердив, що особи, на які органами державної влади було заведено досьє, життєво зацікавлені у можливості отримати до них доступ. Влада була зобов'язана забезпечити ефективною процедурою до-

124 Директива про захист персональних даних, ст. 6 (1) (e).

125 Рішення ЄСПЛ у справі *«Хараламбі проти Румунії» (Haralambie v. Romania),* № 21737/03 від 27 жовтня 2009 р.

ступ до такої інформації. ЄСПЛ визнав, що ані обсяг переданого досьє, ані недоліки архівної системи не виправдовують п'ятирічної затримки у задоволенні прохання заявника про доступ до його досьє. Влада не забезпечила заявника ефективною та доступною процедурою, яка б уможливила доступ до його персональних документів у розумні строки. Суд дійшов висновку, що було порушено статтю 8 ЄКПЛ. Суб'єкти персональних даних повинні бути поінформовані про операції з обробки у легкий та доступний спосіб, який гарантує, що вони розуміють, що відбуватиметься з їхніми персональними даними. Суб'єкт персональних даних має право бути поінформованим володільцем, якщо є запит щодо того, чи обробляються його або її дані, і, якщо так, то які саме.

3.4.2. Формування довіри

Володільці персональних даних повинні документально доводити суб'єктам персональних даних і громадськості, що вони обробляють персональні дані в законний і прозорий спосіб. Операції з обробки не повинні здійснюватися у таємниці і не повинні мати непередбачувані негативні наслідки. Володільці персональних даних повинні пересвідчуватися у тому, що клієнти або громадяни поінформовані про використання своїх персональних даних. Окрім того, володільці персональних даних, наскільки це можливо, повинні діяти у спосіб, який точно відповідає побажанням суб'єкта персональних даних, особливо у випадку, коли його або її згода є правовими підставами для здійснення обробки.

Приклад: у справі *«K.X. та інші проти Словаччини»*[126] заявниками були вісім жінок ромського походження, які під час вагітності та пологів проходили лікування у двох лікарнях у східній Словаччині. Згодом жодна з них, незважаючи на неодноразові спроби, не змогла завагітніти знову. Національні суди зобов'язали лікарні проконсультувати заявниць та їхніх представників і надати рукописні витяги медичних записів, але відхилили їхнє прохання надати дозвіл зробити фотокопії документів, нібито з метою запобігання їхнього неналежного використання. Позитивні зобов'язання держав за статтею 8 ЄКПЛ неодмінно передбачають зобов'язання надавати суб'єкту персональних даних можливості доступу до копій його або її даних. Саме держава мала визначити механізм здійснення копіювання

126 Рішення ЄСПЛ у справі *«K.X. та інші проти Словаччини» (K.H. and Others v. Slovakia)*, № 32881/04 від 28 квітня 2009 р.

персональних даних або в разі необхідності пред'явити переконливі причини для відмови. У справі заявниць національні суди обґрунтували заборону на копіювання медичних документів, здебільшого, необхідністю захисту відповідної інформації від зловживання. Однак, ЄСПЛ не зміг зрозуміти, яким чином заявниці, які у будь-якому випадку мали б отримати доступ до усіх своїх медичних документів, зловживали б інформацією про себе. Окрім того, ризику такого зловживання можна було б запобігти за допомогою інших, аніж відмова в копіюванні документів заявниць, засобів, наприклад, шляхом обмеження кола осіб, які мають право на доступ до документів. Держава не пред'явила існування переконливих причин для відмови заявницям у ефективному доступі до інформації, яка стосувалась їхнього здоров'я. Суд дійшов висновку, що було порушено статтю 8.

Що стосується сфери надання інтернет-послуг, характеристики систем обробки персональних даних повинні забезпечувати суб'єктів персональних даних можливістю чіткого розуміння, що відбуватиметься з їхніми персональними даними.

Ретельність обробки персональних даних також означає, що володільці мають бути готові вийти за межі своїх обов'язкових мінімальних законних вимог щодо обслуговування суб'єкта персональних даних, якщо того вимагатимуть законні інтереси суб'єкта персональних даних.

3.5. Принцип підзвітності

Ключові моменти

- Підзвітність вимагає від володільців активного здійснення заходів щодо підтримки та захисту персональних даних під час їхньої обробки.
- Володільці відповідають за відповідність операцій з обробки законодавству про захист персональних даних.
- Володільці мають бути готові у будь-який час продемонструвати відповідність нормам закону про захист персональних даних суб'єктам персональних даних, громадськості та наглядовим органам.

Організація економічного співробітництва та розвитку (ОЕСР) прийняла в 2013 році «Керівні принципи приватності», у яких підкреслено важливу роль володільців щодо практичного втілення захисту персональних даних. У керів-

них принципах удосконалено принцип підзвітності: «володілець персональних даних повинен нести відповідальність за дотримання заходів, що забезпечують втілення [матеріальне] зазначених вище принципів». [127]

Якщо Конвенція 108 не містить жодних посилань щодо підзвітності володільців, по суті, залишаючи це питання на розсуд національного законодавства, у статті 6 (2) Директиви про захист персональних даних йдеться про те, що забезпечення дотримання принципів якості обробки даних пункту 1 покладається на володільця.

Приклад: прикладом нормативного акту, у якому наголошено на принципі підзвітності, є доповнена у 2009 році[128] Директива «Про секретність та електронні комунікації» (2002/58/ЄС). Положення доповненої статті 4 Директиви зобов'язують реалізовувати політику безпеки, а саме, «гарантувати політику безпеки щодо обробки персональних даних». Таким чином, наскільки це стосується норм безпеки цієї директиви, законодавець вирішив, що існує необхідність внести положення про обов'язкову вимогу мати і гарантувати політику безпеки.

Відповідно до висновку робочої групи «Стаття 29» [129] підзвітність полягає у зобов'язанні володільця:

- вживати заходів, які б за звичайних обставин гарантували дотримання норм захисту даних у контексті операцій з обробки; та
- мати готові документи, які підтверджують суб'єктам персональних даних та органам нагляду, які саме заходи було вжито для досягнення відповідності нормам захисту персональних даних.

Отже, принцип підзвітності вимагає від володільця активно демонструвати відповідність нормам, а не просто чекати суб'єктів персональних даних або наглядових органів, які б вказали на недоліки.

127 OECP (2013), Керівні принципи, що регулюють захист приватності і транскордонні потоки персональних даних, ст. 14.

128 Директива 2009/136/ЄС Європейського парламенту та Ради від 25 листопада 2009 р., яка доповнює Директиву 2002/22/ЄС «Про універсальні послуги та права користувачів стосовно електронних мереж зв'язку та послуг, Директива 2002/58/ЄС «Про обробку персональних даних та захист таємниці у секторі електронних комунікацій» та Регламент (ЄС) № 2006/2004 «Про співробітництво між національними органами влади, відповідальними за дотримання законів про захист прав споживачів», OJ 2009 L 337, с. 11.

129 Робоча група «Стаття 29» , *Висновок 3/2010 про принцип підзвітності*, РГ 173, Брюссель, 13 липня 2010 р.

4 Правила європейського права про захист персональних даних

ЄС	питання, що висвітлюються	РЄ
Правила законної обробки нечутливих даних		
Директива про захист персональних даних, стаття 7 (a)	**згода**	Рекомендація щодо профайлінгу, статті 3.4 (b) та 3.6
Директива про захист персональних даних, стаття 7 (b)	**відносини до укладення контракту**	Рекомендація щодо профайлінгу, стаття 3.4 (b)
Директива про захист персональних даних 7 (c)	**правові зобов'язання володільця персональних даних**	Рекомендація щодо профайлінгу, стаття 3.4 (a)
Директива про захист персональних даних 7 (d)	**життєво важливі інтереси суб'єкта персональних даних**	Рекомендація щодо профайлінгу, стаття 3.4 (b)
Директива про захист персональних даних, стаття 7 (e) та стаття 8 (4) СЄС, C-524/06, *«Губер проти Німеччини» (Huber v. Germany)*, від 16 грудня 2008 р.	**суспільний інтерес та виконання офіційних повноважень**	Рекомендація щодо профайлінгу, стаття 3.4 (b)

ЄС	питання, що висвітлюються	РЄ
Директива про захист персональних даних, стаття 7 (f), стаття 8 (2) та 8 (3) СЄС, Об'єднані справи C-468/10 та C-469/10, *«Національна асоціація кредитних фінансових установ (ASNEF) і Федерація електронної комерції і прямого маркетингу (FECEMD) проти Державної адміністрації» Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, (1) (e) від 24 листопада 2011 р.	**законні інтереси інших осіб**	Рекомендація щодо профайлінгу, стаття 3.4 (b)
Правила законної обробки чутливих даних		
Директива про захист персональних даних, стаття 8 (1)	**загальна заборона на обробку**	Конвенція 108, стаття 6
Директива про захист персональних даних, стаття 8 (2)–(4)	**винятки із загальної заборони на обробку**	Конвенція 108, стаття 6
Директива про захист персональних даних, стаття 8 (5)	**обробка даних, що стосуються обвинувачення у (кримінальних) справах**	Конвенція 108, стаття 6
Директива про захист персональних даних, стаття 8 (7)	**обробка ідентифікаційних кодів**	
Безпекові правила процесу обробки		
Директива про захист персональних даних, стаття 17	**зобов'язання щодо забезпечення безпеки обробки**	Конвенція 108, стаття 7 Рішення ЄСПЛ у справі *«I проти Фінляндії» (I. v. Finland)*, № 20511/03 від 17 липня 2008 р.

ЄС	питання, що висвітлюються	РЄ
Директива про секретність і електронні комунікації, стаття 4 (2)	**повідомлення про порушення безпеки даних**	
Директива про захист персональних даних, стаття 16	**зобов'язання щодо конфіденційності**	
Правила прозорості обробки		
	загальна прозорість	Конвенція 108, стаття 8 (a)
Директива про захист персональних даних, статті 10 та 11	**інформація**	Конвенція 108, стаття 8 (a)
Директива про захист персональних даних, статті 10 та 11	**винятки з обов'язку надавати інформацію**	Конвенція 108, стаття 9
Директива про захист персональних даних, статті 18 та 19	**сповіщення**	Рекомендація щодо профайлінгу, стаття 9.2
Правила дотримання відповідності		
Директива про захист персональних даних, стаття 20	**попередня перевірка**	
Директива про захист персональних даних, стаття 18 (2)	**посадові особи з захисту персональних даних**	Рекомендація щодо профайлінгу, стаття 8.3
Директива про захист персональних даних, стаття 27	**кодекси поведінки**	

Принципи повинні носити загальний характер. Їх застосування у конкретних ситуаціях залишає певне поле розсуду для тлумачення та вибору засобів. **Право РЄ** уповноважує Сторони Конвенції 108 роз'яснювати межі тлумачення у національному законодавстві. У **праві ЄС** ситуація інша: було визнано, що для того, щоб запровадити захист персональних даних на національному рівні, необхідно визначити більш конкретні норми на рівні ЄС, відповідно до яких гармонізувати національні закони держав-членів про захист персональних даних. У викладених у статті 6 Директиви про захист персональних даних принципах передбачено ряд конкретних норм, які належним чином необхідно реалізовувати в національному законодавстві. Тому викладені далі зауваження щодо конкретних правил захисту персональних даних на європейському рівні застосовні, переважно, в правовій системі ЄС.

4.1. Правила законної обробки

Ключові моменти

- Персональні дані обробляються законно, якщо:
  - обробка здійснюється на основі згоди суб'єкта персональних даних; або
  - життєво важливі інтереси суб'єктів персональних даних вимагають обробки їхніх даних; або
  - законні інтереси інших є причиною обробки персональних даних, але доти, доки їх не пересилюють інтереси захисту основоположних прав суб'єктів персональних даних.
- Законна обробка чутливих даних є предметом спеціальних, суворіших вимог.

У Директиві про захист персональних даних є дві різні системи норм, які регулюють процедуру законної обробки персональних даних: одна – для нечутливих даних у статті 7, інша – для чутливих у статті 8.

4.1.1. Законна обробка нечутливих даних

У главі II «Загальні правила законності обробки персональних даних» Директиви 95/46 передбачено, що з урахуванням визначених у статті 13 винятків увесь процес обробки персональних даних повинен відповідати, насамперед, принципам якості персональних даних, викладеним у статті 6 Директиви про захист персональних даних і, по-друге, одному із критеріїв законності обробки персональних даних, передбачених у статті 7.[130] Це пояснює випадки, які узаконюють обробку нечутливих персональних даних.

130 СЄС, об'єднані справи C-465/00, C-138/01 та C-139/01, *«Рахункова палата проти австрійської телерадіокомпанії «Österreichischer Rundfunk» та інших і Нойком та Лауерманн проти австрійської телерадіокомпанії «Österreichischer Rundfunk»* (*Rechnungshof v. Österreichischer Rundfunkand Others and Neukomm and Lauermann v. Österreichischer Rundfunk*) від 20 травня 2003 р., п. 65; СЄС, C-524/06, *«Губер проти Німеччини» (Huber v. Germany)* від 16 грудня 2008 р., п. 48; СЄС, об'єднані справи C-468/10 та C-469/10, *«Національна асоціація кредитних фінансових установ (ASNEF) і Федерація електронної комерції і прямого маркетингу (FECEMD) проти Державної адміністрації»* (*Asociacion Nacional de Establecimientos Financieros de Credito (ASNEF) and Federacion de Comercio Electronico y Marketing Directo (FECEMD) v. Administracion del Estado)* від 24 листопада 2011 р., п. 26.

Згода

Що стосується **права РЄ**, про згоду не йдеться ні у статті 8 ЄКПЛ, ні в Конвенції 108. Попри це згода згадується у судовій практиці ЄСПЛ і декількох рекомендаціях РЄ. Що стосується **права ЄС**, згоду як основу законної обробки персональних даних чітко зафіксовано в статті 7 (a) Директиви про захист персональних даних, а також відображено у статті 8 Хартії.

Взаємовідносини за контрактом

Іншою умовою для здійснення законної обробки персональних даних в рамках **права ЄС**, яку визначено у статті 7 (b) Директиви про захист персональних даних, є: якщо вона «необхідна для виконання контракту, стороною якого є суб'єкт персональних даних». Це положення також поширюється на відносини до укладення контракту. Наприклад, коли сторона має намір укласти контракт, але ще не зробила цього, ймовірно, через те, що має здійснити певну перевірку. Якщо одна зі сторін повинна для цієї мети обробити дані, така обробка є законною доти, доки вона «необхідна для вжиття заходів на запит суб'єкта персональних даних до укладення контракту».

Що стосується права РЄ, «захист прав і свобод інших осіб» як підстава для законного втручання у право на захист персональних даних згадується у статті 8 (2) ЄКПЛ.

Правові зобов'язання володільця

У праві ЄС відкрито згадується ще один критерій законності обробки персональних даних, а саме: якщо обробка «необхідна для задоволення або захисту правової вимоги» (стаття 7 (c) Директиви про захист персональних даних). Це положення стосується володільців, які працюють у приватному секторі; правові зобов'язання володільців, які діють у державному секторі, підпадають під дію статті 7 (e) Директиви. Існують випадки, коли володільці, які працюють у приватному секторі, зобов'язані законом обробляти дані інших осіб, наприклад, лікарів, а лікарні зобов'язані відповідно до закону зберігати інформацію про лікування хворих протягом декількох років; роботодавці повинні обробляти персональні дані своїх працівників з метою соціального забезпечення та оподаткування; у бізнесі обробляють дані про своїх клієнтів з метою оподаткування.

У контексті обов'язкової передачі авіакомпаніями даних про пасажирів органам імміграційного контролю іноземних держав постало питання про те, чи

можуть правові зобов'язання в рамках законодавства іноземної держави бути законними підставами для здійснення обробки персональних даних за правом ЄС (це питання обговорюється більш детально в розділі 6.2.).

Правові зобов'язання володільця є основою законної обробки персональних даних також у **праві РЄ**. Як вже зазначалося раніше, правові зобов'язання володільця персональних даних в приватному секторі є лише одним окремим випадком законних інтересів третіх осіб, про що йдеться у статті 8 (2) ЄКПЛ. Тому наведений вище приклад також має відношення до права РЄ.

Життєво важливі інтереси суб'єкта персональних даних

У **праві ЄС** у статті 7 (d) Директиви про захист персональних даних передбачено, що обробка персональних даних є законною, якщо вона «необхідна для захисту життєво важливих інтересів суб'єкта персональних даних». Такі інтереси, які тісно пов'язані з виживанням суб'єкта даних, можуть стати основою для законного використання персональних даних про стан здоров'я або, наприклад, інформації про зниклих осіб.

У **праві РЄ** у статті 8 ЄКПЛ про життєво важливі інтереси суб'єкта персональних даних як причини законного втручання у право на захист даних не йдеться. Проте у деяких рекомендаціях РЄ, які доповнюють Конвенцію 108 у конкретних сферах, життєво важливі інтереси суб'єкта персональних даних прямо визначено як підстави для законної обробки.[131] Вважається, що життєво важливі інтереси суб'єкта персональних даних чітко прослідковуються серед причин, які обґрунтовують обробку персональних даних: захист основоположних прав ніколи не повинен ставити під загрозу життєво важливі інтереси особи, яку захищають.

Суспільний інтерес та виконання офіційних повноважень

Беручи до уваги, що існує багато способів організації суспільної діяльності, у статті 7 (e) Директиви про захист персональних даних передбачено, що персональні дані можуть бути законно оброблені, якщо обробка «необхідна для виконання завдання, здійснюваного в суспільних інтересах, чи при виконанні офіційних повноважень, якими наділений володілець або третя особа, якій надаються дані [...]».[132]

131 Профайлінг Рекомендація, ст. 3.4 (b).

132 Див. Директиву про захист персональних даних, п. 32 преамбули.

Приклад: у справі *«Губер проти Німеччини»*[133] громадянин Австрії, що проживає у Німеччині, звернувся до Федерального відомства з питань міграції та біженців з проханням видалити його дані з Центрального реєстру іноземців (AZR). Цей реєстр, у якому містяться персональні дані громадян держав – членів ЄС, що проживають у Німеччині більше трьох місяців і не є її громадянами, використовується для цілей статистики, а також для цілей діяльності правоохоронних та судових органів під час розслідування та обвинувачення у злочинній діяльності або тій, яка загрожує громадській безпеці. Суд звернувся за роз'ясненням, чи відповідає здійснювана процедура обробки персональних даних у такому реєстрі, як Центральний реєстр іноземців, до якого також мають доступ інші державні органи, праву ЄС, враховуючи, що для громадян Німеччини такого реєстру немає.

СЄС постановив, по-перше, що відповідно до статті 7 (e) Директиви, персональні дані можуть законно оброблятися тільки за умови, якщо це необхідно для виконання завдання, здійснюваного в суспільних інтересах чи при виконанні офіційних повноважень.

На думку Суду, «враховуючи ціль забезпечення однакового захисту у всіх державах-членах, передбачене у статті 7 (e) Директиви 95/46 поняття необхідності [...] не може бути різним у державах-членах. Тому виходить, що те, що ми розглядаємо, це – поняття, яке має своє незалежне значення у праві Співтовариств і повинне тлумачитись у спосіб, який повністю відображає закладену в статті 1 (1) ціль цієї Директиви.[134]

Суд зазначає, що здійснення права громадянина держави – члена ЄС щодо вільного пересування по території держави-члена, громадянином якої він чи вона не є, не є абсолютним і може бути предметом обмежень і умов, встановлених Договором та прийнятими на його виконання заходами. Отже, навіть, якщо у держави-члена є законні підстави для використання такого реєстру як AZR для допомоги органам, що відповідають за застосування законодавства про право на проживання, у такому реєстрі не повинно бути іншої інформації, окрім тієї, яка необхідна для досягнення цієї конкретної мети. Суд доходить висновку, що така система обробки персональних даних відповідає праву ЄС за умови, що містить

133 СЄС, C-524/06, *«Губер проти Німеччини» (Huber v. Germany)* від 16 грудня 2008 р.

134 Там само, п. 52.

тільки дані, які необхідні для використання такого закону, а централізований характер системи сприяє ефективнішому його застосуванню. Національний суд має встановити, чи є ці умови задовільними в даному конкретному випадку. Якщо ні, то збереження і обробка персональних даних в такому реєстрі, як AZR для статистичних цілей не може, за будь-яких підстав, вважатися необхідною у розумінні статті 7 (e) Директиви 95/46 /ЕС.[135]

Нарешті, стосовно питання використання даних реєстру для цілей боротьби зі злочинністю, Суд вважає, що до таких цілей «обов'язково включено мету щодо переслідування за скоєння злочинів та правопорушень, що не залежить від громадянства того, хто їх скоїв». У цьому реєстрі немає персональних даних про громадян цієї держави-члена, і це розходження у поводженні є дискримінацією, заборону якої передбачено у статті 18 ДфЄС. Отже, у тлумаченні Суду це положення «виключає створення державою-членом для цілей боротьби зі злочинністю системи обробки персональних даних для громадян держав-членів ЄС, які не є громадянами цієї держави-члена».[136]

Використання персональних даних державними органами, які діють в публічній сфері, також підпадає під дію положень статті 8 ЄКПЛ.

Законні інтереси, які переслідує володілець або третя особа

Законний інтерес є не лише у суб'єктів персональних даних. У статті 7 (f) Директиви про захист персональних даних зазначено, що персональні дані можуть законно оброблятися, якщо це «необхідно для законних інтересів, переслідуваних володільцем чи третьою особою або особами, для яких надаються дані, крім випадків, коли над такими інтересами переважають інтереси основоположних прав і свобод суб'єкта персональних даних, що вимагають захисту [...]».

СЄС виніс рішення щодо статті 7 (f) Директиви у такій справі:

Приклад: у справі «*Національна асоціація кредитних фінансових установ (ASNEF) і Федерація електронної комерції і прямого маркетингу*

135 Там само, п. 54, 58, 59, 66–68.

136 Там само, п. 78 та 81.

(FECEMD)»[137] СЄС надав роз'яснення, що національне законодавство не має права доповнювати положення статті 7 (f) Директиви додатковими умовами законності обробки даних. Це стосується ситуації із законом Іспанії «Про захист персональних даних», який містив положення, згідно з яким будь-які фізичні особи могли заявляти про свої законні інтереси на обробку персональних даних лише за умови оприлюднення інформації у державних джерелах.

Суд, передусім, зазначив, що метою Директиви 95/46/ЕС є забезпечення адекватного рівня захисту прав і свобод осіб при здійсненні обробки персональних даних в усіх державах-членах. Результатом гармонізації національних законів, що діють у цій сфері, не повинне бути зниження наявного у них рівня захисту. Натомість її метою має бути забезпечення високого рівня захисту персональних даних у ЄС.[138] Отже, СЄС постановив, що «саме метою забезпечення адекватного рівня захисту у всіх державах-членах обумовлено викладення у статті 7 Директиви 95/46 вичерпного і обмежувального переліку умов, за яких обробка персональних даних може вважатися законною». Окрім того, «держави-члени не можуть доповнювати статтю 7 Директиви 95/46 новими принципами законності обробки персональних даних або додавати вимоги, якими може бути змінено сферу дії одного з шести принципів, передбачених у статті 7».[139] Суд визнав, що у зв'язку з необхідністю дотримання балансу інтересів, визнаного у статті 7 (f) Директиви 95/46/ЄС, «можна взяти до уваги той факт, що серйозність порушення основоположних прав суб'єкта персональних даних у результаті обробки може варіюватися залежно від наявності чи відсутності цих даних у державних джерелах».

Більше того, «положення статті 7 (f) Директиви чітко і повно застерігають державу-члена від можливості здійснювати обробку певних катего-

137 СЄС, об'єднані справи C-468/10 та C-469/10, *«Національна асоціація кредитних фінансових установ (ASNEF) і Федерація електронної комерції і прямого маркетингу (FECEMD) проти Державної адміністрації» Asociacion Nacional de Establecimientos Financieros deCredito (ASNEF) and Federacion de Comercio Electronico y Marketing Directo (FECEMD) v. Administracion del Estado* від 24 листопада 2011 р.

138 Там само, п. 28. див. Директиву про захист персональних даних, п.8 та 10 преамбули.

139 СЄС, об'єднані справи C-468/10 та C-469/10, *«Національна асоціація кредитних фінансових установ (ASNEF) і Федерація електронної комерції і прямого маркетингу (FECEMD) проти Державної адміністрації» Asociacion Nacional de Establecimientos Financieros deCredito (ASNEF) and Federacion de Comercio Electronico y Marketing Directo (FECEMD) v. Administracion del Estado* від 24 листопада 2011 р., пп. 30 та 32.

рій персональних даних без забезпечення балансу між конфронтуючими правами та законними інтересами в кожному конкретному випадку».

У світлі цих міркувань Суд дійшов висновку, що «положення статті 7 (f) Директиви 95/46 слід тлумачити як національні норми застереження, які, за відсутності згоди суб'єкта персональних даних і з метою надання дозволу на здійснення обробки цих персональних даних суб'єкта персональних даних, необхідних для досягнення законних інтересів володільця персональних даних або третьої сторони або сторін, яким ці дані розкриваються, вимагають дотримання не тільки основоположних прав і свобод суб'єкта персональних даних, а й також оприлюднення даних у державних джерелах, тим самим категорично і повно виключає факт неможливості оприлюднення будь-якої обробки персональних даних у таких джерелах.»[140]

Подібні формулювання можна знайти в рекомендаціях РЄ. Рекомендація щодо профайлінгу визнає здійснення обробки персональних даних для законних цілей профайлінгу, якщо необхідно – для законних інтересів інших осіб, «за винятком, коли над такими інтересами переважають основоположні права і свободи суб'єктів персональних даних». [141]

4.1.2. Законна обробка чутливих даних

За правом РЄ повноваження передбачати відповідний захист у зв'язку з використанням персональних даних залишено за національними законодавчими органами, в той час як за **правом ЄС** у статті 8 Директиви про захист персональних даних передбачено детальний порядок обробки категорії даних, які вказують на расове чи етнічне походження, політичні погляди, релігійні чи філософські переконання, профспілкове членство, стан здоров'я чи статеве життя особи. Обробку чутливих даних, в принципі, заборонено.[142] Проте у статті 8 (2) і (3) можна знайти вичерпний перелік винятків із цієї заборони. Ці винятки включають пряму згоду суб'єкта персональних даних, життєво важливі інтереси суб'єкта персональних даних, законні інтереси інших осіб та суспільні інтереси.

140 Там само, пп. 40, 44, 48 та 49.

141 Рекомендація щодо профайлінгу, ст. 3.4 (b).

142 Директива про захист персональних даних, ст. 8 (1).

На відміну від обробки нечутливих даних, взаємовідносини з суб'єктом персональних даних за контрактом не вважаються загальною підставою для здійснення законної обробки чутливих даних. Тому, якщо необхідно здійснити обробку чутливих даних у контексті контракту з суб'єктом персональних даних, для цього, окрім згоди на укладення контракту, потрібна окрема пряма згода суб'єкта персональних даних. Окрім того, безпосередній запит суб'єкта персональних даних на отримання товару або послуг, які обов'язково розкривають чутливі дані, слід вважати прямою згодою.

Приклад: Якщо авіапасажир під час бронювання квитків зазначає про необхідність надати йому або їй інвалідний візок і кошерну їжу, авіакомпанія може використовувати ці дані, навіть без надання пасажиром додаткової згоди на використання його/її даних, які розкривають інформацію про його/її стан здоров'я та релігійні переконання.

Пряма згода суб'єкта персональних даних

Першою умовою здійснення законної обробки будь-яких персональних даних, незалежно від того, чи є вони нечутливими або чутливими, має бути згода суб'єкта персональних даних. У випадку з чутливими даними така згода має бути прямою. Попри це, у національному законодавстві може бути передбачено, що згода на використання чутливих даних не є достатньою правовою підставою для надання дозволу на їх обробку,[143] коли, наприклад, у надзвичайних ситуаціях, обробка здійснюється з незвичайними для суб'єкта персональних даних ризиками.

В одному окремому випадку навіть невисловлену прямо згоду було визнано правовим підґрунтям для здійснення обробки чутливих даних: стаття 8 (2) (e) Директиви передбачає, що здійснення обробки не заборонено, якщо це стосується даних, які явно оприлюднені суб'єктом персональних даних. Це положення, вочевидь, передбачає, що дії суб'єкта персональних даних, спрямовані на оприлюднення його або її даних, мають тлумачитись як такі, що наводять на думку про його або її згоду на використання таких даних.

143 Там само, ст. 8 (2) (a).

Життєво важливі інтереси суб'єкта персональних даних

Як і у випадку з нечутливими персональними даними, чутливі дані можна обробляти, якщо обробка необхідна для захисту життєво важливих інтересів суб'єкта персональних даних.[144]

Для того, щоб така обробка чутливих даних відбувалась з дотриманням законних вимог, необхідно щоб було неможливо поставити питання суб'єкту персональних даних для отримання згоди через втрату ним або нею свідомості або його/її відсутність та неможливість встановити з такою особою зв'язок.

Законні інтереси інших осіб

Як і у випадку з нечутливими даними законні інтереси інших осіб можуть бути підставою для здійснення обробки чутливих даних. До чутливих даних згідно ст. 8 (2) Директиви про захист персональних даних це має відношення у таких випадках:

- коли обробка необхідна для захисту життєво важливих інтересів іншої особи[145], коли суб'єкт персональних даних не може дати згоду через свою недієздатність чи неправоздатність;
- коли обробка чутливих даних використовується в сфері трудового права, як, наприклад обробка даних про здоров'я у контексті особливо небезпечної роботи, або про релігійні переконання, наприклад, у контексті релігійних свят;[146]
- коли фундації, асоціації чи будь-які інші неприбуткові організації у політичних, філософських, релігійних чи профспілкових цілях здійснюють обробку даних своїх членів, спонсорів або інших зацікавлених сторін (такі дані є чутливими, тому що, ймовірно, розкривають релігійні чи політичні переконання цих осіб);[147]
- чутливі дані використовуються у контексті судового провадження або адміністративним органом для порушення, виконання або захисту судового позову.[148]

144 Там само, ст. 8 (2) (c).

145 Там само.

146 Там само, ст. 8 (2) (b).

147 Там само, ст. 8 (2) (d).

148 Там само, ст. 8 (2) (e).

- Окрім того, відповідно до ст. 8 (3) Директиви про захист персональних даних, коли медичні працівники використовують дані про здоров'я з метою медичного обстеження та лікування, керівництво цих служб також відносять до таких винятків. Окремою гарантією є те, що особи визнаються «працівниками, які надають медичні послуги» лише тоді, коли вони беруть на себе професійне зобов'язання зберігати медичну таємницю.

Суспільний інтерес

Окрім того, відповідно до статті 8 (4) Директиви про захист персональних даних, держави-члени можуть вносити додаткові цілі, заради яких чутливі дані оброблюються доти, доки:

- обробка персональних даних здійснюється задля значного суспільного інтересу; та
- додаткові цілі передбачено у національному законодавстві або у рішенні наглядового органу; та
- національне законодавство або рішення наглядового органу містять необхідні гарантії ефективного захисту інтересів суб'єктів персональних даних.[149]

Яскравим прикладом є електронні медичні картотеки, які збираються запровадити в багатьох державах-членах. Такі системи роблять можливим широкомасштабний та загальнонаціональний доступ до зібраної під час лікування особи медичної інформації з боку інших медичних працівників.

Робоча група «Стаття 29» дійшла висновку, що запровадження таких картотек не може бути здійснене в рамках існуючих правових норм статті 8 (3) Директиви про захист персональних даних щодо обробки медичних даних. Якщо припустити, що існування таких електронних медичних картотек створює значний суспільний інтерес, тоді вони регулюватимуться положеннями статті 8 (4) Директиви щодо необхідності існування чіткого правового обґрунтування для їх заснування та гарантій їх безпечного функціонування. [150]

149 Там само, ст. 8 (4)

150 Робоча група «Стаття 29» (2007), Робочий документ щодо обробки персональних даних у зв'язку з електронними медичними картками *(EHR)*, РГ 131, Брюссель, 15 лютого 2007 р.

4.2. Правила стосовно безпеки обробки

Ключові моменти

- Правила стосовно безпеки обробки накладають на володільця та розпорядника зобов'язання здійснювати відповідні технічні й організаційні заходи для захисту від несанкціонованого втручання в операції з обробки персональних даних.
- Необхідний рівень безпеки персональних даних визначається:
  - наявністю на ринку засобів забезпечення безпеки для будь-якого типу обробки; та
  - вартістю;
  - чутливістю оброблених даних.
- Обробка персональних даних в повній безпеці також гарантується загальним зобов'язанням, яке накладається на всіх – і володільців, і розпорядників – слідкувати за забезпеченням конфіденційності персональних даних

Отже, зобов'язання володільців або розпорядників застосовувати адекватні заходи для забезпечення безпеки даних закладено і **у праві РЄ про захист персональних даних**, і у **праві ЄС**.

4.2.1. Елементи безпеки даних

Як передбачено відповідними положеннями **права ЄС:**

> *«Держави-члени передбачають, що володілець повинен здійснювати відповідні технічні й організаційні заходи для захисту персональних даних від випадкового або незаконного знищення чи випадкової втрати, зміни, несанкціонованого розкриття чи доступу, зокрема, якщо обробка включає передачу даних через мережу, і від усіх інших незаконних форм обробки».*[151]

Подібне положення є у **праві РЄ:**

> *«Для захисту персональних даних, що зберігаються у файлах даних для автоматизованої обробки, вживають відповідних заходів безпеки,*

151 Директива про захист персональних даних, ст. 17 (1).

спрямованих на запобігання випадковому чи несанкціонованому знищенню або випадковій втраті, а також на запобігання несанкціонованим доступу, зміні або поширенню».[152]

У сфері безпеки процесу обробки існує багато промислових, національних та міжнародних стандартів. Європейський знак конфіденційності (EuroPriSe), наприклад, є проектом ЄС «Транс'європейські телекомунікаційні мережі» (Eten), у рамках якого вивчалися можливості сертифікації продукції, особливо програмного забезпечення, відповідно до європейських вимог захисту персональних даних. Європейське агентство з мережевої та інформаційної безпеки (ENISA) було створено з метою посилення здатності ЄС, держав-членів ЄС та бізнес-спільноти запобігати, усувати та реагувати на проблеми мережевої та інформаційної безпеки.[153] Європейське агентство з мережевої та інформаційної безпеки регулярно оприлюднює аналіз поточного стану безпеки загроз та рекомендації щодо їх усунення.

Безпека даних досягається не тільки за рахунок встановлення правильного обладнання: апаратного та програмного забезпечення. Для її забезпечення необхідні внутрішні правила. Ці правила, в ідеалі, охоплюють такі питання:

- регулярне забезпечення усіх працівників інформацією про вимоги безпеки та про їхні зобов'язання у рамках законодавства про захист персональних даних, зокрема, у зв'язку з вимогами конфіденційності;
- чіткий розподіл обов'язків та чіткий виклад повноважень у сфері обробки персональних даних, особливо у сфері прийняття рішень щодо здійснення обробки даних та їх передачі третім особам;
- використання персональних даних лише за вказівкою уповноваженої особи чи згідно закладених загальних правил;
- захист доступу до місцезнаходження апаратного і програмного забезпечення володільця або розпорядника, включаючи здійснення перевірки авторизації доступу;
- забезпечення надання задокументованого належним чином дозволу на доступ до персональних даних уповноваженою на це особою;

152 Конвенція 108, ст. 7.

153 Регламент (ЄС) № 460/2004 Європейського парламенту та Ради від 10 березня 2004 р. щодо створення Європейського агентства з мережевої та інформаційної безпеки, OJ 2004 L 77.

- електронна база автоматизованої системи протоколів доступу до персональних даних та регулярна перевірка таких протоколів внутрішнім органом нагляду;
- ретельне документування інших неавтоматизованих форм розкриття інформації про доступ до персональних даних, яке б доводило відсутність незаконної передачі даних.

Проведення відповідних тренінгів для співробітників та їх навчання з питань безпеки персональних даних також є важливою складовою ефективних заходів безпеки. Необхідно також запровадити процедуру інспекції для забезпечення реалізації відповідних заходів на практиці, а не тільки на папері (наприклад, внутрішній або зовнішній аудит).

Заходи щодо підвищення рівня безпеки володільця або розпорядника включають такі інструменти, як захист персональних даних чиновників, навчання співробітників з питань безпеки, проведення регулярних аудитів, тестування можливостей проникнення і якості захисту.

Приклад: у справі «*I. проти Фінляндії*»[154] заявниця не змогла довести факт незаконного доступу до її медичної картки з боку інших співробітників лікарні, у якій вона працювала. Національний суд відхилив її скаргу про порушення права на захист персональних даних. ЄСПЛ дійшов висновку, що було порушено статтю 8 ЄКПЛ, оскільки реєстраційна система лікарні «була такою, яка не дозволяла заднім числом з'ясувати, хто мав доступ до медичної картки пацієнтки, оскільки система висвітлює лише п'ять останніх консультацій, інформація про які видаляється, щойно картка провертається в архів». На думку Суду, вирішальним був той факт, що реєстраційна система лікарні явно на відповідала вимогам національного законодавства, факт, якому національними судами не було надано належної уваги.

Сповіщення про порушення безпеки персональних даних

У закони про захист персональних даних деяких європейських країн було запроваджено новий інструмент для боротьби з порушеннями безпеки персональних даних: зобов'язання постачальників послуг електронного зв'язку сповіщати ймовірних жертв і наглядові органи про факти витоку даних.

154 Рішення ЄСПЛ у справі «*I. проти Фінляндії*» *(I. v. Finland)*, № 20511/03 від 17 липня 2008 р.

За правом ЄС телекомунікаційні провайдери зобов'язані це робити [155] Метою сповіщення суб'єктів персональних даних є попередження збитків: повідомлення про витоки даних та їх можливі наслідки мінімізують ризики негативного впливу на суб'єктів персональних даних. За грубу недбалість на провайдерів також можуть накласти штраф.

Встановлювати внутрішні процедури для ефективного управління та інформування про порушення безпеки слід наперед, оскільки окреслений у національному законодавстві час для інформування суб'єктів персональних даних та/або наглядового органу, зазвичай, є досить коротким.

4.2.2. Конфіденційність

У праві ЄС загальний обов'язок щодо подальшого забезпечення безпеки обробки персональних даних покладено на усіх осіб, володільців або розпорядників, які зобов'язані гарантувати конфіденційність даних.

Приклад: співробітнику страхової компанії телефонують, представляються клієнтом компанії і вимагають інформацію про його договір страхування.

Обов'язок зберігати конфіденційність про дані клієнтів вимагає від працівника дотримання, принаймні, мінімальних заходів безпеки, перш ніж надавати персональні дані. Цього можна досягти, приміром, якщо запропонувати клієнту перетелефонувати пізніше за номером, вказаним у його досьє.

У статті 16 Директиви про захист персональних даних про конфіденційність йдеться лише у контексті відносин володілець-розпорядник обробки. Питання можливості чи неможливості збереження володільцями конфіденційності персональних даних розглядається у статтях 7 та 8 Директиви у контексті того, що вони не можуть розкривати дані третім особам.

155 Див. Директиву 2002/58/ЄС Європейського парламенту та Ради від 12 липня 2002 р. «Про обробку персональних даних та захист таємниці у секторі електронних комунікацій (*Директива про секретність та електронні комунікації*), OJ 2002 L 201, ст. 4 (3), у редакції Директиви 2009/136/ЄС Європейського парламенту та Ради від 25 листопада 2009 р., яка доповнює Директиву 2002/22/ЄС «Про універсальні послуги та права користувачів стосовно електронних мереж зв'язку та послуг»; Директива 2002/58/ЄС «Про обробку персональних даних та захист таємниці у секторі електронних комунікацій» та Регламент (ЄС) № 2006/2004 «Про співробітництво між національними органами влади, відповідальними за дотримання законів про захист прав споживачів», OJ 2009 L 337.

Обов'язок зберігати конфіденційність не стосується ситуацій, коли персональні дані стають відомими особі у його або її статусі фізичної особи, а не як співробітника володільця або розпорядника. У такому випадку стаття 16 Директиви про захист персональних даних не застосовується, оскільки, фактично, використання персональних даних фізичними особами повністю виключено зі сфери дії Директиви, якщо таке використання підпадає під так звані винятки побутового характеру.[156] Винятки побутового характеру – це використання персональних даних «фізичною особою під час діяльності виключно особистого чи побутового характеру.[157] Проте з огляду на рішення СЄС у справі *«Боділ Ліндквіст»* [158] це виключення повинно тлумачитися у вужчому значенні, особливо у зв'язку з розкриттям даних. Зокрема, виключення побутового характеру не повинне поширюватися на виклад персональних даних в Інтернеті для необмеженої кількості користувачів (деталі див. у розділах 2.1.2, 2.2, 2.3.1 і 6.1)

За правом РЄ зобов'язання зберігати конфіденційність випливає із поняття «безпека даних» статті 7 Конвенції 108, у якій йдеться про безпеку персональних даних.

Для розпорядників збереження конфіденційності означає, що вони можуть використовувати надані володільцем персональні дані тільки відповідно до його інструкцій. Для співробітників володільця або розпорядника збереження конфіденційності означає, що вони використовують персональні дані тільки відповідно до наданих їхніми уповноваженими керівниками інструкцій.

У будь-якому контракті між володільцями та їхніми розпорядниками має бути передбачено зобов'язання щодо збереження конфіденційності. Окрім того, володільці або розпорядники повинні вживати конкретних заходів щодо встановлення для своїх співробітників правового обов'язку зберігати конфіденційність, що, зазвичай, досягається шляхом включення пунктів про конфіденційність до контракту про працевлаштування.

У багатьох державах – членах ЄС та державах, які є Сторонами Конвенції 108, порушення професійних обов'язків щодо збереження конфіденційності карається у кримінальному порядку.

156 Директива про захист персональних даних, ст. 3 (2) другий абзац.

157 Там само.

158 СЄС, C-101/01, *«Ліндквіст» (Lindqvist),* 6 листопада 2003 р.

4.3. Правила прозорості обробки

Ключові моменти

- Перш ніж розпочати обробку персональних даних володілець повинен, щонайменше, поінформувати суб'єктів персональних даних про особу володільця та мету здійснення обробки, за винятком випадків, коли у суб'єкта персональних даних вже є така інформація.
  - коли дані збираються від третіх осіб, обов'язок інформувати не застосовується, якщо:
  - обробка персональних даних передбачена законом; або
  - надання інформації є неможливим чи вимагає непропорційних зусиль.
- Окрім того, перш ніж розпочати обробку персональних даних володілець повинен:
  - повідомити наглядовий орган про заплановані операції з обробки; або
  - мати внутрішнє документальне обґрунтування здійснення обробки від незалежного фахівця із захисту персональних даних, якщо це передбачено у національному законодавстві.

Принцип ретельності обробки персональних даних передбачає прозорість обробки. І з цією метою у **праві РЄ** закладено норми, які дозволяють будь-кому встановлювати факт існування досьє на обробку своїх персональних даних, його цілі та відповідального володільця.[159] Право визначати методи досягнення цього залишено за національним законодавством. **Право ЄС** у цьому питанні є більш точно сформульованим, оскільки забезпечення прозорості досягається зобов'язанням володільця інформувати суб'єкта персональних даних і громадськість шляхом сповіщення.

Обидві правові системи передбачають існування у національному законодавстві винятків і обмежень з положень про обов'язок володільця дотримуватись прозорості, якщо такі обмеження необхідні для охорони певних суспільних інтересів чи захисту суб'єкта персональних даних, чи прав і свобод інших осіб доти, доки це необхідно в демократичному суспільстві.[160] Такі винятки є необ-

159 Конвенція 108, ст. 8 (a).

160 Там само, ст. 9 (2); та Директива про захист персональних даних, ст. 13 (1).

хідними, наприклад, у контексті розслідування злочинів, проте можуть застосовуватись за інших обставин.

4.3.1. Інформація

Згідно до вимог **права РЄ і права ЄС** володільці персональних даних зобов'язані заздалегідь інформувати суб'єкта персональних даних про намір здійснити обробку.[161] Це зобов'язання не залежить від запиту суб'єкта персональних даних, а має проактивно здійснюватись володільцем незалежно від того, чи виказує суб'єкт персональних даних зацікавленість в інформуванні, чи ні.

Зміст інформації

В інформації має бути зазначено мету обробки, а також дані про особу володільця та його контакти.[162] Положення Директиви про захист персональних даних вимагають надавати додаткову інформацію, якщо вона необхідна «з огляду на особливі обставини, за яких дані збираються, для гарантії справедливої обробки по відношенню до суб'єкта персональних даних». У статтях 10 та 11 Директиви визначено, серед іншого, категорії даних для обробки та категорії одержувачів таких даних, а також існування права доступу до даних та можливості їх корегування. В разі, коли інформацію збирають у суб'єктів персональних даних, в інформації має бути зазначено про обов'язковість чи добровільність надання відповідей, а також про можливі наслідки ненадання відповіді.[163]

З точки зору **права РЄ** надання такої інформації може вважатися належною практикою, як того вимагає принцип ретельної обробки персональних даних, і в цьому контексті таке надання інформації також є частиною права РЄ.

Принцип ретельної обробки вимагає викладення інформації у легкій для розуміння суб'єктами персональних даних формі. Мова, якою викладено інформацію, має бути зрозумілою тим, кому вона адресується. Її рівень і тип мають орієнтуватися на цільову аудиторію, наприклад, дорослих або дітей, широкий загал чи вчених експертів.

Деякі суб'єкти персональних даних можуть мати бажання отримати коротку інформацію про те, як і чому обробляють їхні дані, а інші вимагатимуть де-

161 Конвенція 108, ст. 8 (a); та Директива про захист персональних даних, ст. 10 та 11.

162 Конвенція 108, ст. 8 (a); та Директива про захист персональних даних, ст. 10 (a) та (b).

163 Директива про захист персональних даних, ст. 10 (c).

тального пояснення. Питання, як збалансувати цей аспект справедливого інформування, розглядається у висновку Робочої групи «Стаття 29», у якому підтримується ідея так званих багаторівневих повідомлень,[164] що дозволяють суб'єкту персональних даних вирішити, якому рівню деталізації інформації він або вона віддає перевагу.

Час повідомлення інформації

Директива про захист персональних даних містить ненабагато відмінні положення про час надання інформації, який залежить від того, чи збираються відомості у суб'єкта персональних даних (стаття 10), чи у третьої особи (стаття 11). В разі збору інформації у суб'єкта персональних даних інформація повинна бути надана не пізніше моменту збирання. Якщо інформація збирається у третіх осіб, то повідомлення має бути зроблене не пізніше моменту реєстрації даних володільцем або до того, як відомості вперше розголошуються третім особам.

Винятки з обов'язку інформувати

Відповідно до права ЄС загальний виняток із положення щодо зобов'язання інформувати суб'єкт персональних даних стосується ситуації, коли суб'єкта персональних даних вже поінформовано.[165] Це стосується ситуацій, коли суб'єкту персональних даних в залежності від обставин справи вже відомо, що його або її дані оброблятимуться для визначеної мети певним володільцем.

У положеннях статті 11 Директиви щодо зобов'язання інформувати суб'єкт персональних даних, якщо від нього або від неї не були отримані дані, також йдеться про те, що на процедуру обробки даних, зокрема, у статистичних цілях чи з метою історичних чи наукових досліджень, таке зобов'язання не розповсюджується, якщо:

- надання такої інформації виявляється неможливим; або
- може спричинити непропорційні зусилля; або
- реєстрація або розкриття даних чітко передбачено законом.[166]

Тільки у статті 11 (2) Директиви про захист персональних даних йдеться про те, що суб'єктів даних не потрібно інформувати про операції з обробки у разі, якщо

164 Робоча група «Стаття 29» (2004), *Висновок 10/2004 щодо більш гармонізованих інформаційних положень*, РГ 100, Брюссель, 25 листопада 2004 р.

165 Директива про захист персональних даних, ст. 10 та 11 (1).

166 Там само, п. 40 преамбули та стаття 11 (2).

їх передбачено законом. Припускаючи загалом, що суб'єкти персональних даних ознайомлені з вимогами закону, можна стверджувати, що якщо дані збираються у суб'єкта персональних даних в рамках статті 10 Директиви, то суб'єкт персональних даних вже поінформований. Але враховуючи, що факт знання закону лише припускається, принцип справедливої обробки вимагає відповідно до статті 10, щоб суб'єкта даних було поінформовано навіть у випадку, коли здійснення обробки передбачено законом, зокрема, з огляду на те, що інформування суб'єкта персональних даних не є занадто обтяжливою процедурою, якщо інформація збирається безпосередньо у самого суб'єкта персональних даних.

Що стосується права РЄ, то в Конвенції 108 чітко передбачено винятки з положень статті 8. До того ж передбачені у статтях 10 та 11 Директиви про захист персональних даних винятки можуть вважатися прикладами належної практики для винятків, передбачених у статті 9 Конвенції 108.

Різні способи інформування

Ідеальним способом інформування було б окреме звернення до кожного суб'єкта персональних даних в усній або письмовій формі. Якщо дані збираються у суб'єкта персональних даних, надання інформації повинне здійснюватися паралельно зі збиранням. Якщо дані збираються у третіх осіб, то, враховуючи очевидні практичні труднощі, пов'язані з тим, щоб дістатися до суб'єктів персональних даних, інформацію може бути надано шляхом відповідного оприлюднення.

Одним із найбільш ефективних способів інформування є виклад на офіційній веб-сторінці володільця відповідних умов надання інформації, наприклад політики конфіденційності веб-сайту. Проте в інформаційній політиці компанії або державного органу має враховуватися факт існування значної частини населення, яка не є інтернет-користувачами.

4.3.2. Повідомлення

Положення національного законодавства можуть зобов'язати володільця повідомляти компетентний наглядовий орган про операції з обробки для того, щоб їх було оприлюднено. Як альтернатива, у них може бути передбачено, що володільці можуть користуватися послугами фахівця з питань захисту персональних даних, відповідального, зокрема, за ведення реєстру здійснюваних володільцем операцій з обробки.[167] Доступ до цього внутрішнього реєстру має бути забезпечений для осіб, які звертаються із запитами.

167 Там само, ст. 18 (2) другий абзац.

Приклад: Повідомлення, а також документи, які підготовлені фахівцем із захисту персональних даних, повинні містити опис основних характеристик обробки персональних даних. Це охоплює інформацію про володільця, мету обробки, правове обґрунтування обробки, категорії даних для обробки, ймовірних третіх осіб одержувачів і можливість або відсутність можливості транскордонної передачі даних, і якщо так, то яких.

Оприлюднені наглядовим органом повідомлення повинні заноситись до спеціального реєстру. Для того, щоб відповідати своїй меті, доступ до цього реєстру має бути легким і безкоштовним. Те саме стосується і документації, яку зберігає фахівець із захисту персональних даних володільця.

У національному законодавстві можуть бути встановлені винятки з обов'язку повідомляти компетентний наглядовий орган або звертатись до внутрішнього фахівця з питань захисту персональних даних у випадках обробки, щодо яких існує мала вірогідність особливого ризику для суб'єктів персональних даних, що також передбачено в статті 18 (2) Директиви про захист персональних даних.[168]

4.4. Правила щодо забезпечення відповідності

Ключові моменти

- Розвиваючи принцип відповідальності, Директива про захист персональних даних передбачає декілька інструментів забезпечення відповідності:
  - попередній контроль національним наглядовим органом за запланованими операціями з обробки персональних даних;
  - посадових осіб з питань захисту персональних даних, які надають володільцю спеціальні консультації у сфері захисту персональних даних;
  - кодекси поведінки, у яких зазначаються існуючі правила захисту персональних даних, що застосовуються в певній сфері суспільного життя, особливо в бізнесі.
- У праві РЄ подібні інструменти забезпечення відповідності пропонуються в Рекомендації щодо профайлінгу.

168 Там само, ст. 18 (2) перший абзац.

4.4.1. Попередня перевірка

Відповідно до статті 20 Директиви про захист персональних даних перед початком обробки даних наглядовий орган повинен перевіряти операції з обробки даних, які через мету або обставини обробки можуть становити певний ризик для прав і свобод суб'єктів персональних даних. Національне законодавство має визначати, які операції з обробки персональних даних підлягають попередній перевірці. Результатом такої перевірки може стати або заборона операцій з обробки персональних даних, або видання розпорядження щодо зміни характеристик запропонованого формату цих операцій. Метою статті 20 Директиви є забезпечення того, щоб надто ризиковані операції з обробки даних навіть не починалися, оскільки наглядовий орган має право забороняти такі операції. Передумовою ефективності цього механізму є обов'язкове сповіщення наглядового органу. Щоб наглядові органи могли гарантувати, що володільці виконуватимуть свої зобов'язання щодо забезпечення сповіщення, вони повинні мати такі владні повноваження, як можливість штрафувати володільців.

Приклад: Якщо компанія здійснює операції з обробки персональних даних, які відповідно до національного законодавства підлягають попередній перевірці, ця компанія повинна надати наглядовому органу документацію щодо запланованих операцій з обробки даних. Компанії не дозволяється починати операції з обробки даних до одержання позитивної відповіді наглядового органу.

У деяких державах-членах національне законодавство в якості альтернативи передбачає, що операції з обробки даних можна починати, якщо протягом певного терміну, наприклад, трьох місяців, з боку наглядового органу відсутнє будь-яке реагування.

4.4.2. Посадові особи з питань захисту персональних даних

Директива про захист персональних даних допускає, щоб національне законодавство передбачало можливість призначити володільцями особу, яка виконуватиме функції посадової особи із захисту персональних даних.[169] Метою

169 Там само, ст. 18 (2) другий абзац.

діяльності такої посадової особи є мінімізація негативного впливу від обробки персональних даних на права і свободи суб'єктів персональних даних.[170]

> Приклад: У Німеччині, відповідно до пункту 1 Статті 4f Федерального закону про захист персональних даних (*Bundesdatenschutzgesetz*), приватні компанії зобов'язані призначати внутрішню посадову особу з питань захисту персональних даних, якщо в таких компаніях на постійній основі працюють 10 або більше осіб, які займаються автоматизованою обробкою персональних даних.

Як чітко зазначено у Директиві, можливість досягнути цієї мети вимагає певного рівня незалежності для такої посадової особи в межах організації володільця. Для забезпечення ефективного функціонування такої посадової особи також необхідно передбачити міцний захист трудових прав, щоб унеможливити необґрунтоване звільнення з роботи.

З метою узгодити з національним законодавством про захист персональних даних концепцію внутрішніх посадових осіб з питань захисту персональних даних, така концепція була затверджена також в окремих рекомендаціях РЄ.[171]

4.4.3. Кодекси поведінки

Задля сприяння дотриманню визначених норм бізнесовий та інші сектори можуть розробити докладні правила, які регулюватимуть їхню стандартну діяльність з обробки персональних даних, узагальнюючи в такий спосіб найкращі практики. Консультації представників сектору сприятимуть пошуку рішень, які будуть практичними, а тому й зможуть виконуватися. Відповідно державам-членам і Європейській Комісії рекомендується заохочувати розробку кодексів поведінки, призначених сприяти належному виконанню норм національного законодавства, прийнятих державами-членами відповідно до Директиви та з врахуванням особливих рис різних секторів.[172]

Для забезпечення відповідності цих кодексів поведінки положенням національного законодавства, прийнятим відповідно до Директиви про захист персональних даних, держави-члени повинні встановити процедуру оціню-

170 Там само.

171 Див., наприклад, Рекомендацію щодо профайлінгу, ст. 8.3.

172 Див. Директиву про захист персональних даних, ст. 27 (1).

вання кодексів. Така процедура зазвичай вимагатиме залучення національного органу, торгових асоціацій та інших органів, які представляють інші категорії володільців.[173]

Проекти кодексів Співтовариств і поправки чи доповнення до чинних кодексів Співтовариств можуть подаватися до Робочої групи «Стаття 29» для проведення їх оцінювання. Після схвалення кодексів цією Робочою групою Європейська комісія може забезпечити їх належне оприлюднення.[174]

Приклад: Європейська федерація прямого та інтерактивного маркетингу (FEDMA) розробила Європейський кодекс поведінки з питань використання персональних даних у прямому маркетингу. Кодекс був успішно поданий на розгляд Робочої групи «Стаття 29». Додаток, що стосується електронних маркетингових комунікацій, було додано до кодексу в 2010 році.[175]

173 Там само, ст. 27 (2).

174 Там само, ст. 27 (3).

175 Робоча група статті 29 (2010), Висновок 4/2010 щодо Європейського кодексу поведінки Європейської федерації прямого та інтерактивного маркетингу (FEDMA) з питань використання персональних даних у прямому маркетингу, WP 174, Брюссель, 13 липня 2010 р.

5 Права суб'єктів персональних даних та їх здійснення

ЄС	питання, що висвітлюються	РЄ
Право на доступ		
Директива про захист персональних даних, стаття 12 Суд ЄС, C-553/07, *«Мер і члени міської ради Роттердаму проти М.Е.Е. Рейкебура»*, 7 травня 2009 р.	**Право на доступ до власних даних**	Конвенція № 108, стаття 8 (b)
	Право на виправлення, стирання (видалення) або блокування	Конвенція № 108, стаття 8 (c) ЄСПЛ, *«Джемалеттін Джанли проти Туреччини»*, № 22427/04, 18 листопада 2008 р. ЄСПЛ, *«Зегерштед-Віберг та інші проти Швеції»*, № 62332/00, 6 червня 2006 р. ЄСПЛ, *«Чуботару проти Молдови»*, № 27138/04, 27 квітня 2010 р.

ЄС	питання, що висвітлюються	РЄ
Право на заперечення		
Директива про захист персональних даних, стаття 14 (1) (a)	**Право на заперечення, пов'язане з конкретною ситуацією суб'єкта персональних даних**	Рекомендація щодо профайлінгу, стаття 5.3
Директива про захист персональних даних, стаття 14 (1) (b)	**Право на заперечення проти подальшого використання персональних даних з метою прямого маркетингу**	Рекомендація щодо прямого маркетингу, стаття 4.1
Директива про захист персональних даних, стаття 15	**Право на заперечення проти автоматизованих рішень**	Рекомендація щодо профайлінгу, стаття 5.5
Незалежний нагляд		
Хартія, стаття 8 (3) Директива про захист персональних даних, стаття 28 Регламент інституцій ЄС щодо захисту персональних даних, Розділ V Регламент щодо захисту персональних даних Суд ЄС, C-518/07, *«Європейська комісія проти Федеративної Республіки Німеччина»*, 9 березня 2010 р. Суд ЄС, C-614/10, *«Європейська комісія проти Республіка Австрія»*, 16 жовтня 2012 р. Суд ЄС, C-288/12, *«Європейська комісія проти Угорщини»*, 8 квітня 2014 р.	**Національні наглядові органи**	Конвенція № 108, Додатковий протокол, стаття 1

ЄС	питання, що висвітлюються	РЄ
Засоби правового захисту та санкції		
Директива про захист персональних даних, стаття 12	**Направлення запитів до володільця**	Конвенція № 108, стаття 8 (b)
Директива про захист персональних даних, стаття 28 (4) Регламент інституцій ЄС щодо захисту даних, стаття 32 (2)	**Претензії, подані до наглядового органу**	Конвенція № 108, Додатковий протокол, стаття 1 (2) (b)
Хартія, стаття 47	**Суди (в цілому)**	ЄКПЛ, стаття 13
Директива про захист персональних даних, стаття 28 (3)	**Національні суди**	Конвенція № 108, Додатковий протокол, стаття 1 (4)
ДФЄС, стаття 263 (4) Регламент інституцій ЄС щодо захисту персональних даних, стаття 32 (1) ДФЄС, стаття 267	**Суд ЄС**	
	ЄСПЛ	ЄКПЛ, стаття 34
Засоби правового захисту та санкції		
Хартія, стаття 47 Директива про захист персональних даних, статті 22 і 23 Суд ЄС, C-14/83, *«Сабіне фон Колсон і Елізабет Каманн проти землі Північний Рейн-Вестфалія»*, 10 квітня 1984 р. Суд ЄС, C-152/84, *«М.Х. Маршалл проти Управління охорони здоров'я регіону Саутгемптону та Південно-Західного Гемпширу»*, 26 лютого 1986 р.	**Порушення національного законодавства про захист персональних даних**	ЄКПЛ, стаття 13 (лише для держав-членів РЄ) Конвенція № 108, стаття 10 ЄСПЛ, *«К. У. проти Фінляндії»*, № 2872/02, 2 грудня 2008 р. ЄСПЛ, *«Бірюк проти Литви»*, № 23373/03, 25 листопада 2008 р.

ЄС	питання, що висвітлюються	РЄ
Регламент інституцій ЄС щодо захисту персональних даних, статті 34 і 49 Суд ЄС, C-28/08 P, *«Європейська комісія проти компанії «The Bavarian Lager Co. Ltd»*, 29 червня 2010 р.	**Порушення права ЄС інституціями та органами ЄС**	

Ефективність правових норм у цілому та прав суб'єктів персональних даних зокрема значною мірою залежить від існування відповідних механізмів їх реалізації. В європейському праві у сфері захисту персональних даних національне законодавство повинно наділяти суб'єкт персональних даних правом на захист своїх даних. Для надання суб'єктам персональних даних допомоги у здійсненні їхніх прав та для нагляду за обробкою персональних даних національним законодавством також повинні створюватися незалежні наглядові органи. Крім того, право на ефективний засіб правового захисту, яке гарантується ЄКПЛ та Хартією, вимагає, щоб засоби правового захисту були доступними кожному.

5.1. Права суб'єктів персональних даних

Ключові моменти

- Кожен має право відповідно до національного законодавства вимагати від будь-якого володільця інформацію щодо того, чи займається цей володілець обробкою його персональних даних.
- Відповідно до національного законодавства суб'єкти персональних даних мають право на:
  - доступ до своїх даних через будь-якого володільця, який займається обробкою таких даних;
  - виправлення (або, за потреби, блокування) своїх персональних даних володільцем, який займається обробкою цих даних, якщо вони є неточними;
  - видалення своїх персональних даних або, за потреби, їх блокування володільцем, якщо цей володілець займається їх обробкою незаконно.

- Крім того, суб'єкти персональних даних мають право висувати володільцям заперечення проти:
  - автоматизованих рішень (прийнятих з використанням персональних даних, оброблених лише за допомогою автоматичних засобів);
  - обробки своїх персональних даних, якщо вона призводить до непропорційних результатів;
  - використання своїх персональних даних задля прямого маркетингу.

5.1.1. Право на доступ

Відповідно до права ЄС стаття 12 Директиви про захист персональних даних містить елементи права суб'єктів персональних даних на доступ, у тому числі права на отримання від володільця «підтвердження того, чи обробляються дані, які їх стосуються, та інформації, принаймні, про цілі обробки, категорії розглянутих даних і про одержувачів чи категорії одержувачів, яким надаються дані», а також «виправлення, стирання чи блокування даних, обробка яких не відповідає положенням даної Директиви, зокрема через неповноту чи неточність даних».

У праві РЄ існують такі ж права, які мають бути передбачені національним законодавством (стаття 8 Конвенції № 108). У декількох рекомендаціях РЄ використовується термін «доступ», а різні аспекти права на доступ описуються і пропонуються для імплементації до національного законодавства у той самий спосіб, який зазначено в попередньому пункті.

Відповідно до статті 9 Конвенції № 108 та статті 13 Директиви про захист персональних даних, обов'язок володільців давати відповіді на запити суб'єктів персональних даних на отримання доступу може бути обмежений в результаті наявності переважаючих законних інтересів інших осіб. До переважаючих законних інтересів можуть відноситись державні інтереси, такі як національна безпека, громадська безпека і розслідування кримінальних правопорушень, а також приватні інтереси, які переважають інтереси захисту персональних даних. Будь-які виключення або обмеження повинні бути необхідними у демократичному суспільстві і пропорційними меті, що переслідується. У дуже виняткових ситуаціях, наприклад, через медичні показання, захист суб'єкта персональних даних може потребувати обмеження в прозорості; це передусім стосується обмеження права кожного суб'єкта персональних даних на доступ.

Щоразу, коли персональні дані обробляються лише з метою проведення наукового дослідження або у статистичних цілях, Директива про захист персональних даних допускає обмеження національним законодавством права на доступ; однак повинні бути наявними достатні правові гарантії. Зокрема, мають існувати гарантії того, що в процесі такої обробки персональних даних не буде вжито чи прийнято жодних заходів чи рішень стосовно певної особи «за явної відсутності якого-небудь ризику втручання у персональне життя суб'єкта даних».[176] Подібні положення містяться у статті 9 (3) Конвенції № 108.

Право на доступ до власних персональних даних

Відповідно до права РЄ право на доступ до власних персональних даних прямо визнається статтею 8 Конвенції № 108. ЄСПЛ неодноразово постановляв, що існує право на доступ до інформації про свої персональні дані, якою володіють або яку використовують інші особи, і це право виникає з необхідності поважати приватне життя.[177] У справі *«Леандер»*[178] ЄСПЛ дійшов висновку про те, що право на доступ до персональних даних, які зберігаються державними органами, може за певних обставин обмежуватися.

Відповідно до права ЄС право на доступ до власних персональних даних прямо визнається статтею 12 Директиви про захист персональних даних і, як основне право, статтею 8 (2) Хартії.

Стаття 12 (а) Директиви передбачає, що держави-члени повинні гарантувати кожному суб'єкту даних право на доступ до його персональних даних та інформації. Зокрема, кожен суб'єкт персональних даних має право отримати від володільця підтвердження того, чи обробляються пов'язані з ним дані, а також інформацію, яка повинна охоплювати, принаймні, наступне:

- цілі обробки;
- категорії відповідних даних;
- дані, що проходять обробку;
- одержувачів або категорії одержувачів, яким розкриваються дані;
- будь-яку наявну інформацію про джерело даних, що проходять обробку;

176 Директива про захист персональних даних, ст. 13 (2).

177 ЄСПЛ, *«Гаскін проти Сполученого Королівства»*, № 10454/83, 7 липня 1989 р.; ЄСПЛ, *«Одієвр проти Франції»* [GC], № 42326/98, 13 лютого 2003 р.; ЄСПЛ, *«К.Х. та інші проти Словаччини»*, № 32881/04, 28 квітня 2009 р.; ЄСПЛ, *«Годеллі проти Італії»*, № 33783/09, 25 вересня 2012 р.

178 ЄСПЛ, *«Леандер проти Швеції»*, № 9248/81, 26 березня 1987 р.

- у разі автоматизованих рішень, логіку, що застосовується в процесі автоматизованої обробки даних.

Національне законодавство може передбачати надання володільцем такої додаткової інформації, як, наприклад, посилання на нормативно-правову базу, що дозволяє обробку персональних даних.

Приклад: Маючи доступ до своїх персональних даних, кожен може визначити, чи є ці дані точними. Тому необхідно, щоб суб'єкта персональних даних було проінформовано про категорії даних, що обробляються, а також про зміст цих даних. Таким чином, недостатньо, щоб володілець просто сказав суб'єкту персональних даних, що він обробляє інформацію про його ім'я, адресу, дату народження та сфери інтересів. Володілець також повинен повідомити суб'єкту даних, що обробляється його «ім'я: N.N.; адреса: 1040, Відень, Шварценбергплац, 11, Австрія; дата народження: 10.10.1974 р.; та сфера інтересів (за заявою суб'єкта даних): класична музика». Крім того, в останньому пункті повинна міститися інформація про джерело даних.

Повідомлення суб'єкта персональних даних про здійснення обробки даних і будь-яку наявну інформацію стосовно їх джерела має здійснюватися в доступній для розуміння формі, що означає, що володільцю, можливо, доведеться більш докладно пояснювати суб'єкту персональних даних, що саме він обробляє. Наприклад, саме лише цитування технічних абревіатур або медичних термінів у відповідь на запит на надання доступу є, як правило, недостатнім, навіть якщо зберігаються лише ці абревіатури і терміни.

Інформація про джерело даних, які обробляє володілець, має надаватися у відповідь на запит на надання доступу за умови, що вона є доступною. Це положення слід тлумачити з огляду на принципи відкритості та відповідальності. Володілець не може знищити інформацію про джерело даних, щоб бути звільненим від необхідності розкривати її; він також не може ігнорувати звичайні стандартні та загальновизнані потреби у забезпеченні документування у сфері своєї діяльності. Відсутність документування щодо джерел оброблених персональних даних є, як правило, невиконанням зобов'язань володільця стосовно права на доступ.

Якщо проводиться автоматизоване оцінювання, необхідно пояснювати загальну логіку цього оцінювання, в тому числі конкретні критерії, які бралися до уваги в процесі оцінювання суб'єкта персональних даних.

З Директиви не зрозуміло, чи стосується право на доступ до інформації минулого, а якщо так, то про який саме період у минулому йде мова. У зв'язку з цим, що підкреслює практика Суду ЄС, право на доступ до власних даних не може надміру обмежуватися в часі. Суб'єктам персональних даних також повинна надаватися розумна можливість отримати інформацію про останні операції з обробки персональних даних.

Приклад: У справі *«Рейкебур»*[179] в Суду ЄС попросили визначити, чи може відповідно до статті 12 (a) Директиви право особи на доступ до інформації про одержувачів або категорії одержувачів персональних даних, а також про зміст повідомлених даних, обмежуватися одним роком перед поданням нею запиту на отримання доступу.

Щоб визначити, чи дозволяє стаття 12 (a) Директиви таке обмеження за часом, Суд вирішив витлумачити цю статтю з огляду на цілі Директиви. Спершу Суд заявив, що право на доступ є необхідним для здійснення суб'єктом персональних даних права на виправлення, стирання чи блокування володільцем його даних (стаття 12 (b)) або повідомлення третіх осіб, яким розкриваються ці дані, про таке виправлення, стирання чи блокування (стаття 12 (c)). Право на доступ є також необхідним для того, щоб суб'єкт персональних даних міг здійснювати своє право на заперечення проти обробки своїх персональних даних (стаття 14) або право на подання позову у разі, якщо він зазнав збитків (статті 22 і 23).

Для забезпечення практичної дії положень, згаданих вище, Суд постановив, що «це право повинно неодмінно стосуватися минулого. Якби це було не так, суб'єкт персональних даних не міг би ефективно здійснювати своє право на те, щоб його дані вважалися незаконно або неправильно виправленими, стертими чи заблокованими, або на подання позову до суду та отримання компенсації за зазнані збитки».

Право на виправлення, стирання та блокування персональних даних

«Будь-яка особа повинна мати можливість використати право доступу до даних, які стосуються її і перебувають в обробці, з метою їхньої перевірки, осо-

179 Суд ЄС, C-553/07, *«Мер і члени міської ради Роттердаму проти М.Е.Е. Ріджкебура»*, 7 травня 2009 р.

бливо перевірки точності і законності обробки.»[180] Згідно з цими принципами суб'єкти персональних даних повинні мати гарантоване національним законодавством право домагатися від володільця виправлення, стирання чи блокування своїх даних, якщо вони вважають, що їх обробка не відповідає положенню Директиви, зокрема, через неточний або неповний характер персональних даних.[181]

Приклад: У справі «*Джемалеттін Джанли проти Туреччини*»[182] ЄСПЛ встановив порушення статті 8 ЄКПЛ у неправильній звітності поліції в кримінальному провадженні.

Заявник двічі залучався до кримінального провадження через своє начебто членство у нелегальних організаціях, але жодного разу не був засуджений. Коли заявник був знову заарештований та звинувачений в іншому кримінальному правопорушенні, поліція подала до кримінального суду звіт під назвою «*довідкова форма щодо додаткових правопорушень*», у якому заявник зазначався як член двох нелегальних організацій. Подання заявником клопотання про внесення змін до звіту і поліцейського досьє було безрезультатним. ЄСПЛ постановив, що інформація, зазначена у звіті поліції, могла підпадати під дію статті 8 ЄКПЛ, оскільки публічна інформація також може входити до категорії «приватне життя», якщо вона систематично збирається і зберігається в архівах органів влади. Крім того, поліцейський звіт був некоректним, а його підготовка та передача до кримінального суду не відповідали закону. Суд дійшов висновку, що мало місце порушення статті 8.

Приклад: У справі «*Зегерштед-Віберг та інші проти Швеції*»[183] заявники були пов'язані з певними ліберальними і комуністичними політичними партіями. Вони підозрювали, що відомості про них було внесено до протоколів служби безпеки. ЄСПЛ задовольнило те, що зберігання даних, про які йшла мова, мало правові підстави і переслідувало законну мету. Стосовно декого із заявників ЄСПЛ виявив, що тривале збережен-

180 Директива про захист персональних даних, декларативна частина 41.

181 Там само, ст. 12 (b).

182 ЄСПЛ, «*Джемалеттін Джанли проти Туреччини*», № 22427/04, 18 листопада 2008 р., пп. 33, 42 і 43; ЄСПЛ, «*Даля проти Франції*», № 964/07, 2 лютого 2010 р.

183 ЄСПЛ, «*Сегерштед-Віберг та інші проти Швеції*», № 62332/00, 6 червня 2006 р., пп. 89 і 90; Див. також, наприклад: ЄСПЛ, «*М.К. проти Франції*», № 19522/09, 18 квітня 2013 р.

ня цих даних було непропорційним втручанню у їх приватне життя. Наприклад, стосовно пана Шміда органи влади зберігали інформацію, що під час демонстрацій в 1969 році він чинив сильний опір поліції. ЄСПЛ виявив, що ця інформація могла не переслідувати жодного відповідного інтересу національної безпеки, особливо враховуючи її історичний характер. ЄСПЛ дійшов висновку, що стосовно чотирьох з п'яти заявників мало місце порушення статті 8 ЄКПЛ.

В деяких випадках буде достатнім, щоб суб'єкт персональних даних просто попросив виправити, наприклад, написання його імені або змінити адресу чи телефонний номер. Проте якщо це прохання пов'язане з такими правовими питаннями, як правова ідентичність суб'єкта персональних даних або правильне місце проживання для доставки юридичних документів, його може бути недостатньо, а володілець може мати право вимагати доказів стверджуваної неточності. Такі вимоги не повинні покладати непомірний тягар доказування на суб'єкта персональних даних і тим самим позбавляти його можливості виправити свої дані. ЄСПЛ виявив порушення статті 8 ЄКПЛ у декількох справах, у яких заявник не зміг оскаржити точність інформації, що зберігалася в журналах обліку секретних документів.[184]

Приклад: У справі *«Чуботару проти Молдови»*[185] заявник не зміг змінити в офіційних документах реєстраційний запис щодо свого етнічного походження з молдавського на румунське нібито через те, що він не обґрунтував своє прохання. ЄСПЛ вважав прийнятним, щоб при реєстрації етнічної ідентичності індивіда держави вимагали об'єктивних доказів. Якщо б така вимога базувалася винятково на суб'єктивних і необґрунтованих підставах, органи влади могли б відмовити у її виконанні. Проте вимога заявника була заснована не лише на його суб'єктивному сприйнятті своєї етнічної приналежності; він був у змозі вказати на такі зв'язки з румунською етнічною групою, як мова, ім'я, взаємопорозуміння тощо, які можна було об'єктивно довести. Однак відповідно до національного законодавства заявник повинен був надати докази того, що його батьки належали до етнічної групи румунів. Враховуючи історичні реалії Молдови, така вимога створила непереборний бар'єр для реєстрації етнічної ідентичності, відмінної від тієї, за якою радянська влада зареєструвала його

184 ЄСПЛ, *«Ротару проти Румунії»*, № 28341/95, 4 травня 2000 р.

185 ЄСПЛ, *«Чуботару проти Молдови»*, № 27138/04, 27 квітня 2010 р., пп. 51 і 59.

батьків. Щоб не дати заявнику домогтися розгляду його вимоги з врахуванням доказів, які можна об'єктивно перевірити, держава не виконала свого позитивного зобов'язання щодо гарантування заявнику дійсної поваги до його приватного життя. Суд дійшов висновку, що тут мало місце порушення статті 8 ЄКПЛ.

Під час цивільного процесу або провадження та до того, як державна влада прийме рішення про те, чи є дані вірними, суб'єкт персональних даних може подати запит, щоб до файлу з його даними було внесено запис або примітку, у якій би зазначалося, що точність даних оскаржується, а офіційне рішення все ще не прийняте. Протягом цього періоду володілець персональних даних не повинен представляти дані як достовірні або остаточні, особливо третім особам.

Запит суб'єкта персональних даних з вимогою стерти або видалити дані часто базується на твердженні про те, що обробка даних не має законної підстави. Такі твердження часто виникають, коли згоду було відкликано або якщо певні дані більше не потрібні для досягнення мети збирання даних. Тягар доказування того, що обробка даних є законною, буде покладений на володільця персональних даних, оскільки він відповідає за законність обробки даних. Відповідно до принципу відповідальності, володілець повинен у будь-який час бути в змозі продемонструвати, що для обробки даних існує міцна правова підстава; в іншому випадку обробку слід зупинити.

Якщо обробка даних оскаржується, оскільки дані нібито є неправильними або обробляються незаконно, відповідно до принципу справедливої обробки даних суб'єкт персональних даних може вимагати, щоб дані, які є предметом спору, були заблоковані. Це означає, що дані не видаляються, але володілець повинен утримуватися від їх використання впродовж періоду блокування. Це особливо необхідно, якщо подальше використання даних, які є неточними або зберігаються незаконно, може зашкодити суб'єкту персональних даних. Національне законодавство має надати докладнішу інформацію про те, коли можуть виникати зобов'язання з блокування використання персональних даних та як це має здійснюватися.

Крім того, суб'єкти персональних даних мають право домагатися того, щоб володілець сповістив третіх осіб про будь-яке блокування, виправлення чи стирання, якщо вони отримали дані до початку цих операцій з обробки даних. Оскільки володілець мав задокументувати розкриття даних третім особам, ідентифікація одержувачів даних та звернення до них з проханням видали-

ти дані мають бути можливими. Проте якщо тим часом дані були опубліковані, наприклад, в мережі Інтернет, це може унеможливити цілковите видалення даних, оскільки одержувачі даних не можуть бути знайдені. Відповідно до Директиви про захист персональних даних, звернення до одержувачів даних для виправлення, видалення чи блокування даних є обов'язковим, «якщо це не виявляється неможливим або вимагає непропорційних зусиль».[186]

5.1.2. Право на заперечення

Право на заперечення включає в себе право на заперечення проти автоматизованих індивідуальних рішень, право на заперечення, пов'язане з конкретною ситуацією суб'єкта персональних даних, і право на заперечення проти подальшого використання даних в цілях прямого маркетингу.

Право на заперечення проти автоматизованих індивідуальних рішень

Автоматизовані рішення – це рішення, прийняті з використанням персональних даних, оброблених виключно за допомогою автоматичних засобів. Якщо цілком імовірно, що такі рішення можуть мати значний вплив на життя окремих осіб, оскільки вони стосуються, наприклад, кредитоспроможності, результативності в роботі, поведінки або надійності, для уникнення недопустимих наслідків необхідний спеціальний захист. Директива про захист персональних даних передбачає, що автоматизовані рішення не повинні визначати питання, які є важливими для людей, і вимагає, щоб особа мала право на перегляд автоматизованого рішення.[187]

Приклад: Важливим практичним прикладом автоматизованого прийняття рішень є оцінка кредитоспроможності. Для швидкого прийняття рішення щодо кредитоспроможності майбутнього клієнта в нього беруться певні дані, такі як інформація про професію, сімейний стан, і поєднуються з даними про цього суб'єкта, отриманими з інших джерел, наприклад, з кредитних інформаційних систем. Ці дані автоматично вносяться до алгоритму оцінювання, який обчислює загальне значення, що дає уявлення про кредитоспроможність потенційного клієнта. Таким чином, співробіт-

186 Директива про захист персональних даних, ст. 12 (c), друга половина речення.

187 Там само, ст. 15 (1).

ник компанії може протягом декількох секунд прийняти рішення про те, чи є суб'єкт персональних даних прийнятним в якості клієнта.

Тим не менш, відповідно до Директиви держави-члени повинні забезпечити, щоб стосовно особи не приймалося автоматизоване індивідуальне рішення, якщо інтереси суб'єкта персональних даних або не знаходяться під загрозою, бо рішення було прийняте на його користь, або гарантуються іншими відповідними засобами.[188] Право на заперечення проти автоматизованих рішень притаманне також і **праву РЄ**, як можна побачити з Рекомендації щодо профайлінгу.[189]

Право на заперечення, пов'язане з конкретною ситуацією суб'єкта персональних даних

Загального права суб'єктів персональних даних на заперечення проти обробки своїх даних не існує.[190] Проте стаття 14 (a) Директиви про захист персональних даних наділяє суб'єкта персональних даних правом висувати заперечення на незаперечних законних підставах, пов'язаних з його конкретною ситуацією. Подібне право було визнано в Рекомендації РЄ щодо профайлінгу.[191] Такі положення спрямовані на пошук правильної рівноваги між правами на захист даних суб'єкта персональних даних і законними правами інших осіб під час обробки даних суб'єкта персональних даних.

Приклад: Банк зберігає дані про своїх клієнтів, які не виконують зобов'язання щодо сплати платежів по кредитам, протягом семи років. Клієнт, дані якого зберігаються в цій базі даних, просить надати йому ще один кредит. Переглядається база даних, надається оцінка фінансового стану, і клієнту відмовляють у наданні кредиту. Клієнт, однак, може заперечити проти того, щоб його персональні дані були занесені до бази даних, і вимагати їх видалення, якщо він може довести, що невиконання платіжних зобов'язань було лише результатом помилки, яку було виправлено відразу після того, як клієнт дізнався про неї.

188 Там само, ст. 15 (2).

189 Рекомендація щодо профайлінгу, ст. 5 (5).

190 Див. також ЄСПЛ, *«M.C. проти Швеції»*, № 20837/92, 27 серпня 1997 р., у якій медичні дані було повідомлено без згоди чи можливості висунути заперечення; або ЄСПЛ, *«Леандер проти Швеції»*, № 9248/81, 26 березня 1987 р.; або ЄСПЛ, *«Мослі проти Сполученого Королівства»*, № 48009/08, 10 травня 2011 р.

191 Рекомендація щодо профайлінгу, ст. 5 (3).

В результаті успішного заперечення, володілець більше не може обробляти дані, про які йде мова. Однак операції з обробки даних суб'єкта персональних даних, які були здійснені до висунення заперечення, залишаються законними.

Право на заперечення проти подальшого використання персональних даних з метою прямого маркетингу

Стаття 14 (b) Директиви про захист персональних даних передбачає конкретне право на заперечення проти використання своїх даних з метою прямого маркетингу. Таке право також закріплене у Рекомендації РЄ щодо прямого маркетингу.[192] Цей вид заперечення може висуватися до того, як дані стануть доступними третім особам з метою прямого маркетингу. Тому суб'єкту персональних даних повинна надаватися можливість висунути заперечення до здійснення передачі даних.

5.2. Незалежний нагляд

Ключові моменти

- Для забезпечення ефективного захисту персональних даних відповідно до національного законодавства мають створюватися незалежні наглядові органи.
- Національні наглядові органи повинні діяти у повній незалежності; це повинно гарантуватися установчим правом і відображатися у конкретній організаційній структурі наглядового органу.
- Наглядові органи мають конкретні завдання, зокрема:
  - здійснювати контроль та забезпечувати захист персональних даних на національному рівні;
  - консультувати суб'єктів персональних даних і володільців, а також уряд і громадськість в цілому;
  - розглядати скарги і допомагати суб'єкту персональних даних у випадку заявлених порушень прав на захист даних;
  - здійснювати нагляд за володільцями та особами, які займаються обробкою даних;

192 Комітет міністрів РЄ (1985), Рекомендація Rec(85)20 державам-членам щодо захисту персональних даних, що використовуються для прямого маркетингу, 25 жовтня 1985 р., ст. 4 (1).

- якщо це необхідно, втручатися шляхом:
  - попередження, винесення догани або навіть штрафування володільців та осіб, які займаються обробкою персональних даних,
  - видання розпоряджень про виправлення, блокування або видалення персональних даних,
  - накладення заборони на обробку;
- передавати справи до суду.

Директива про захист персональних даних вимагає здійснення незалежного нагляду як важливого механізму забезпечення ефективного захисту персональних даних. Директива запровадила інструмент для здійснення захисту персональних даних, якого не було ані в Конвенції № 108, ані в Керівних принципах з приватності ОЕСР.

Враховуючи, що незалежний нагляд виявився незамінним для розвитку ефективного захисту персональних даних, нове положення переглянутих Керівних принципів з приватності ОЕСР, прийнятих в 2013 році, закликає країни-члени «створювати і підтримувати органи влади із забезпечення приватності управлінням, ресурсами і технічними знаннями, необхідними для ефективного здійснення ними своїх повноважень та прийняття рішень на основі об'єктивності, безсторонності та послідовності».[193]

Відповідно до права РЄ Додатковий протокол до Конвенції № 108 зробив створення органів нагляду обов'язковим. У статті 1 цього інструменту міститься правова база для незалежних наглядових органів, яку Договірні Сторони повинні імплементувати у своє національне законодавство. Для опису завдань і повноважень цих органів він використовує формулювання, подібні до тих, які застосовуються в Директиві про захист персональних даних. Тому відповідно до права ЄС та РЄ наглядові органи в принципі повинні функціонувати подібним чином.

Відповідно до права ЄС компетенції та організаційна структура наглядових органів вперше були викладені у статті 28 (1) Директиви про захист персональних даних. Регламент інституцій ЄС щодо захисту персональних даних[194] створює

193 ОЕСР (2013), Керівні принципи, що регулюють захист приватності і транскордонну предачу персональних даних, п. 19 (c).

194 Регламент № 45/2001 Європейського парламенту та Ради (ЄС) від 18 грудня 2000 р. про захист фізичних осіб, що стосується обробки персональних даних установами і органами Спільноти і щодо вільного переміщення таких даних, OJ 2001 L 8, ст. 41–48.

Європейського інспектора із захисту персональних даних (ЄІЗПД) як наглядовий орган для обробки даних з боку органів та інституцій ЄС. Окреслюючи ролі та обов'язки наглядового органу, цей регламент спирається на досвід, накопичений з часу оприлюднення Директиви про захист персональних даних.

Незалежність органів влади з питань захисту персональних даних гарантується статтею 16 (2) ДФЄС і статтею 8 (3) Хартії. Це останнє положення конкретно розглядає контроль з боку незалежного органу, як суттєвий елемент основного права на захист персональних даних. Крім того, Директива про захист персональних даних вимагає, щоб держави-члени створювали наглядові органи для контролю за застосуванням Директиви, які б діяли у повній незалежності.[195] Не лише закон, що лежить в основі створення наглядового органу, повинен містити положення, яке б головним чином гарантувало незалежність, але й певна організаційна структура органу влади повинна демонструвати незалежність.

В 2010 році Суд ЄС вперше зіткнувся з питанням сфери застосування вимоги щодо незалежності наглядових органів з питань захисту персональних даних.[196] Наступні приклади ілюструють його думку з цього приводу.

Приклад: У справі *«Європейська комісія проти Німеччини»*[197] Європейська комісія звернулася до Суду ЄС з проханням визнати, що Німеччина неправильно транспонувала вимогу щодо «повної незалежності» наглядових органів, відповідальних за забезпечення захисту персональних даних, і, таким чином, не виконала свої зобов'язання за статтею 28 (1) Директиви про захист персональных даних. На думку Комісії, проблема полягала в тому, що Німеччина перевела під нагляд держави органи влади, відповідальні за контроль за обробкою персональних даних поза межами державного сектору в різних федеральних землях.

На думку Суду, оцінка суті позову залежала від сфери застосування вимоги щодо незалежності, що міститься в цьому положенні, а отже, від її тлумачення.

Суд підкреслив, що слова «у повній незалежності» статті 28 (1) Директиви повинні тлумачитися на основі фактичного формулювання цьо-

195 Директива про захист персональних даних, ст. 28 (1), останнє речення; Конвенція № 108, Додатковий протокол, ст. 1 (3).

196 Див. АОП (2010), Основні права: виклики та досягнення в 2010 році, Річний звіт за 2010 рік, стор. 59. АОП розглянула це питання більш детально у своєму звіті про Захист даних у Європейському Союзі: роль національних органів з питань захисту даних, який було опубліковано у травні 2010 року.

197 Суд ЄС, C-518/07, «*Європейська комісія проти Федеративної Республіки Німеччина*», 9 березня 2010 р., п. 27.

го положення, а також цілей та задуму Директиви про захист персональних даних.[198] Суд підкреслив, що наглядові органи є «гарантами» прав, пов'язаних з обробкою персональних даних, яку забезпечує Директива, і що таким чином їх створення у державах-членах вважається «важливою складовою захисту фізичних осіб в плані обробки персональних даних».[199] Суд дійшов висновку, що «виконуючи свої обов'язки, наглядові органи повинні діяти об'єктивно і неупереджено. З цією метою вони повинні залишатися вільними від будь-якого зовнішнього впливу, в тому числі прямого чи непрямого впливу держави або *федеральних земель*, а не лише органів, за діяльністю яких здійснюється нагляд».[200]

Суд ЄС також виявив, що значення терміну «повна незалежність» слід тлумачити із врахуванням незалежності ЄІЗПД, як це визначено у Регламенті інституцій ЄС щодо захисту персональних даних. Як підкреслив Суд, у статті 44 (2) регламенту надається роз'яснення поняття незалежності та додається, що при виконанні своїх обов'язків ЄІЗПД не може ані просити, ані отримувати інструкції від будь-кого. Це виключає нагляд держави за діяльністю незалежного органу із захисту персональних даних.[201]

Відповідно, Суд ЄС постановив, що німецькі інституції із захисту персональних даних на федеральному рівні держави, відповідальні за контроль за обробкою персональних даних недержавними органами, не були достатньо незалежними, оскільки знаходилися під наглядом з боку держави.

Приклад: У справі «*Європейська комісія проти Австрії*»[202] Суд ЄС вказав на подібні проблеми пов'язані з позицією окремих членів та співробітників Органу з питань захисту персональних даних Австрії (Комісії з питань захисту персональних даних, КЗПД). У цій справі Суд дійшов висновку, що австрійське законодавство перешкоджало Органу з питань захисту персональних даних Австрії виконувати свої функції в повній незалежності у розумінні Директиви про захист персональних даних. Незалежність КЗПД Австрії не було гарантовано в достатній мірі, тому що Федеральна канцелярія забезпечувала КЗПД персоналом, наглядала за нею і мала право у будь-який час отримати інформацію про її діяльність.

198 Там само, пп. 17 і 29.

199 Там само, п. 23.

200 Там само, п. 25.

201 Там само, п. 27.

202 Суд ЄС, C-614/10, «*Європейська комісія проти Республіки Австрія*», 16 жовтня 2012 р., пп. 59 і 63.

Приклад: У справі *«Європейська комісія проти Угорщини»*[203] Суд ЄС зазначив, що «вимога [...] щодо забезпечення того, щоб кожен наглядовий орган був здатний виконувати покладені на нього завдання у повній незалежності покладає на відповідну державу-члена зобов'язання дати можливість цьому органу відпрацювати повний термін своїх повноважень».

Суд також постановив, що «передчасно завершивши термін повноважень наглядового органу із захисту персональних даних, Угорщина не виконала свої зобов'язання за Директивою 95/46/ЕС [...].»

Відповідно до національного законодавства наглядові органи мають такі повноваження і можливості:[204]

- консультувати володільців і суб'єктів персональних даних з усіх питань захисту персональних даних;
- стежити за операціями з обробки даних та втручатися відповідним чином;
- виносити попередження або догану володільцям;
- видавати розпорядження про виправлення, блокування, стирання або знищення персональних даних;
- вводити тимчасову або остаточну заборону на обробку персональних даних;
- направляти матеріали у справі до суду.

Для здійснення своїх функцій наглядовий орган повинен мати доступ до всіх персональних даних та інформації, необхідної для розслідування, а також доступ до будь-яких приміщень, у яких володілець зберігає відповідну інформацію.

Між національними юрисдикціями існують значні відмінності в тому, що стосується процедур та юридичної сили висновків наглядового органу. Вони можуть варіюватися від рекомендацій, подібних до рекомендацій омбудсмена, до рішень, які мають негайно виконуватися. Тому при аналізі ефективності засобів правового захисту, доступних в рамках якоїсь юрисдикції, інструменти правового захисту повинні оцінюватися в їх контексті.

203 Суд ЄС, C-288/12, *«Європейська комісія проти Угорщини»*, 8 квітня 2014 р., пп. 50 і 67.

204 Директива про захист персональних даних, ст. 28; див. далі Конвенцію № 108, Додатковий протокол, ст. 1.

5.3. Засоби правового захисту та санкції

Ключові моменти

- Відповідно до Конвенції № 108 та Директиви про захист персональних даних національне законодавство повинно передбачати належні засоби правового захисту та санкції за порушення права на захист персональних даних.
  - Відповідно до законодавства ЄС право на ефективний засіб правового захисту вимагає, щоб національне законодавство встановлювало засоби правового захисту від порушень прав на захист персональних даних незалежно від можливості звернення до контролюючого органу.
  - Санкції повинні встановлюватися національним законодавством та бути ефективними, еквівалентними, пропорційними та стримуючими.
- Перш ніж передавати справи до судів, слід звертатися до володільця. Питання щодо того, чи перед зверненням до суду також обов'язково звертатися до наглядового органу, повинно регулюватися національним законодавством.
- Щодо порушень законодавства у сфері захисту персональних даних суб'єкти персональних даних можуть звертатися до ЄСПЛ як до останньої інстанції і за умови дотримання певних умов.
- Крім того, суб'єкти персональних даних можуть звертатися до Суду ЄС, але тільки в дуже обмежених випадках.

Права, передбачені законодавством у сфері захисту персональних даних, можуть здійснюватися лише особою, права якої знаходяться під загрозою; це може бути той, хто, принаймні, стверджує, що він є суб'єктом персональних даних. Таких осіб у здійсненні їх прав можуть представляти особи, які відповідають необхідним вимогам, передбаченим національним законодавством. Неповнолітніх повинні представляти їхні батьки або опікуни. У наглядовому органі особу також може представляти об'єднання осіб, законна мета якого полягає в підтримці прав на захист персональних даних.

5.3.1. Направлення запитів до володільця

Права, зазначені у Розділі 3.2, повинні дотримуватись передовсім володільцем. Звернення до національного наглядового органу або безпосередньо до суду не допоможе, оскільки такий орган може лише порадити спершу звернутися до володільця, а суд визнає заяву неприйнятною. Формальні вимоги до

юридично обґрунтованого запиту до володільця, особливо стосовно того, чи повинен цей запит подаватися у письмовій формі, мають регулюватися національним законодавством.

Особа, до якої звернулися як до володільця, повинна надати відповідь на запит, навіть якщо вона не є володільцем. У будь-якому випадку відповідь має надійти до суб'єкта персональних даних у терміни, визначені національним законодавством, навіть якщо у ній лише буде зазначено, що жодні дані запитувача не обробляються. Відповідно до положень статті 12 (a) Директиви про захист персональних даних та статті 8 (b) Конвенції № 108, запит повинен оброблятися «без надмірної затримки». Тому національне законодавство має визначати період для надання відповіді, який повинен бути досить коротким, але, тим не менш, дозволяти володільцю належним чином розглянути запит.

Перш ніж відповісти на запит, особа, до якої звернулися як до володільця, повинна встановити особу запитувача, щоб визначити, чи є він насправді тією особою, за яку він/вона себе видає, і таким чином уникнути серйозного порушення конфіденційності. Якщо вимоги щодо встановлення особи конкретно не регулюються національним законодавством, їх повинен визначити сам володілець. Принцип ретельної обробки персональних даних вимагає, щоб володільці не призначали надміру обтяжливих умов для підтвердження особистості (і автентичності запиту, про яку йде мова у Розділі 2.1.1).

Національне законодавство також має вирішувати питання про те, чи можуть володільці, перш ніж відповідати на запити, вимагати від запитувача сплатити комісію: стаття 12 (a) Директиви та стаття 8 (b) Конвенції № 108 передбачають, що відповідь на запити про надання доступу повинні надаватися «без надмірних [...] витрат». Національне законодавство багатьох європейських країн передбачає, що на запити, подані відповідно до законодавства у сфері захисту персональних даних, відповідь повинна надаватися безкоштовно за умови, що надання відповіді не потребує надмірних і незвичайних зусиль; у свою чергу, володільці є зазвичай захищеними національним законодавством від зловживання правом на отримання відповіді на запити.

Якщо особа, інституція або орган, до якої надійшло звернення як до володільця, не заперечує того, що вона є володільцем, у визначені національним законодавством терміни вона повинна:

- або задовольнити запит і повідомити запитувача про те, як було виконано його запит; або
- поінформувати запитувача про те, чому його запит буде відхилено.

5.3.2. Подання скарг до наглядового органу

Якщо після подання запиту на отримання доступу або висунення заперечення володільцю особа не отримує своєчасної і задовільної відповіді, ця особа може звернутися до національного наглядового органу з питань захисту персональних даних з проханням про допомогу. В ході розгляду питання наглядовим органом слід з'ясувати, чи була особа, установа або орган, до якої звернувся запитувач, дійсно зобов'язана відреагувати на запит та чи була ця реакція правильною і достатньою. Відповідна особа має бути поінформована наглядовим органом про результат розгляду її прохання.[205] Правові наслідки результатів розгляду питання національними наглядовими органами залежать від національного законодавства: чи можуть рішення наглядового органу виконуватися в законному порядку, що означає, що вони підлягають виконанню офіційним органом, та чи необхідно звернутися до суду, якщо володілець не виконує рішення (висновок, вказівку тощо) наглядового органу.

У разі, якщо права на захист персональних даних, які гарантує стаття 16 ДФЄС, як стверджується, було порушено інституціями або органами ЄС, суб'єкт персональних даних може подати скаргу до ЄІЗД,[206] незалежного наглядового органу з питань захисту персональних даних, відповідно до Регламенту інституцій ЄС щодо захисту персональних даних, у якому викладено обов'язки та повноваження ЄІЗД. За відсутності відповіді ЄІЗД протягом шести місяців скарга вважається такою, яку було відхилено.

Повинна існувати можливість звернення до суду для оскарження рішень національного наглядового органу. Це стосується суб'єкта персональних даних, а також володільців, які були сторонами у розгляді питання наглядовим органом.

Приклад: 24 липня 2013 року Інформаційний Комісар Сполученого Королівства видав постанову з вимогою до поліції графства Хартфордшир припинити використовувати систему розпізнавання автомобільних номерів, яку він вважав протизаконною. Дані, зібрані за допомогою камер, зберігалися як в локальних базах даних поліції, так і в централізованій базі даних. Фотографії номерних знаків зберігалися протягом двох років, а фотографії автомобілів – 90 днів. Вважалося, що таке широке використання камер та інших форм спостереження було непропорційним відносно проблеми, яку пропонувалось вирішити.

205 Директива про захист персональних даних, ст. 28 (4).

206 Регламент № 45/2001 Європейського парламенту та Ради (ЄС) від 18 грудня 2000 р. про захист фізичних осіб, що стосується обробки персональних даних установами і органами Спільноти і щодо вільного переміщення таких даних, OJ 2001 L 8.

5.3.3. Подання скарги до суду

Відповідно до Директиви про захист персональних даних у разі, якщо особа, подавши запит до володільця відповідно до законодавства у сфері захисту персональних даних, не задоволена відповіддю володільця, ця особа повинна мати право звернутись з оскарженням до національної судової інстанції.[207]

Питання щодо того, чи обов'язково перед зверненням до суду спершу звертатися до наглядового органу, повинно регулюватися національним законодавством. Однак у більшості випадків особам, які здійснюють свої права на захист персональних даних, буде доречно спочатку звернутися до наглядового органу, оскільки розгляд вимог щодо надання ними допомоги має бути не забюрократизованим та безоплатним. Експертна оцінка, задокументована у рішенні наглядового органу (висновку, вказівці тощо) також може допомогти суб'єкту персональних даних захищати свої права в судових інстанціях.

Відповідно до права РЄ порушення прав на захист персональних даних, які, як стверджується, були допущені на національному рівні Договірних Сторін ЄКПЛ та водночас становлять порушення статті 8 ЄКПЛ, можуть також бути оскаржені в ЄСПЛ після вичерпання усіх доступних національних засобів правового захисту. Заява до ЄСПЛ про порушення статті 8 ЄКПЛ також повинна відповідати іншим критеріям прийнятності (статті 34–37 ЄКПЛ).[208]

Хоча заяви до ЄСПЛ подаються лише проти Договірних Сторін, вони можуть також опосередковано стосуватися дій чи бездіяльності сторін-приватних осіб, з огляду на те, що Договірна Сторона не виконала свої позитивні зобов'язання за ЄКПЛ та не забезпечила у своєму національному законодавстві достатній рівень захисту від порушень прав на захист персональних даних.

Приклад: У справі «*К.Ю. проти Фінляндії*»[209] неповнолітній заявник скаржився, що на інтернет-сайті знайомств про нього було розміщено оголошення сексуального характеру. Постачальник послуг не розкрив йому відомості про особу, яка розмістила цю інформацію, через свої зобов'язання дотримуватися конфіденційності, накладені на нього законодавством Фінляндії. Заявник стверджував, що законодавство Фінляндії

207 Директива про захист персональних даних, ст. 22.

208 ЄКПЛ, ст. 34–37, доступно за посиланням: www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis&c=#n1347458601286_pointer.

209 ЄСПЛ, *К.У. проти Фінляндії*, № 2872/02, 2 грудня 2008 р.

не надавало достатній рівень захисту від таких дій приватної особи, яка розмістила в Інтернеті компромат про заявника. ЄСПЛ постановив, що держави не тільки мають утримуватися від довільного втручання в персональне життя осіб, але й можуть бути суб'єктами позитивних зобов'язань, які включають в себе «вжиття заходів, призначених гарантувати повагу до приватного життя навіть у сфері міжособистісних відносин». У справі заявника, його практичний й ефективний захист потребував здійснення ефективних кроків для виявлення порушника і притягнення його до відповідальності. Проте держава не надала такого захисту, і Суд дійшов висновку, що мало місце порушення статті 8 ЄКПЛ.

Приклад: У справі *«Кьопке проти Німеччини»*[210] заявницю підозрювали у здійсненні крадіжки на робочому місці, а тому за нею здійснювалося приховане відеоспостереження. ЄСПЛ вирішив, що «ніщо не вказувало на те, що національні органи влади не змогли в межах свого поля розсуду досягти справедливої рівноваги між правом заявниці на повагу до свого приватного життя, передбаченого статтею 8, та інтересом її роботодавця у захисті своїх майнових прав і державним інтересом у належному здійсненні правосуддя». Тому скаргу було визнано неприйнятною.

Якщо ЄСПЛ визнає, що держава-учасниця порушила будь-яке з прав, які захищає ЄКПЛ, ця держава-учасниця зобов'язана виконати рішення ЄСПЛ. Виконавчі заходи повинні передусім покласти край порушенню та виправити, наскільки це можливо, його негативні наслідки для заявника. Виконання рішень також може потребувати вжиття загальних заходів для запобігання порушенням, подібним до тих, які виявив Суд, шляхом внесення змін до законодавства, через судову практику чи інші заходи.

Стаття 41 ЄКПЛ передбачає, що в разі виявлення ЄСПЛ порушення ЄКПЛ він може присудити заявникові справедливу компенсацію за рахунок держави-учасниці.

Відповідно до права ЄС[211] жертви порушень національного законодавства у сфері захисту персональних даних, яке імплементує право ЄС у сфері захисту персональних даних, можуть в деяких випадках подати свої справи на

210 ЄСПЛ, *Кьопке проти Німеччини* (dec.), № 420/07, 5 жовтня 2010 р.

211 ЄС (2007), Лісабонський договір про внесення змін до Договору про Європейський Союз та Договору про заснування Європейського Співтовариства, підписаний у Лісабоні, 13 грудня 2007 р., OJ 2007 C 306. Див. також консолідовані версії Договору про Європейський Союз, OJ 2012 C 326, та Договору про функціонування Європейського Союзу, OJ 2012 C 326.

розгляд Суду ЄС. Існує два можливих сценарії того, як заява суб'єкта персональних даних про те, що його/її права на захист персональних даних було порушено, може призвести до провадження в Суді ЄС.

За першим сценарієм суб'єкт персональних даних повинен бути прямою жертвою адміністративного або нормативного акту ЄС, який порушує право особи на захист персональних даних. Відповідно до статті 263 (4) ДФЄС:

> *«будь-яка фізична чи юридична особа може [...]порушити провадження проти рішення, адресованого цій особі, або проти рішення, що стосується її безпосередньо та особисто, та проти нормативного акту, що стосується її безпосередньо та не призводить до виконавчих заходів.»*

Таким чином, жертви незаконної обробки персональних даних органом ЄС можуть звернутися безпосередньо до Загального суду, який є органом Суду ЄС, що має компетенцію виносити рішення в питаннях, які розглядаються у Регламенті інституцій ЄС щодо захисту персональних даних. Також існує можливість звернення безпосередньо до Суду ЄС, якщо правова норма ЄС безпосередньо впливає на чиєсь правове становище.

Другий сценарій стосується компетенції Суду ЄС (Суду) виносити преюдиціальні рішення відповідно статті 267 ДФЄС.

В ході провадження на національному рівні суб'єкти персональних даних можуть попросити національний суд запросити в Суду роз'яснення стосовно тлумачення Договорів ЄС та тлумачення і чинності актів інституцій, органів або агенцій ЄС. Такі роз'яснення відомі як преюдиціальні рішення. Вони не є безпосереднім засобом правового захисту для заявника, але дозволяють національним судам переконатися в тому, що вони застосовують правильне тлумачення права ЄС.

Якщо сторона в судовому процесі в національному суді просить передати питання на розгляд Суду ЄС, робити це зобов'язані лише ті національні суди, які діють в якості останньої інстанції та щодо рішень яких немає жодного засобу судового захисту.

Приклад: У справі *«Земельний уряд Карінтії та інші»*[212] Конституційний суд Австрії звернувся до Суду ЄС з питанням щодо правомірності ста-

212 Суд ЄС, Об'єднані справи C-293/12 і C-594/12, *«Компанія «Digital Rights Ireland» і Зайтлінгер та інші проти Ірландії»*, 8 квітня 2014 р.

тей 3–9 Директиви 2006/24/ЄС (*Директиви про збереження персональних даних*) з огляду на статті 7, 9 і 11 Хартії та щодо того, чи були деякі положення Федерального закону Австрії про телекомунікації, які транспонували Директиву про збереження персональних даних, несумісними з аспектами Директиви про захист персональних даних і Регламенту інституцій ЄС щодо захисту персональних даних.

Пан Зайтлінгер, один із заявників в ході провадження в Конституційному суді, заявляв, що використовує телефон, Інтернет та електронну пошту як для роботи, так і в приватному житті. В результаті інформація, яку він відправляв та отримував, проходила через суспільні телекомунікаційні мережі. Відповідно до Закону Австрії про телекомунікації 2003 року, його телекомунікаційний провайдер був юридично зобов'язаний збирати і зберігати дані про його користування мережею. Пан Зайтлінгер усвідомив, що це збирання та зберігання його персональних даних у жодному разі не було необхідним для технічних цілей відправлення інформації від пункту А до пункту Б в мережі. Насправді, збирання і зберігання цих даних не було навіть віддалено необхідним для виставлення рахунків. Звичайно, пан Зайтлінгер не погоджувався на таке використання його персональних даних. Єдиною підставою для збирання і зберігання усіх цих додаткових даних був Закон Австрії про телекомунікації 2003 року.

Тому пан Зайтлінгер подав позов до Конституційного суду Австрії, у якому він стверджував, що юридичні зобов'язання його телекомунікаційного провайдера порушували його основні права, гарантовані статтею 8 Хартії ЄС.

Суд ЄС приймає рішення тільки стосовно складових елементів направленого йому преюдиціального запиту. Національний суд залишається компетентним приймати рішення у початковій справі.

В принципі, Суд повинен дати відповідь на поставлені йому запитання. Він не може відмовитися приймати преюдиціальне рішення на тій підставі, що така відповідь не буде ані доречною, ані своєчасною для початкової справи. Він може, однак, відмовитися, якщо питання не входить до сфери його компетенції.

Нарешті, якщо права на захист персональних даних, які гарантує стаття 16 ДФЄС, були нібито порушені інституцією або органом ЄС в процесі обробки

персональних даних, суб'єкт персональних даних може подати скаргу до Загального суду Суду ЄС (стаття 32 (1) і (4) Регламенту інституцій ЄС щодо захисту персональних даних). Це ж стосується і рішень ЄІЗД стосовно таких порушень (стаття 32 (3) Регламенту інституцій ЄС щодо захисту персональних даних).

Хоча Загальний суд Суду ЄС є компетентним вирішувати питання, пов'язані з Регламентом інституцій ЄС щодо захисту персональних даних, якщо особа, яка є співробітником інституції або органу ЄС, добивається захисту в судовому порядку, вона повинна звернутися до Трибуналу цивільної служби ЄС.

Приклад: Справа *«Європейська комісія проти компанії «The Bavarian Lager Co. Ltd»*[213] ілюструє доступні засоби правового захисту від діяльності чи рішень інституцій та органів ЄС, пов'язаних із захистом персональних даних.

Компанія «The Bavarian Lager» запросила від Європейської комісії доступ до повного протоколу засідання, проведеного Комісією, яке, як стверджувалось, стосувалося правових питань, що мали відношення до цієї компанії. Комісія відхилила запит компанії на отримання доступу на підставі переважаючих інтересів захисту персональних даних.[214] Компанія «The Bavarian Lager» подала до Суду ЄС скаргу на це рішення на підставі статті 32 Регламенту інституцій ЄС щодо захисту персональних даних; точніше, до Суду першої інстанції Європейських Співтовариств (попередника Загального суду). У своєму рішенні у справі T-194/04 *«Компанія «The Bavarian Lager» проти Європейської комісії»* Суд першої інстанції скасував рішення Комісії про відхилення запиту на надання доступу. Європейська комісія подала апеляцію на це рішення до Суду ЄС. Суд виніс рішення (засідаючи Великою палатою), яке скасувало рішення Суду першої інстанції і підтвердило відмову Європейської комісії у запиті на надання доступу.

213 Суд ЄС, C-28/08 P, *«Європейська комісія проти компанії «The Bavarian Lager Co. Ltd»*, 29 червня 2010 р.

214 Для проведення аналізу аргументу, див.: ЄІЗД (2011), Публічний доступ до документів, що містять персональні дані, після прийняття рішення у справі *«The Bavarian Lager»*, Брюссель, ЄІЗД, доступно за посиланням: www.secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_ Lager_EN.pdf.

5.3.4. Санкції

Відповідно до права РЄ стаття 10 Конвенції № 108 передбачає, що кожна Сторона повинна встановити відповідні санкції та засоби правового захисту стосовно порушень положень національного права, які запроваджують основоположні принципи захисту персональних даних, визначені в Конвенції № 108.[215] **Відповідно до права ЄС** стаття 24 Директиви про захист персональних даних встановлює, що держави-члени «вживають відповідних заходів для забезпечення повного виконання положень даної Директиви і, зокрема, встановлюють санкції, що повинні накладатися у випадку порушення прийнятих положень [...]».

Обидва документи надають державам-членам широку свободу розсуду у виборі відповідних санкцій та засобів правового захисту. У жодному з правових документів не надаються конкретні вказівки стосовно характеру або типу відповідних санкцій; вони також не наводять приклади санкцій.

Однак:

> *«хоча держави-члени ЄС користуються полем розсуду у визначенні того, які заходи є найбільш придатними для забезпечення прав, що особи отримують від права ЄС, відповідно до принципу лояльного співробітництва, сформульованого в статті 4 (3) ДЄС, слід дотримуватися мінімальних вимог щодо ефективності, еквівалентності, пропорційності та переконливості»*[216]

Суд ЄС неодноразово стверджував, що національне законодавство не є повністю вільним у визначенні санкцій.

Приклад: У справі *«Фон Колсон і Каманн проти землі Північний Рейн-Вестфалія»*[217] Суд ЄС зазначив, що всі держави-члени, яким адресована Директива, зобов'язані вживати у своїх національних правових системах усіх необхідних заходів для забезпечення того, щоб вона була повністю ефек-

215 ЄСПЛ, *«I. проти Фінляндії»*, № 20511/03, 17 липня 2008 р.; ЄСПЛ, *«K.U. проти Фінляндії»*, № 2872/02, 2 грудня 2008 р.

216 АОП (2012), Висновок Агенції Європейського Союзу з питань основних прав стосовно запропонованого пакету реформ у сфері захисту персональних даних, 2/2012, Відень, 1 жовтня 2012 р., стор. 27.

217 Суд ЄС, C-14/83, *«Сабіне фон Колсон і Елізабет Каманн проти землі Північний Рейн-Вестфалія»*, 10 квітня 1984 р.

тивною та відповідала поставленій меті. Суд постановив, що, хоча держави-члени вільні вибрати шляхи та засоби забезпечення імплементації Директиви, ця свобода не впливає на покладені на них зобов'язання. Зокрема, ефективний засіб правового захисту повинен надавати індивіду можливість повною мірою добиватися права, про яке йде мова, та здійснювати його. Для досягнення цього справжнього та ефективного захисту засоби правового захисту повинні приводити в дію штрафні та/або компенсаційні процедури, що ведуть до санкцій, які мають стримувальну дію.

Стосовно санкцій за порушення права ЄС з боку інституцій або органів ЄС, у зв'язку зі спеціальною сферою застосування Регламенту інституцій ЄС щодо захисту персональних даних санкції передбачено тільки у вигляді дисциплінарного стягнення. Відповідно до статті 49 Регламенту, «будь-яке невиконання зобов'язань за цим Регламентом, навмисно чи з необережності, дозволить притягнути посадову особу або іншого службовця Європейських Співтовариств до дисциплінарної відповідальності [...]».

6 Транскордонний обмін персональними даними

ЄС	питання, що висвітлюються	РЄ
Транскордонна передача персональних даних		
Директива про захист персональних даних, стаття 25 (1) Суд ЄС, C-101/01, «*Bodil Lindqvist*», 6 листопада 2003 р.	**Визначення**	Конвенція № 108, Додатковий протокол, стаття 2 (1)
Вільна передача персональних даних		
Директива про захист персональних даних, стаття 1 (2)	**Між державами-членами ЄС**	
	Між Договірними Сторонами Конвенції № 108	Конвенція № 108, стаття 12 (2)
Директива про захист персональних даних, стаття 25	**Третім країнам, що забезпечують адекватний рівень захисту даних**	Конвенція № 108, Додатковий протокол, стаття 2 (1)
Директива про захист персональних даних, стаття 26 (1)	**Третім країнам в окремих випадках**	Конвенція № 108, Додатковий протокол, стаття 2 (2) (a)
Обмежена передача персональних даних		
Директива про захист персональних даних, стаття 26 (2) Директива про захист персональних даних, стаття 26 (4)	**Договірні умови**	Конвенція № 108, Додатковий протокол, стаття 2 (2) (b) Керівництво з підготовки договірних положень

ЄС	питання, що висвітлюються	РЄ
Директива про захист персональних даних, стаття 26 (2)	**Зобов'язальні корпоративні норми**	
Приклади: Угода між ЄС і США щодо записів реєстрації пасажирів (ЗРП) Угода між ЄС і США щодо системи SWIFT	**Спеціальні міжнародні угоди**	

Директива про захист персональних даних не лише передбачає вільну **передачу персональних даних** між державами-членами, але й містить положення стосовно вимог до передачі персональних даних третім країнам, які не є членами ЄС. РЄ також визнала важливість виконання норм щодо **передачі персональних** даних до третіх країн і в 2001 році прийняла Додатковий протокол до Конвенції № 108. В Протоколі відтворено найважливіші елементи регулювання пов'язаних із транскордонною передачею персональних даних від Сторін Конвенції і держав-членів ЄС.

6.1. Характер транскордонного обміну персональними даними

Ключовий момент

- Транскордонна передача персональних даних – це передача персональних даних одержувачу, який знаходиться під іноземною юрисдикцією.

Стаття 2 (1) Додаткового протоколу до Конвенції № 108 описує транскордонний передачу персональних даних як передачу персональних даних одержувачу, який знаходиться під іноземною юрисдикцією. Стаття 25 (1) Директиви про захист персональних даних регулює «передачу третій країні персональних даних, що проходять обробку чи призначені для проходження обробки після їх передачі [...]». Така передача персональних даних допускається тільки відповідно до правил, викладених у статті 2 Додаткового протоколу до Конвенції № 108, а для держав-членів ЄС – додатково в статтях 25 і 26 Директиви про захист персональних даних.

Приклад: У справі «*Боділ Ліндквіст*»[218] Суд ЄС постановив, що «операція, яка полягає у відсилці до Інтернет-сторінок різних осіб та ідентифікацію їх за прізвищем або в інший спосіб, наприклад, через вказування їхніх телефонних номерів або інформації про умови їхньої праці та хобі, становить «обробку персональних даних повністю або частково за допомогою автоматичних засобів» за змістом статті 3 (1) Директиви 95/46».

Потім Суд зазначив, що Директива також встановлює конкретні норми, покликані дозволити державам-членам контролювати передачу персональних даних третім країнам.

Однак враховуючи, по-перше, стан розвитку Інтернету на той час, коли розроблялася Директива, і, по-друге, відсутність у Директиві критеріїв, застосовних до користування Інтернетом, «ніхто не може припускати, що законодавчий орган Співтовариств мав намір поширити дію виразу «передача [даних] третій країні» на завантаження [...] даних на Інтернет-сторінку, навіть якщо ці дані стали таким чином доступними для осіб, що знаходяться в третіх країнах та володіють технічними засобами доступу до них.»

В іншому випадку, якщо Директива «тлумачилася таким чином, щоб означати, що передача персональних даних в третю країну здійснюється щоразу, коли персональні дані завантажуються на Інтернет-сторінку, передача даних обов'язково буде передачею всім третім країнам, де є технічні засоби, необхідні для доступу до Інтернету. Таким чином, передбачений [Директивою] особливий режим обов'язково став би режимом загального застосування відносно операцій в Інтернеті. Таким чином, якщо б Комісія виявила [...], що навіть одна з третіх країн не забезпечила адекватний рівень захисту, держави-члени були б зобов'язані запобігти розміщенню будь-яких персональних даних в Інтернеті.»

Принцип, згідно з яким сама лише публікація (персональних) даних не повинна вважатися транскордонною передачею персональних даних, застосовується також до інтерактивних публічних реєстрів або таких засобів масової інформації, як (електронні) газети і телебачення. Тільки повідомлення, спрямоване конкретним одержувачам, відповідає поняттю «транскордонна передача персональних даних».

218 Суд ЄС, C-101/01, «*Боділ Ліндквіст*», 6 листопада 2003 р., пп. 27, 68 і 69.

6.2. Вільний обмін персональними даними між державами-членами або між договірними сторонами

Ключовий момент

- Передача персональних даних іншій державі-члену Європейського економічного простору або іншій Договірній Стороні Конвенції № 108 повинна бути вільною від обмежень.

Відповідно до права РЄ згідно зі статтею 12 (2) Конвенції № 108 між Сторонами Конвенції повинен існувати вільний потік персональних даних. Національне законодавство не може обмежувати експорт персональних даних Договірній Стороні крім випадків, коли:

- цього вимагає особливий характер даних;[219] або
- обмеження необхідне для уникнення обходу внутрішніх правових положень щодо транскордонної передачі персональних даних третім особам.[220]

Відповідно до права ЄС обмеження або заборона вільного обміну персональними даними між державами-членами з міркувань захисту персональних даних забороняються статтею 1 (2) Директиви про захист персональних даних. Зону вільного обміну персональними даними було розширено Угодою про створення Європейського економічного простору (ЄЕП),[221] яка включила Ісландію, Ліхтенштейн і Норвегію у внутрішній ринок.

Приклад: Якщо філія міжнародної групи компаній, заснованих у декількох державах-членах ЄС, до яких відносяться Словенія та Франція, передає персональні дані зі Словенії до Франції, передача таких даних не повинна обмежуватися або заборонятися національним законодавством Словенії.

219 Конвенція № 108, ст. 12 (3) (a).

220 Там само, ст. 12 (3) (b).

221 Рішення Ради (ЄС) та Європейської комісії від 13 грудня 1993 року про укладення Угоди про Європейський економічний простір між Європейськими Співтовариствами, їх державами-членами і Республікою Австрія, Фінляндською Республікою, Князівством Ліхтенштейн, Королівством Норвегія, Королівством Швеція і Швейцарською Конфедерацією, OJ 1994 L 1.

Проте якщо та ж словенська філія бажає передати ті ж персональні дані материнській компанії у США, словенський експортер даних повинен пройти процедуру, передбачену законодавством Словенії щодо транскордонної передачі персональних даних до третіх країн, які не забезпечують адекватний рівень захисту персональних даних, якщо тільки материнська компанія не приєдналася до принципів конфіденційності «Safe Harbor» («Безпечна гавань»), добровільного кодексу поведінки для забезпечення адекватного рівня захисту даних (див. підрозділ 6.3.1).

Транскордонна передача персональних даних до держав-членів ЄЕП у цілях, що знаходяться поза компетенцією внутрішнього ринку, наприклад, для розслідування злочинів, не підпадає, однак, під положення Директиви про захист персональних даних, а тому не підпадає під дію принципу вільного обміну персональними даними. Що ж до права РЄ, то в рамки Конвенції № 108 і Додаткового протоколу до Конвенції № 108 включено всі сфери, хоча Договірні Сторони можуть передбачати виключення. Усі держави ЄЕП також є Сторонами Конвенції № 108.

6.3. Вільний обмін персональними даними з третіми країнами

Ключові моменти

- Передача персональних даних третім країнам є вільною від обмежень, передбачених національним законодавством у сфері захисту персональних даних, якщо:
  - адекватність рівня захисту персональних даних з боку одержувача було підтверджено; або
  - вона є необхідною в конкретних інтересах суб'єкта персональних даних або законних переважних інтересах інших осіб, особливо у важливих суспільних інтересах.
- Адекватність рівня захисту персональних даних у третій країні означає, що основні принципи захисту персональних даних було ефективно імплементовано в національне законодавство цієї країни.
- Відповідно до права ЄС адекватність рівня захисту персональних даних у третій країні оцінюється Європейською комісією. Відповідно до права РЄ спосіб оцінювання адекватності рівня захисту персональних даних повинен регулюватися національним законодавством.

6.3.1. Вільний обмін персональними даними за умови адекватного рівня захисту

Право РЄ допускає, щоб національне законодавство дозволяло вільну передачу персональних даних до держав, які не є сторонами Конвенції у випадку, якщо держава або організація, що одержує ці дані, забезпечує адекватний рівень захисту для цільової передачі персональних даних.[222] Спосіб оцінки рівня захисту персональних даних в іншій країні та встановлення особи, яка має це робити, визначається у національному законодавстві.

Відповідно до права ЄС вільна передача персональних даних до третіх країн з адекватним рівнем захисту персональних даних передбачена статтею 25 (1) Директиви про захист персональних даних. Вимога щодо адекватності рівня захисту, а не еквівалентності, уможливлює застосування різних способів реалізації захисту персональних даних. Згідно зі статтею 25 (6) Директиви Європейська комісія компетентна оцінювати рівень захисту персональних даних в зарубіжних країнах через висновки про адекватність рівня захисту та проведення консультацій стосовно оцінювання з Робочою групою «Стаття 29», яка зробила суттєвий внесок у тлумачення статей 25 і 26.[223]

Висновки Європейської комісії щодо адекватності рівня захисту мають силу правових зобов'язань. Якщо Європейська комісія публікує в *Офіційному журналі Європейського Союзу* висновок щодо адекватності рівня захисту певної країни, усі країни-члени ЄЕП і їх органи зобов'язані слідувати цьому висновку, а це означає, що дані можуть надходити до цієї країни без перевірки або проходження процедури ліцензування в національних органах.[224]

Європейська комісія також здатна оцінити окремі частини правової системи країни чи обмежитися окремими темами. Наприклад, Комісія зробила висновок щодо адекватності рівня захисту, що стосується виключно приватного ко-

222 Конвенція № 108, Додатковий протокол, ст. 2 (1).

223 Див., наприклад, Робоча група статті 29 (2003), Робочий документ стосовно передачі персональних даних третім країнам: застосування статті 26 (2) Директиви ЄС про захист персональних даних до зобов'язальних корпоративних норм міжнародної передачі даних, WP 74, Брюссель, 3 червня 2003 р.; і Робоча група статті 29 (2005), Робочий документ стосовно спільного тлумачення статті 26 (1) Директиви 95/46/ЕС від 24 жовтня 1995 р., WP 114, Брюссель, 25 листопада 2005 р.

224 Для перегляду списку (постійно оновлюється) країн, які одержали висновок щодо адекватності рівня захисту, див. домашню сторінку Європейської комісії, Генеральний директорат з питань юстиції, доступно за посиланням: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

мерційного права Канади.[225] Також існує декілька висновків щодо адекватного рівня захисту передачі персональних даних, що базуються на угодах між ЄС та зарубіжними державами. Ці рішення стосуються виключно одного типу передачі даних, наприклад, передачі записів реєстрації пасажирів на авіалініях іноземним органам прикордонного контролю, коли авіакомпанія літає з ЄС у напрямку певних зарубіжних країн (див. підрозділ 6.4.3). Найостанніша практика передачі даних на основі спеціальних угод між ЄС і третіми країнами здебільшого відміняє необхідність прийняття висновків щодо адекватності рівня захисту, припускаючи, що сама угода надає адекватний рівень захисту даних.[226]

Один з найважливіших висновків щодо адекватності рівня захисту фактично не стосується набору правових положень.[227] Він радше стосується норм, які більш схожі на кодекс поведінки, відомих як Принципи конфіденційності «Safe Harbor» («Безпечна гавань»). Ці принципи були розроблені ЄС і США для американських комерційних організацій. Членство в «Безпечній гавані» досягається через добровільне зобов'язання, проголошене у Міністерстві торгівлі США та засвідчене у списку, який публікує це міністерство. В якості одного з важливих елементів адекватності є ефективність реалізації захисту даних. Угода «Безпечна гавань» також передбачає певний ступінь державного нагляду: до «Безпечної гавані» можуть приєднатися лише ті компанії, які знаходяться під наглядом Федеральної торгової комісії США.

6.3.2. Вільний обмін персональними даними в особливих випадках

Відповідно до права РЄ стаття 2 (2) Додаткового протоколу до Конвенції № 108 дозволяє передачу персональних даних третім країнам, які не забезпе-

225 Європейська комісія (2002), Рішення № 2002/2/ЕС від 20 грудня 2001 року, прийняте відповідно до Директиви 95/46/ЕС Європейського парламенту і Ради (ЄС), щодо адекватного рівня захисту персональних даних, передбаченого Актом про захист персональної інформації та електронних документів Канади, OJ 2002 L 2.

226 Наприклад, Угода між Сполученими Штатами Америки та Європейським Союзом щодо використання і передачі записів реєстрації пасажирів Міністерству національної безпеки Сполучених Штатів (OJ 2012 L 215, стор. 5–14) або Угода між Європейським Союзом та Сполученими Штатами Америки щодо обробки і передачі Європейським Союзом Сполученим Штатам даних про фінансові повідомлення у цілях Програми відслідковування фінансування тероризму, OJ 2010 L 8, стор. 11–16.

227 Європейська комісія (2000), Рішення Європейської комісії № 2000/520/ЕС від 26 липня 2000 року, прийняте відповідно до Директиви 95/46/ЕС Європейського парламенту і Ради (ЄС), щодо захисту, передбаченого принципами конфіденційності «Safe Harbor», та пов'язаних з ними типових питань, виданих Міністерством торгівлі США, OJ 2000 L 215.

чують адекватного рівня захисту даних, за умови, що така передача передбачається національним законодавством і є необхідною для:

- особливих інтересів суб'єкта персональних даних; або
- законних переважаючих інтересів інших осіб, особливо важливих суспільних інтересів.

Відповідно до права ЄС стаття 26 (1) Директиви про захист персональних даних містить положення подібні до тих, що містяться в Додатковому протоколі до Конвенції № 108.

Відповідно до Директиви, інтереси суб'єкта персональних даних можуть виправдовувати вільний **обмін персональними даними** з третьою країною, якщо:

- суб'єкт персональних даних надав недвозначну згоду на експорт даних; або
- суб'єкт персональних даних встановлює чи готується встановити договірні відносини, які чітко вимагають, щоб дані передавалися одержувачу за кордон; або
- в інтересах суб'єкта персональних даних був укладений договір між володільцем персональних даних і третьою стороною; або
- передача є необхідною для захисту життєво важливих інтересів суб'єкта персональних даних.
- дані передаються з державних реєстрів; це є прикладом переважаючих інтересів у тому, щоб громадськість мала можливість отримати доступ до інформації, що зберігається в державних реєстрах.

Законні інтереси інших осіб можуть виправдовувати вільну транскордонну передачу персональних даних:[228]

- внаслідок існування важливого суспільного інтересу, крім питань національної або державної безпеки, оскільки на них не поширюється Директива про захист персональних даних; або
- задля встановлення, здійснення або захисту законних вимог.

Випадки, згадані вище, слід зрозуміти як виключення з правила, згідно з яким вільна передача персональних даних до інших країн вимагає забезпечення країною-одержувачем адекватного рівня захисту даних. Винятки за-

228 Директива про захист персональних даних, ст. 26 (1) (d).

вжди повинні тлумачитися в обмежувальний спосіб. Робоча група «Стаття 29» неодноразово підкреслювала це в контексті статті 26 (1) Директиви про захист персональних даних, особливо якщо підставою для передачі персональних даних представлена згода.[229] Робоча група «Стаття 29» дійшла висновку, що загальні норми стосовно правового значення згоди також є застосовними до статті 26 (1) Директиви. Якщо в контексті трудових відносин, наприклад, незрозуміло, що згода, надана працівниками, була справді вільною, то передача персональних даних не може бути заснована на статті 26 (1) (a) Директиви. У таких випадках застосовуватиметься стаття 26 (2), яка вимагає від національних органів з питань захисту персональних даних видавати ліцензії для передачі персональних даних.

6.4. Обмеження передачі персональних даних до третіх країн

Ключові моменти

- Перед передачею персональних даних до третіх країн, які не забезпечують адекватний рівень захисту персональних даних, володілець може бути зобов'язаний надати запланований до передачі потік даних для оцінки до наглядового органу.
- Під час цієї перевірки володілець, який бажає експортувати дані, повинен продемонструвати два моменти:
  - що існує правова основа для передачі даних одержувачу; і
  - що одержувач вживає усіх заходів, щоб гарантувати адекватний рівень захисту персональних даних.
- Заходи для встановлення одержувачем адекватного рівня захисту даних можуть включати:
  - договірні умови між володільцем, який експортує персональні дані, та іноземним одержувачем даних; або
  - зобов'язальні корпоративні норми, які зазвичай застосовуються для передачі даних в межах міжнародної групи компаній.
- Передача даних органам влади зарубіжних країн також може регулюватися спеціальною міжнародною угодою.

229 Див., зокрема, Робоча група статті 29 (2005), Робочий документ стосовно спільного тлумачення статті 26 (1) Директиви 95/46/ЕС від 24 жовтня 1995 р., WP 114, Брюссель, 25 листопада 2005 р.

Директива про захист персональних даних та Додатковий протокол до Конвенції № 108 допускають, щоб національне законодавство встановлювало режими для транскордонної передачі персональних даних у треті країни, які не забезпечують адекватний рівень захисту даних, за умови, що володілець досягнув особливих домовленостей для гарантування одержувачем адекватного рівня захисту даних і що володілець може довести це компетентному органу. Ця вимога чітко зазначена лише в Додатковому протоколі до Конвенції № 108; проте відповідно до Директиви про захист персональних даних вона також вважається стандартною процедурою.

6.4.1. Договірні умови

Як у **праві РЄ**, так і в **праві ЄС** умови договору між володільцем, що експортує дані, та одержувачем у третій країні зазначаються в якості можливого засобу гарантування одержувачем достатнього рівня захисту персональних даних.

На **рівні ЄС** Європейська комісія з допомогою Робочої групи «Стаття 29» розробила стандартні договірні умови, які були офіційно засвідчені Рішенням Комісії як доказ адекватного рівня захисту персональних даних.[230] Оскільки рішення Комісії є обов'язковими для держав-членів у повному обсязі, національні органи, які відповідають за контроль за транскордонними потоками даних, повинні підтверджувати ці стандартні договірні умови у своїх процедурах.[231] Таким чином, якщо володілець, що експортує дані, та одержувач у третій країни домовляються і підписують ці умови, це має надати наглядовому органу достатні докази того, що гарантії адекватного рівня захисту реально діють.

Існування стандартних договірних умов у нормативній базі ЄС не забороняє володільцям формулювати інші договірні умови *ad hoc*. Вони, однак, повинні забезпечувати такий самий рівень захисту, який забезпечують стандартні договірні умови. Найважливішими характеристиками стандартних договірних умов є:

- пункт, що визначає бенефіціара третьої сторони, який дозволяє суб'єктам персональних даних здійснювати свої договірні права, навіть якщо вони не є стороною договору;
- одержувач даних або імпортер, який погоджується пройти процедуру в національному наглядовому органі володільця, що експортує дані, і/або в суді у разі виникнення спору.

230 Директива про захист персональних даних, ст. 26 (4).

231 ДФЄС, ст. 288.

Наразі доступні два набори стандартних умов передачі даних від володільця до володільця, один з яких може вибрати володілець, що експортує дані.[232] Для передачі даних від володільця або розпорядника існує тільки один набір стандартних договірних умов.[233]

В контексті **права РЄ** Консультативний комітет Конвенції № 108 розробив керівництво з підготовки договірних умов.[234]

6.4.2. Зобов'язальні корпоративні норми

Багатосторонні Зобов'язальні корпоративні норми (ЗКН) дуже часто зачіпають одночасно декілька європейських органів з питань захисту персональних даних.[235] Для затвердження ЗКН проект ЗКН разом зі стандартними бланками заявки слід надіслати до керівного органу.[236] Керівний орган може бути ідентифікованим за стандартним бланком заявки. Потім цей орган інформує усі наглядові органи країн-членів ЄЕП, у яких розташовані філії групи, хоча їх участь в процесі оцінки ЗКН є добровільною. Хоча це не обов'язково, усім відповідним органам з питань захисту персональних даних слід включити результат оцінки у свої формальні процедури ліцензування.

232 Набір I міститься у Додатку до: Європейська комісія (2001), Рішення Європейської комісії № 2001/497/ЕС від 15 червня 2001 року щодо стандартних договірних умов передачі персональних даних третім країнам, прийнятого відповідно до Директиви 95/46/ЕС, OJ 2001 L 181; набір II міститься у Додатку до: Європейська комісія (2004), Рішення Європейської комісії № 2004/915/ЕС від 27 грудня 2004 року, про внесення змін до Рішення № 2001/497/ЕС стосовно впровадження альтернативного набору стандартних договірних умов передачі персональних даних третім країнам, OJ 2004 L 385.

233 Європейська комісія (2010), Рішення Європейської комісії № 2010/87 від 5 лютого 2010 року щодо стандартних договірних умов передачі персональних даних операторам з обробки даних, розташованих у третіх країнах, прийняте відповідно до Директиви 95/46/ЕС Європейського парламенту і Ради (ЄС), OJ 2010 L 39.

234 РЄ, Консультативний комітет Конвенції № 108 (2002), Керівництво з підготовки договірних умов, що регулюють захист даних під час передачі персональних даних третім особам, не зобов'язаним забезпечувати адекватний рівень захисту даних.

235 Зміст та структуру відповідних зобов'язальних корпоративних норм пояснено в документах: Робоча група статті 29 (2008), Робочий документ, що закладає основу структури Зобов'язальних корпоративних норм, WP 154, Брюссель, 24 червня 2008 р.; і Робоча група статті 29 (2008), Робочий документ, у якому наведено таблицю елементів та принципів, що містяться у Зобов'язальних корпоративних нормах, WP 153, Брюссель, 24 червня 2008 р.

236 Робоча група статті 29 (2007), Рекомендація № 1/2007 щодо стандартної заявки на затвердження Зобов'язальних корпоративних норм щодо передачі персональних даних, WP 133, Брюссель, 10 січня 2007 р.

6.4.3. Спеціальні міжнародні угоди

ЄС уклав спеціальні угоди стосовно двох типів передачі персональних даних:

Записи реєстрації пасажирів

Записи реєстрації пасажирів (PNR; ЗРП) збираються авіаперевізниками в процесі резервування та містять прізвища, адреси, дані кредитних карток та номери посадкових місць авіапасажирів. Відповідно до законодавства Сполучених Штатів (США) компанії-авіаперевізники зобов'язані надавати Міністерству національної безпеки США доступ до цих даних перед відльотом пасажирів. Це стосується і рейсів до або зі США.

Для забезпечення адекватного рівня захисту даних ЗРП в 2004 році відповідно до положень Директиви 95/46/ЕС був прийнятий «пакет ЗРП».[237] Пакет включав в себе пункт про адекватність обробки даних, яку проводить Міністерство національної безпеки США.

Після того, як Суд ЄС скасував «пакет ЗРП»,[238] ЄС і Сполучені Штати підписали дві окремі угоди з подвійною метою: по-перше, щоб забезпечити правову основу для розкриття даних ЗРП органам влади США, а по-друге – встановити адекватний рівень захисту даних у країні-одержувачі.

Перша угода, яку було підписано в 2012 році та яка стосувалася того, як країни ЄС і США повинні здійснювати обмін та управління даними, мала декілька недоліків; того ж року для кращого забезпечення правової визначеності її замінила інша угода.[239] Нова угода пропонує значні поліпшення. Вона обмежує та уточнює цілі, у яких може використовуватися інфор-

237 Рішення Ради (ЄС) № 2004/496/ЕС від 17 травня 2004 року про укладення Угоди між Європейським Співтовариством і Сполученими Штатами Америки щодо обробки і передачі авіаперевізниками даних ЗРП Міністерству національної безпеки Сполучених Штатів і Бюро митного та прикордонного контролю, OJ 2004 L 183, стор. 83; і Рішення Європейської комісії № 2004/535/ЕС від 14 травня 2004 року щодо адекватного рівня захисту персональних даних, що містяться і Записах реєстрації пасажирів літаків, які передаються Бюро митного та прикордонного контролю Сполучених Штатів, OJ 2004 L 235, стор. 11–22.

238 Суд ЄС, об'єднані справи C-317/04 і C-318/04, *«Європейський парламент проти Ради Європейського Союзу»*, 30 травня 2006 р., пп. 57, 58 і 59, у яких Суд постановив, що як адекватний рівень захисту, так і угода, пов'язана з обробкою даних, виключаються зі сфери застосування Директиви.

239 Рішення Ради (ЄС) № 2012/472/EU від 26 квітня 2012 року про укладення Угоди між Сполученими Штатами Америки та Європейським Союзом щодо використання і передачі Записів реєстрації пасажирів Міністерству національної безпеки Сполучених Штатів, OJ 2012 L 215/4. Текст Угоди додається до цього Рішення, OJ 2012 L 215, стор. 5–14.

мація, наприклад, тяжкі транснаціональні злочини та тероризм, і визначає термін, протягом якого можуть зберігатися дані: через шість місяців дані повинні бути знеособлені та замасковані. Відповідно до законодавства США кожен має право на відшкодування в адміністративному та судовому порядку, якщо його дані були використані неналежним чином. Також кожен має право на доступ до власних даних ЗРП і можливість вимагати від Міністерства національної безпеки США виправити, а також стерти їх, якщо інформація є неточною.

Угода, яка набула чинності 1 липня 2012 року, залишатиметься чинною протягом семи років, до 2019 року.

У грудні 2011 року Рада Європейського Союзу схвалила укладення оновленої Угоди між ЄС та Австралією щодо обробки та передачі даних ЗРП.[240] Угода між ЄС та Австралією стосовно даних ЗРП є ще одним кроком на порядку денному ЄС, до якого входять глобальні керівні принципи ЗРП[241], створення порядку використання ЗРП в ЄС[242] і переговори про укладення угод з третіми країнами.[243]

Дані щодо передачі фінансових повідомлень

Міжнародна міжбанківська система передачі інформації та здійснення платежів (SWIFT), яка розташована в Бельгії та є оператором з обробки даних більшості глобальних грошових переказів європейських банків, співпрацювала з дзеркальним центром у США і зіткнулася з проханням розкри-

240 Рішення Ради (ЄС) № 2012/381/EU від 13 грудня 2011 року про укладення Угоди між Європейським Союзом та Австралією щодо обробки та передачі авіаперевізниками даних Записів реєстрації пасажирів (ЗРП) Австралійській митній службі та службі прикордонного контролю, OJ 2012 L 186/3. Текст Угоди, яка замінила попередню угоду 2008 року, додається до Рішення, OJ 2012 L 186, стор. 4–16.

241 Див., зокрема, Комюніке Європейської комісії від 21 вересня 2010 року щодо глобального підходу до передачі даних Записів реєстрації пасажирів (ЗРП) третім країнам, COM(2010) 492 остаточна версія, Брюссель, 21 вересня 2010 р. Див. також: Робоча група статті 29 (2010), Висновок № 7/2010 стосовно Комюніке Європейської комісії щодо глобального підходу до передачі даних Записів реєстрації пасажирів (ЗРП) третім країнам, WP 178, Брюссель, 12 листопада 2010 р.

242 Пропозиція до Директиви Європейського парламенту і Ради (ЄС) щодо використання даних ЗРП для запобігання, виявлення, розслідування та судового переслідування терористичної діяльності й тяжких злочинів, COM(2011) 32 остаточна версія, Брюссель, 2 лютого 2011 р. У квітні 2011 року Європейський парламент звернувся до АОП з проханням надати висновок щодо цієї Пропозиції та її відповідності Хартії основних прав Європейського Союзу. Див.: АОП (2011), Висновок № 1/2011 – Записи реєстрації пасажирів, Відень, 14 червня 2011 р.

243 ЄС веде переговори з Канадою про нову угоду щодо ЗРП, яка замінить чинну угоду 2006 року.

ти дані Міністерству фінансів США для цілей проведення розслідування тероризму.[244]

З точки зору ЄС, для розкриття цих в основному європейських даних, які були доступними у Сполучених Штатах тільки тому, що там розташовувався один з центрів обробки даних системи SWIFT, не було достатньої правової основи.

В 2010 році з метою зумовити необхідну правову основу і забезпечити адекватний рівень захисту даних між ЄС і США було укладено спеціальну угоду, відому як «SWIFT-угода».[245]

В рамках цієї угоди фінансові дані, що зберігаються системою SWIFT, продовжують надаватися Міністерству фінансів США з метою запобігання, розслідування, виявлення, або переслідування тероризму та його фінансування. Міністерство фінансів США може запросити в системи SWIFT надати йому фінансові дані за умови, що цей запит:

- якомога чіткіше ідентифікує фінансові дані;
- чітко обґрунтовує необхідність цих даних;
- сформульований якомога докладніше, щоб звести до мінімуму обсяг запитуваних даних;
- не вимагає жодних даних стосовно Єдиної європейської платіжної системи (SEPA; ЄЄПС).

Європол повинен отримувати копію кожного запиту Міністерства фінансів США і перевіряти, чи дотримано у ньому принципів SWIFT-угоди.[246] Якщо підтвердиться, що їх було дотримано, система SWIFT повинна надати фінансові дані безпосередньо Міністерству фінансів США. Міністерство має зберігати

244 Див. у зв'язку з цим: Робоча група статті 29 (2011), Висновок № 14/2011 щодо питань захисту даних, пов'язаних із запобіганням відмиванню грошей і фінансуванню тероризму, WP 186, Брюссель, 13 червня 2011 р.; Робоча група статті 29 (2006), Висновок № 10/2006 щодо обробки персональних даних Міжнародною міжбанківською системою передачі інформації та здійснення платежів (SWIFT), WP 128, Брюссель, 22 листопада 2006 р.; Комісія із захисту недоторканності приватного життя Бельгії (2008), «Процедура контролю та рекомендування, ініційована відносно компанії «SWIFT», Рішення, 9 грудня 2008 р.

245 Рішення Ради (ЄС) № 2010/412/EU від 13 липня 2010 року про укладення Угоди між Європейським Союзом та Сполученими Штатами Америки щодо обробки і передачі Європейським Союзом Сполученим Штатам даних про фінансові повідомлення у цілях Програми відслідковування фінансування тероризму, OJ 2010 L 195, стор. 3 і 4. Текст Угоди додається до цього Рішення, OJ 2010 L 195, стор. 5–14.

246 Об'єднаний наглядовий орган Європолу провів аудит такої діяльності Європолу, результати якого доступні за посиланням: http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en.

фінансові дані у захищеному фізичному середовищі, де вони будуть доступними лише аналітикам, які розслідують тероризм або його фінансування; фінансові дані не повинні бути поєднані з будь-якими іншими базами даних. В цілому, фінансові дані, отримані від системи SWIFT, повинні видалятися не пізніше, ніж через п'ять років з моменту їх отримання. Фінансові дані, які мають відношення до конкретних розслідувань або судових переслідувань, можуть зберігатися до тих пір, поки вони є необхідними для цих розслідувань або судових переслідувань.

Міністерство фінансів США може передавати інформацію про дані, отримані від системи SWIFT, конкретним правоохоронним органам, органам державної безпеки або боротьби з тероризмом в межах чи за межами Сполучених Штатів виключно з метою розслідування, виявлення, запобігання чи судового переслідування тероризму та його фінансування. Якщо подальша передача фінансових даних стосується громадянина або резидента держави-члена ЄС, будь-який обмін даними з органами влади третьої країни вимагає попередньої згоди компетентних органів відповідної держави-члена. Винятки можуть бути зроблені, якщо обмін даними є важливим для запобігання безпосередній і серйозній загрозі державній безпеці.

За дотриманням принципів SWIFT-угоди стежать незалежні наглядачі, в тому числі особа, призначена Європейською комісією.

Суб'єкти персональних даних мають право отримувати від компетентного органу ЄС з питань захисту даних підтвердження того, що їх права на захист персональних даних було дотримано. Відповідно до SWIFT-угоди, суб'єкти персональних даних також мають право на виправлення, стирання чи блокування своїх даних, які зібрало та зберігає Міністерство фінансів США. Проте право суб'єктів персональних даних на доступ може підлягати певним правовим обмеженням. Якщо суб'єкту персональних даних було відмовлено у доступі, його має бути проінформовано в письмовій формі про відмову та про його право на відшкодування в адміністративному і судовому порядку в Сполучених Штатах.

SWIFT-угода залишатиметься чинною протягом п'яти років, до серпня 2015 року. Надалі вона щоразу автоматично продовжуватиметься на один рік, якщо одна із сторін принаймні за шість місяців не повідомить іншу про свій намір не продовжувати угоду.

7

Захист персональних даних у контексті діяльності поліції та кримінального судочинства

ЄС	питання, що висвітлюються	РЄ
	Загальні	Конвенція № 108
	Поліція	Рекомендація щодо використання персональних даних поліцією
		ЄСПЛ, *«Б.Б. проти Франції»*, № 5335/06, 17 грудня 2009 р. ЄСПЛ, *«С. і Марпер проти Сполученого Королівства»*, № 30562/04 і 30566/04, 4 грудня 2008 р. ЄСПЛ, *«Веттер проти Франції»*, №59842/00, 31 травня 2005 р.
	Кіберзлочинність	Конвенція про кіберзлочинність
Захист даних в контексті транскордонного співробітництва поліції і судових органів		
Рамкове рішення про захист персональних даних	**Загальні**	Конвенція № 108 Рекомендація щодо використання персональних даних поліцією
Прюмське рішення	**Спеціальні дані: відбитки пальців, ДНК, хуліганство тощо.**	Конвенція № 108 Рекомендація щодо використання персональних даних поліцією
Рішення про Європол Рішення про Євроюст Регламент щодо Фронтексу	**Спеціальні агенції**	Конвенція № 108 Рекомендація щодо використання персональних даних поліцією

ЄС	питання, що висвітлюються	РЄ
Рішення про ШІС II	**Спеціальні спільні інформаційні системи**	Конвенція № 108
Регламент ВІС		Рекомендація щодо використання
Регламент щодо системи		персональних даних поліцією
Eurodac		ЄСПЛ, *«Даля проти Франції»*,
Рішення про МІС		№ 964/07, 2 лютого 2010 р.

Щоб збалансувати інтереси індивіда у захисті персональних даних та суспільні інтереси у збиранні даних заради боротьби зі злочинністю й забезпеченні національної і державної безпеки, РЄ і ЄС прийняли окремі правові документи.

7.1. Право РЄ щодо захисту персональних даних у сфері діяльності поліції та кримінального судочинства

Ключові моменти

- Конвенція № 108 і Рекомендація щодо використання персональних даних поліцією охоплюють усі сфери діяльності поліції.
- Конвенція про кіберзлочинність (Будапештська конвенція) є зобов'язальним міжнародно-правовим документом, що стосується боротьби із злочинами, вчиненими проти і за допомогою електронних мереж.

На європейському рівні Конвенція № 108 охоплює усі сфери обробки персональних даних, а її положення призначені для регулювання обробки персональних даних в цілому. Отже, Конвенція № 108 застосовується до захисту персональних даних у сфері діяльності поліції та кримінального судочинства, хоча договірні сторони можуть обмежити її застосування.

Правові завдання поліції та органів кримінального судочинства часто вимагають обробки персональних даних, яка може спричинити серйозні наслідки для відповідних осіб. Рекомендація щодо використання персональних даних поліцією, прийнята Радою Європи в 1987 році, надає договірним Сторонам по-

ради щодо того, як їм слід вводити в дію принципи Конвенції № 108 в контексті обробки персональних даних поліцейськими органами.[247]

7.1.1. Рекомендація щодо використання персональних даних поліцією

ЄСПЛ неодноразово постановляв, що збирання та зберігання персональних даних поліцією або органами національної безпеки становить втручання у право, гарантоване статтею 8 (1) ЄКПЛ. Багато ухвал ЄСПЛ стосуються виправдання такого втручання.[248]

Приклад: У справі *«Б.Б. проти Франції»*[249] ЄСПЛ вирішив, що включення особи, засудженої за вчинення статевого злочину, до національної бази даних судових рішень підпадало під дію статті 8 ЄКПЛ. Однак враховуючи, що були реалізовані достатні гарантії захисту даних, такі, як право суб'єкта персональних даних звертатись із запитом про вилучення таких даних, обмеженість терміну зберігання даних і обмежений доступ до них, між конкуруючими приватними та суспільними інтересами було дотримано справедливого балансу. Суд дійшов висновку, що порушення статті 8 ЄКПЛ не було.

Приклад: У справі *«С. і Марпер проти Сполученого Королівства»*[250] обох заявників було обвинувачено у вчиненні кримінальних правопорушень, але не було засуджено. Проте поліція утримувала і зберігала їхні відбитки пальців, профілі ДНК та клітинні зразки. Необмежене зберігання біометричних даних дозволялося законом, якщо особа підозрювалася у вчиненні кримінального правопорушення, навіть якщо її пізніше було виправдано чи звільнено. ЄСПЛ постановив, що всеосяжне і нерозбірливе зберігання персональних даних, яке не було обмежене в часі, і наявність у виправданих осіб лише обмежених можливостей подати запит на видалення даних становило непропорційне втручання у право заявників на повагу до приватного життя. Суд вирішив, що мало місце порушення статті 8 ЄКПЛ.

247 РЄ, Комітет міністрів (1987), Рекомендація Rec(87)15 державам-членам, яка регулює використання персональних даних у роботі поліції, 17 вересня 1987 р.

248 Див., наприклад, ЄСПЛ, *«Леандер проти Швеції»*, № 9248/81, 26 березня 1987 р.; ЄСПЛ, *«М.М. проти Сполученого Королівства»*, № 24029/07, 13 листопада 2012 р.; ЄСПЛ, *«М.К. проти Франції»*, № 19522/09, 18 квітня 2013 р.

249 ЄСПЛ, *«Б.Б. проти Франції»*, № 5335/06, 17 грудня 2009 р.

250 ЄСПЛ, *«С. і Марпер проти Сполученого Королівства»*, № 30562/04 і 30566/04, 4 грудня 2008 р., пп. 119 і 125.

Наступні декілька ухвал ЄСПЛ торкаються питання щодо правомірності втручання у право на захист персональних даних в результаті здійснення стеження.

Приклад: У справі *«Аллан проти Сполученого Королівства»*[251] органи влади таємно записали приватні розмови, які ув'язнений вів зі своїм другом у тюремній кімнаті для побачень, а також зі співобвинуваченим у тюремній камері. ЄСПЛ постановив, що використання аудіо- і відеозаписувальних пристроїв у камері заявника і тюремній кімнаті для побачень, а також прикріплення їх до тіла співкамерника прирівнювалося до втручання у право заявника на приватне життя. Оскільки на той час не існувало жодної передбаченої законом системи регулювання використання поліцією прихованих записуючих пристроїв, таке втручання не відповідало закону. Суд дійшов висновку, що мало місце порушення статті 8 ЄКПЛ.

Приклад: У справі *«Класс та інші проти Німеччини»*[252] заявники стверджували, що декілька законодавчих актів Німеччини, які дозволяли здійснювати таємне стеження за поштою і телефонним зв'язком, порушували статтю 8 ЄКПЛ, зокрема тому, що особі не було повідомлено про заходи зі спостереження і вона не могла звернутися до судів після їх припинення. ЄСПЛ постановив, що загроза стеження, безумовно, була втручанням у свободу спілкування між користувачами поштових і телекомунікаційних послуг. Однак він визнав, що були задіяні достатні гарантії недопущення зловживань. Законодавчий орган Німеччини виправдовувало те, що він вважав вжиття таких заходів необхідним у демократичному суспільстві в інтересах національної безпеки та запобігання заворушенням чи злочинам. Суд дійшов висновку, що порушення статті 8 ЄКПЛ не було.

Оскільки обробка персональних даних органами поліції може справляти значний вплив на відповідних осіб, яких це стосується, докладні правила захисту даних для зберігання баз даних у цій галузі є особливо необхідними. Рекомендація РЄ щодо використання персональних даних поліцією мала вирішити проблему, надаючи вказівки щодо того, як слід збирати дані для роботи поліції; як повинні зберігатися файли даних у цій галузі; кому слід надавати доступ до цих файлів, а також за яких умов дані повинні передаватися іноземним органам поліції; яким чином суб'єкти персональних даних можуть

251 ЄСПЛ, *«Аллан проти Сполученого Королівства»*, № 48539/99, 5 листопада 2002 р.

252 ЄСПЛ, *«Класс та інші проти Німеччини»*, № 5029/71, 6 вересня 1978 р.

здійснювати свої права на захист своїх даних; і як повинен реалізуватися контроль з боку незалежних органів. У ній також розглядається зобов'язання забезпечувати адекватний рівень безпеки даних.

Рекомендація не передбачає нічим не обмеженого і нерозбірливого збирання даних органами поліції. Вона обмежує органи поліції у зборі персональних даних в тій мірі, наскільки це необхідно для запобігання реальній небезпеці або припинення певного кримінального правопорушення. Будь-яке збирання додаткових даних повинно базуватися на конкретному національному законодавстві. Обробка чутливих даних має обмежуватися тим, що є абсолютною необхідністю в контексті конкретного розслідування.

Якщо персональні дані збираються без відома суб'єкта даних, останній повинен бути проінформований про збирання даних, як тільки таке розкриття більше не перешкоджатиме розслідуванню. Збирання даних за допомогою технічного спостереження чи інших автоматизованих засобів також повинно базуватися на конкретних правових положеннях.

Приклад: У справі «*Веттер проти Франції*»[253] анонімні свідки звинуватили заявника у вбивстві. Оскільки заявник регулярно навідувався до будинку свого друга, з дозволу слідчого судді поліція встановила там пристрої для прослуховування. На підставі записаних розмов заявника було заарештовано і притягнуто до відповідальності за вбивство. Він подав клопотання про визнання запису неприйнятним у якості доказу, стверджуючи, зокрема, що він не був передбачений законом. Для ЄСПЛ предметом спору було те, чи «відповідало закону» використання пристроїв для прослуховування. Встановлення у приватному приміщенні апаратури для таємного прослуховування явно не підпадало під дію статті 100 *і наступних* статей Кримінально-процесуального кодексу, оскільки ці положення стосувалися прослуховування телефонних ліній. Стаття 81 Кодексу не зазначала з розумною чіткістю обсяг чи спосіб здійснення органами влади свободи розсуду у наданні дозволу на підслуховування приватних розмов. Відповідно, заявник не скористався мінімальним ступенем захисту, право на який громадянам у демократичному суспільстві надає верховенство права. Суд дійшов висновку, що мало місце порушення статті 8 ЄКПЛ.

253 ЄСПЛ, «*Веттер проти Франції*», № 59842/00, 31 травня 2005 р.

У Рекомендації зроблено висновок про те, що зберігаючи персональні дані слід чітко розрізняти: адміністративні дані і поліцейські дані; різні типи суб'єктів персональних даних, наприклад, підозрюваних, засуджених, потерпілих та свідків; і дані, які вважаються неспростовними фактами, та ті, що засновані на підозрах або припущеннях.

Мета використання поліцейських даних має бути чітко визначена. Це має вплив на повідомлення поліцейських даних третім особам: передача або повідомлення таких даних у рамках сфери діяльності поліції повинні визначатися тим, чи існує законний інтерес в обміні цією інформацією. Передача або повідомлення таких даних за межі сфери діяльності поліції мають допускатися лише за наявності чіткого правового зобов'язання або дозволу. Їх передача або повідомлення за кордон повинні обмежуватися іноземними поліцейськими органами і базуватися на спеціальних правових положеннях, можливо на міжнародних угодах, якщо тільки вони не є необхідними для запобігання серйозній і неминучій небезпеці.

Обробка даних поліцією повинна підлягати незалежному нагляду для забезпечення дотримання національного законодавства про захист персональних даних. Суб'єкти персональних даних повинні мати усі права на доступ, що містяться в Конвенції № 108. Якщо права суб'єкта персональних даних на доступ були обмежені в інтересах ефективного поліцейського розслідування згідно зі статтею 9 Конвенції № 108, суб'єкт даних повинен мати передбачене національним законодавством право звернутися до національного наглядового органу з питань захисту персональних даних чи іншого незалежного органу.

7.1.2. Будапештська конвенція про кіберзлочинність

Оскільки в ході злочинної діяльності зловмисники все частіше вдаються до використання електронних систем обробки даних та впливають на їх роботу, для вирішення цієї проблеми необхідні нові положення кримінального права. Тому РЄ прийняла міжнародний правовий документ, Конвенцію про кіберзлочинність – також відому як Будапештська конвенція – для вирішення питання про злочини, вчинені проти і за допомогою електронних мереж.[254] До цієї Конвенції також можуть приєднуватися держави, які не є членами Ради Європи, і станом на середину 2013 року учасниками конвенції були чотири держа-

254 Рада Європи, Комітет міністрів (2001), Конвенція про кіберзлочинність, CETS № 185, Будапешт, 23 листопада 2001 р., набула чинності 1 липня 2004 р.

ви, які не входять до РЄ (Австралія, Домініканська Республіка, Японія і Сполучені Штати Америки), а 12 інших держав, що також не є її членами, підписали її чи отримали пропозицію щодо приєднання.

Конвенція про кіберзлочинність залишається найвпливовішою міжнародною угодою, що регулює питання порушення закону через Інтернет або інші інформаційні мережі. Вона вимагає від сторін модернізувати і гармонізувати своє кримінальне законодавство проти дій хакерів та інших порушень безпеки, включаючи порушення авторських прав, шахрайство за допомогою комп'ютера, дитячу порнографію та іншу протиправну кібердіяльність. Конвенція також передбачає процесуальні повноваження, що охоплюють обшук комп'ютерних мереж і перехоплення комунікацій в контексті боротьби з кіберзлочинністю. Нарешті, вона створює можливості для ефективного міжнародного співробітництва. Додатковий протокол до Конвенції стосується питання криміналізації пропаганди расизму та ксенофобії у комп'ютерних мережах.

Хоча Конвенція насправді не є інструментом забезпечення захисту персональних даних, вона криміналізує діяльність, яка може порушувати право суб'єкта даних на захист своїх даних. Він також зобов'язує Договірні Сторони передбачити при виконанні Конвенції адекватний рівень захисту прав і свобод людини, в тому числі таких прав, гарантованих ЄКПЛ, як право на захист персональних даних.[255]

7.2. Право ЄС щодо захисту персональних даних у сфері діяльності поліції та кримінального судочинства

Ключові моменти

- На рівні ЄС захист персональних даних у секторі поліції та кримінального судочинства регулюється тільки в контексті транскордонного співробітництва поліцейських та судових органів.
- Існують спеціальні режими захисту даних для Європейського поліцейського управління (Європол) та Європейського бюро судової співпраці (Євроюст), які є органами ЄС, що допомагають і сприяють транскордонному правозастосуванню.

255 Там само, ст. 15 (1).

- Спеціальні режими захисту персональних даних також існують для спільних інформаційних систем, встановлених на рівні ЄС для транскордонного обміну інформацією між компетентними поліцейськими та судовими органами. Їх важливими прикладами є Шенгенська інформаційна система II, Візова інформаційна система (ВІС) і Євродак, централізована система, що містить дані про відбитки пальців громадян третіх країн, які шукають притулку в одній з держав-членів ЄС.

Директива про захист даних не застосовується до сфери діяльності поліції та кримінального судочинства. У підрозділі 7.2.1 описано найважливіші правові документи в цій галузі.

7.2.1. Рамкове рішення про захист персональних даних

Рамкове рішення Ради ЄС № 2008/977/ЈНА про захист персональних даних, що обробляються в рамках поліцейського та судового співробітництва у кримінальних справах (*Рамкове рішення про захист персональних даних*)[256] спрямоване на забезпечення захисту персональних даних фізичних осіб при їх обробці з метою запобігання, розслідування, виявлення і переслідування кримінального правопорушення або виконання кримінального покарання. Від імені держав-членів або ЄС діють компетентні органи, що працюють у сфері діяльності поліції та кримінального судочинства. Ці органи є агенціями чи органами ЄС, а також органами держав-членів.[257] Застосовність рамкового рішення обмежується забезпеченням захисту даних в процесі транскордонного співробітництва між цими органами і не поширюється на питання національної безпеки.

Рамкове рішення про захист персональних даних значною мірою спирається на принципи і визначення, що містяться в Конвенції № 108 та Директиві про захист персональних даних.

Дані повинні використовуватися лише компетентним органом і тільки з метою, для досягнення якої їх було передано або надано. Приймаюча держава-член повинна поважати будь-які обмеження для обміну даними, передбачені у законодавстві держави-члена, яка їх передає. Проте за певних умов дозволяється використання даних приймаючою державою з іншою метою. Реєстрація та документування передачі даних є специфічним обов'язком компетент-

256 Рада Європейського Союзу (2008), Рамкове рішення Ради (ЄС) № 2008/977/ЈНА від 27 листопада 2008 р. про захист персональних даних, що обробляються в рамках поліцейського та судового співробітництва у кримінальних справах (Рамкове рішення про захист даних), OJ 2008 L 350.

257 Там само, ст. 2 (h).

них органів для надання допомоги з роз'яснення обов'язків, що випливають із скарг. Передача третім особам даних, отриманих в процесі транскордонного співробітництва, потребує дозволу держави-члена, з якої походять дані, хоча в екстрених випадках передбачені виключення.

Компетентні органи повинні вживати необхідних заходів з безпеки для захисту персональних даних від будь-якої незаконної форми обробки.

Кожна з держав-членів повинна гарантувати, що один або декілька незалежних національних наглядових органів нестимуть відповідальність за консультування та контроль за застосуванням положень, прийнятих відповідно до Рамкового рішення про захист персональних даних. Вони також повинні розглядати претензії, подані будь-якою особою стосовно захисту його/її прав і свобод під час обробки персональних даних компетентними органами.

Суб'єкт персональних даних має право на інформацію про обробку своїх персональних даних, на доступ до них, їх виправлення, стирання чи блокування. Якщо у здійсненні цих прав відмовлено з незаперечних підстав, суб'єкт персональних даних повинен мати право звернутися до компетентного національного наглядового органу та/або суду. Якщо особа зазнає збитків унаслідок порушення національного законодавства, що вводить в дію Рамкове рішення про захист персональних даних, ця особа має право на отримання компенсації від володільця.[258] Як правило, суб'єкти персональних даних повинні мати доступ до засобів судового захисту від будь-якого порушення їх прав, гарантованих національним законодавством, що вводить в дію Рамкове рішення про захист персональних даних.[259]

Європейська комісія запропонувала реформу, яка складається із Загального регламенту щодо захисту персональних даних[260] і Загальної директиви про захист персональних даних.[261] Ця нова Директива замінить чинне Рамкове рішення про захист персональних даних і застосовуватиме загальні принципи та норми поліцейського і судового співробітництва у кримінальних справах.

258 Там само, ст. 19.

259 Там само, ст. 20.

260 Європейська комісія (2012), Пропозиція щодо Регламенту Європейського парламенту і Ради (ЄС) про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних (Загальний регламент щодо захисту персональних даних), COM(2012) 11 остаточна версія, Брюссель, 25 січня 2012 р.

261 Європейська комісія (2012), Пропозиція щодо Директиви Європейського парламенту і Ради (ЄС) про захист фізичних осіб при обробці персональних даних компетентними органами з метою запобігання, розслідування, виявлення чи судового переслідування кримінальних правопорушень або виконання кримінальних покарань та вільного переміщення таких даних (Загальна директива про захист персональних даних), COM(2012) 10 остаточна версія, Брюссель, 25 січня 2012 р.

7.2.2. Більш специфічні правові інструменти захисту персональних даних у сфері поліцейського та правоохоронного транскордонного співробітництва

На додаток до Рамкового рішення про захист персональних даних, обмін інформацією, якою держави-члени володіють в конкретних сферах, регулюється низкою таких правових інструментів, як Рамкове рішення Ради (ЄС) № 2009/315/ЮНА про організацію та зміст обміну інформацією, отриманою з відомостей про судимість, між державами-членами і Рішення Ради ЄС щодо домовленостей про співпрацю між органами фінансової розвідки держав-членів стосовно обміну інформацією.[262]

Важливо відзначити, що транскордонне співробітництво[263] між компетентними органами усе більше включає в себе обмін даними про імміграцію. Ця галузь права не відноситься до питань діяльності поліції та кримінального судочинства, але багато в чому стосується роботи поліції й органів правосуддя. Те саме можна сказати і про дані щодо товарів, які імпортуються до ЄС або експортуються з нього. Ліквідація внутрішнього прикордонного контролю всередині ЄС посилила ризик шахрайства, що робить необхідним для держав-членів активізувати співпрацю, зокрема, шляхом покращення транскордонного обміну інформацією, та більш ефективно виявляти і переслідувати порушення національного митного законодавства та митного законодавства ЄС.

Прюмське рішення

Важливим прикладом інституціоналізованого транскордонного співробітництва у формі обміну національними даними є Рішення Ради (ЄС) № 2008/615/ЮНА про посилення транскордонного співробітництва, зокрема, у боротьбі з тероризмом і транскордонною злочинністю (*Прюмське рішення*), яке

262 Рада Європейського Союзу (2009), Рамкове рішення Ради (ЄС) № 2009/315/ЮНА від 26 лютого 2009 року про організацію та зміст обміну інформацією, отриманою з відомостей про судимості, між державами-членами, OJ 2009 L 93; Рада Європейського Союзу (2000), Рішення Ради (ЄС) 2000/642/ЮНА від 17 жовтня 2000 року відносно домовленостей про співпрацю між підрозділами фінансової розвідки держав-членів у плані обміну інформацією, OJ 2000 L 271.

263 Європейська комісія (2012), Комюніке Європейської комісії до Європейського парламенту і Ради (ЄС) – Зміцнення співробітництва між правоохоронними органами в ЄС: Європейська модель обміну інформацією (EIXM), COM(2012) 735 остаточна версія, Брюссель, 7 грудня 2012 р.

у 2008 році включило Прюмську угоду в право ЄС.[264] Прюмська угода – міжнародний договір щодо поліцейського співробітництва, підписаний в 2005 році Австрією, Бельгією, Францією, Німеччиною, Люксембургом, Нідерландами та Іспанією.[265]

Метою Прюмського рішення було допомогти державам-членам поліпшити обмін інформацією задля запобігання та боротьби зі злочинністю у трьох напрямках, передбачаючи протидію тероризму, транскордонній злочинності та нелегальній міграції. Для цього в Рішенні викладено положення стосовно:

- автоматизованого доступу до ДНК-профілів, даних відбитків пальців і певних національних реєстраційних даних транспортних засобів;
- надання даних відносно основних подій, які мають транскордонний вимір;
- надання інформації для запобігання терористичній діяльності;
- інших заходів для посилення транскордонного поліцейського співробітництва.

Бази даних, до яких надає доступ Прюмське рішення, регулюються виключно національним законодавством, але обмін даними додатково регулює Рішення, а віднедавна й Рамкове рішення про захист персональних даних. Компетентними органами, які здійснюють нагляд за такими потоками даних, є національні наглядові органи з питань захисту персональних даних.

7.2.3. Захист персональних даних Європолом та Євроюстом

Європол

Європол – це правоохоронний орган ЄС зі штаб-квартирою в місті Гаага та Національними підрозділами Європолу (НПЄ) в кожній з держав-членів. Європол був створений в 1998 році; його теперішній правовий статус інсти-

264 Рада Європейського Союзу (2008), Рішення Ради (ЄС) № 2008/615/ЈНА від 23 червня 2008 року про посилення транскордонного співробітництва, зокрема, у боротьбі з тероризмом і транскордонною злочинністю, OJ 2008 L 210.

265 Конвенція між Королівством Бельгія, Федеративною Республікою Німеччина, Королівством Іспанія, Французькою Республікою, Великим Герцогством Люксембург, Королівством Нідерландів та Республікою Австрія щодо посилення транскордонного співробітництва, зокрема, у боротьбі з тероризмом, транскордонною злочинністю та нелегальною міграцією; доступна за посиланням: http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf.

туції ЄС ґрунтується на Рішенні Ради (ЄС) про створення Європейського поліцейського відомства (*Рішення про Європол*).[266] Метою Європолу є надання допомоги у запобіганні та розслідуванні організованої злочинності, тероризму та інших форм тяжких злочинів, перерахованих у Додатку до Рішення про Європол, що впливають на дві або більше держави-члени.

Для досягнення своїх цілей Європол створив Інформаційну систему Європолу (Europol Information System – EIS), яка пропонує державам-членам базу даних для обміну розвідувальними даними та інформацією через свої НПЄ. Інформаційна система Європолу може використовуватися для відкриття доступу до даних, що стосуються: осіб, які є підозрюваними або яких було засуджено за здійснення кримінального правопорушення, що входить до компетенції Європолу; або осіб, факти щодо яких вказують на те, що вони готуються вчинити такі правопорушення. Європол і НПЄ можуть як вносити дані безпосередньо до Інформаційної системи Європолу, так і вилучати дані з неї. Тільки сторона, яка внесла дані в систему, може змінити, виправити або видалити їх.

У разі необхідності, для виконання своїх завдань Європол може зберігати, змінювати і використовувати дані стосовно кримінальних правопорушень в аналітичних робочих картотеках. Аналітичні робочі картотеки відкриті для збирання, обробки або використання даних з метою надання допомоги у конкретних розслідуваннях кримінальних правопорушень, які Європол проводить разом з державами-членами ЄС.

У відповідь на останні події, 1 січня 2013 року в межах Європолу був створений Європейський центр боротьби з кіберзлочинністю.[267] Центр слугує інформаційним порталом ЄС з питань кіберзлочинності, який сприяє більш швидкому реагуванню у разі вчинення онлайн-злочинів, розробляє та розгортає потенціал цифрової судово-медичної експертизи та надає інформацію про передовий досвід розслідування кіберзлочинів. Центр спеціалізується на кіберзлочинах, які:

266 Рада Європейського Союзу (2009), Рішення Ради (ЄС) від 6 квітня 2009 року про створення Європейського поліцейського відомства, OJ 2009 L 121 (Європол). Див. також Пропозицію Європейської комісії щодо регламенту, яка забезпечує правову основу для створення нового Європолу, який стане наступником і замінить собою Європол, сформований Рішенням Ради (ЄС) № 2009/371/JHA від 6 квітня 2009 року про створення Європейського поліцейського відомства (Європолу), і CEPOL, сформований Рішенням Ради (ЄС) № 2005/681/JHA про створення Європейського поліцейського коледжу (CEPOL), COM(2013) 173 остаточна версія.

267 Див. також: ЄІЗД (2012), Висновок Інспектора з захисту персональних даних щодо Комюніке Європейської комісії до Ради (ЄС) і Європейського парламенту щодо створення Європейського центру боротьби з кіберзлочинністю, Брюссель, 29 червня 2012 р.

- скоюються організованими групами для отримання злочинним шляхом великих доходів, наприклад, через онлайн-шахрайство;
- заподіюють серйозну шкоду потерпілому, наприклад, через сексуальну експлуатацію дітей в інтернеті;
- справляють негативний вплив на критичну інфраструктуру та інформаційні системи в ЄС.

Режим захисту персональних даних, який регулює діяльність Європолу, посилюється. У статті 27 Рішення про Європол визначено, що потрібно дотримуватися принципів, викладених у Конвенції № 108 та Рекомендації щодо використання персональних даних поліцією стосовно автоматизованої і неавтоматизованої обробки даних. Передача даних між Європолом і державами-членами також повинна відповідати нормам, що містяться у Рамковому рішенні про захист персональних даних.

Для забезпечення дотримання відповідного законодавства про захист персональних даних і, зокрема, щоб при обробці персональних даних не порушувалися права особи, діяльність Європолу перевіряється і контролюється незалежним Спільним наглядовим органом Європолу (СНО).[268] Кожна особа має право на доступ до будь-яких персональних даних про неї, якими може володіти Європол, а також право вимагати, щоб ці персональні дані були перевірені, виправлені або стерті. Якщо особа не задоволена рішенням Європолу щодо здійснення цих прав, вона може звернутися до Апеляційного комітету СНО.

Якщо внаслідок юридичних або фактичних помилок у даних, які зберігаються та обробляються Європолом, було завдано шкоди, постраждала сторона може вимагати відшкодування тільки у компетентному суді держави-члена, у якій сталася подія, що спричинила завдану шкоду.[269] Європол компенсує державі-члену кошти, якщо шкода є результатом невиконання Європолом своїх правових зобов'язань.

Євроюст

Створений у 2002 році Євроюст є органом ЄС зі штаб-квартирою в місті Гаазі, який сприяє судовому співробітництву у розслідуванні та судовому переслідуванні

268 Рішення про Європол, ст. 34.

269 Там само, ст. 52.

ванні тяжких злочинів, які стосуються щонайменше двох держав-членів.[270] Євроюст компетентний:

- стимулювати і покращувати координування розслідувань та судових переслідувань між компетентними органами різних держав-членів;
- допомагати у виконанні запитів і рішень, що стосуються судового співробітництва.

Функції Євроюсту здійснюються національними членами. Кожна держава-член делегує в Євроюст одного суддю або прокурора, статус якого відповідає національному законодавству і який наділений необхідними повноваженнями для виконання завдань, необхідних для стимулювання і вдосконалення судового співробітництва. Крім того, національні члени діють спільно як колегія для виконання спеціальних завдань Євроюсту.

Євроюст може обробляти персональні дані за умови, що це необхідно для досягнення його цілей. Однак ці дані обмежуються конкретною інформацією щодо осіб, які підозрюються у скоєнні чи участі в кримінальному правопорушенні, або яких було засуджено за правопорушення, що входить до компетенції Євроюсту. Євроюст також може обробляти певну інформацію про свідків або жертв кримінальних правопорушень що входять до його компетенції.[271] За виняткових обставин, протягом обмеженого періоду часу Євроюст може обробляти більш широкі персональні дані, які стосуються обставин правопорушення, якщо ці дані мають безпосереднє відношення до розслідування, що проводиться. В межах своєї компетенції Євроюст може співпрацювати з іншими інституціями, органами та агенціями ЄС і обмінюватися з ними персональними даними. Також Євроюст може співпрацювати і обмінюватися персональними даними з третіми країнами та організаціями.

Стосовно захисту даних, Євроюст повинен гарантувати рівень захисту, який би був щонайменше рівноцінним принципам Конвенції Ради Європи № 108 і наступним поправкам до неї. Під час обміну даними повинні дотримуватися

270 Рада Європейського Союзу (2002), Рішення Ради (ЄС) № 2002/187/JHA від 28 лютого 2002 року про заснування Євроюсту з метою посилення боротьби з серйозними злочинами, OJ 2002 L 63; Рада Європейського Союзу (2003), Рішення Ради (ЄС) № 2003/659/JHA від 18 червня 2003 року про внесення змін до Рішення № 2002/187/JHA про заснування Євроюсту з метою посилення боротьби з серйозними злочинами, OJ 2003 L 44; Рада Європейського Союзу (2009), Рішення Ради (ЄС) № 2009/426/JHA від 16 грудня 2008 року про зміцнення Євроюсту та внесення змін до Рішення № 2002/187/JHA про заснування Євроюсту з метою посилення боротьби з серйозними злочинами, OJ 2009 L 138 (Рішення про Євроюст).

271 Консолідована версія Рішення Ради (ЄС) № 2002/187/JHA зі змінами, внесеними Рішенням Ради (ЄС) № 2003/659/JHA і Рішенням Ради (ЄС) № 2009/426/JHA, ст. 15 (2).

певні правила й обмеження, які встановлюються або в угоді про співробітництво, або в робочих домовленостях відповідно до Рішень Ради (ЄС) про Євроюст і Правил щодо захисту персональних даних Євроюсту.[272]

В межах Євроюсту було створено незалежний СНО, завданням якого є контролювати обробку персональних даних, яку здійснює Євроюст. Фізичні особи можуть звернутися до СНО, якщо вони не задоволені відповіддю Євроюсту на запит щодо надання доступу, виправлення, блокування або стирання персональних даних. Якщо Євроюст обробляє персональні дані незаконно, він несе відповідальність за шкоду, заподіяну суб'єкту персональних даних, згідно з національним законодавством держави-члена, у якій розташована його штаб-квартира, а саме Нідерландів.

7.2.4. Захист персональних даних у спільних інформаційних системах на рівні ЄС

На додачу до обміну даними між державами-членами та створення спеціалізованих органів ЄС для боротьби з транскордонною злочинністю на рівні ЄС було створено декілька спільних інформаційних систем, які слугують платформою для обміну даними між компетентними національними органами та органами ЄС заради конкретних цілей забезпечення дотримання законодавства, у тому числі закону про імміграцію та митного права. Деякі з цих систем були розроблені з багатосторонніх угод, які згодом було доповнено такими правовими документами і системами ЄС, як Шенгенська інформаційна система (SIS), Візова інформаційна система (VIS), Євродак (Eurodac), Євросюр (Eurosur) або Митна інформаційна система (CIS).

Агенція ЄС з великомасштабних інформаційно-технологічних систем (eu-LISA),[273] створена в 2012 році, відповідає за довгострокове оперативне управління Шенгенською інформаційною системою другого покоління (SIS II), Візовою інформаційною системою (VIS) і системою Eurodac. Ключовим завданням агенції eu-LISA є забезпечення ефективного, надійного і безперебійного функціонування інформаційно-технологічних систем. Вона також відповідає за вжиття необхідних заходів для гарантування безпеки систем і даних.

272 Правила процедури з обробки та захисту персональних даних в Євроюсті, OJ 2005 C 68/01, 19 березня 2005 р., п. 1.

273 Регламент (ЄС) № 1077/2011 Європейського парламенту і Ради (ЄС) від 25 жовтня 2011 року про заснування Європейської агенції з оперативного менеджменту великомасштабних IT-систем у сфері свободи, безпеки та правосуддя, OJ 2011 L 286.

Шенгенська інформаційна система

В 1985 році декілька держав-членів колишніх Європейських Співтовариств підписали Угоду між урядами держав Економічного Союзу Бенілюкс, Німеччини та Франції про поступове скасування перевірок на спільних кордонах (*Шенгенську угоду*), спрямовану на створення зони вільного пересування осіб у межах Шенгенської зони без перешкод з боку прикордонного контролю.[274] Щоб урівноважити загрозу державній безпеці, яка могла виникнути у зв'язку з відкритими кордонами, на зовнішніх кордонах Шенгенської зони було встановлено посилений прикордонний контроль, а також посилено тісну співпрацю між національними поліцейськими та судовими органами.

Внаслідок приєднання до Шенгенської угоди додаткових держав, Амстердамською угодою було остаточно інтегровано Шенгенську систему в правове поле ЄС.[275] Імплементація цього рішення відбулася в 1999 році. Остання версія Шенгенської інформаційної системи, так звана «SIS II», почала функціонувати 9 квітня 2013 року. Тепер вона обслуговує усі держави-члени ЄС, а також Ісландію, Ліхтенштейн, Норвегію та Швейцарію.[276] Європол і Євроюст також мають доступ до SIS II.

SIS II складається з центральної системи (C-SIS), національної системи (N-SIS) у кожній з держав-членів і комунікаційної інфраструктури між центральною системою та національними системами. C-SIS містить певні дані, внесені державами-членами стосовно осіб та об'єктів. C-SIS використовується органами національного прикордонного контролю, поліції та митниці, а також візовими і судовими органами на всій території Шенгенської зони. Кожна з держав-членів оперує національною копією C-SIS, відомою як Національна Шенгенська інформаційна система (N-SIS), яка постійно оновлюється і тим самим оновлює C-SIS. До N-SIS звертаються, а вона видає сигнал про тривогу, якщо:

- особа не має права на в'їзд і перебування на території Шенгенської зони; або

274 Угода між Урядами держав Економічного Союзу Бенілюкс, Федеративної Республіки Німеччина та Французької Республіки про поступове скасування перевірок на спільних кордонах, OJ 2000 L 239.

275 Європейські Співтовариства (1997), Амстердамський договір про внесення змін до Договору про Європейський Союз, договорів про заснування Європейських Співтовариств і деяких пов'язаних з ними актів, OJ 1997 C 340.

276 Регламент (ЄС) № 1987/2006 Європейського парламенту і Ради (ЄС) від 20 грудня 2006 року щодо заснування, функціонування та використання Шенгенської інформаційної системи другого покоління (SIS II), OJ 2006 L 381, і Рада Європейського Союзу (2007), Рішення Ради (ЄС) № 2007/533/JHA від 12 червня 2007 року про заснування, функціонування та використання Шенгенської інформаційної системи другого покоління (SIS II), OJ 2007 L 205.

- особа чи об'єкт розшукуються судовими або правоохоронними органами; або
- особу визнано безвісно відсутньою; або
- про такі речі, як банкноти, автомобілі, фургони, вогнепальна зброя і документи, що засвідчують особу, було повідомлено як про викрадене або втрачене майно.

У разі сигналу тривоги подальші кроки вчиняються із використанням Національних Шенгенських інформаційних систем.

У SIS II є такі нові функції, як можливість внесення біометричних даних, таких як відбитки пальців і фотографії; або нові категорії для видання сигналу тривоги, наприклад, викрадені човни, літаки, контейнери чи засоби платежу; і посилені сигнали оповіщення про осіб та об'єкти; копії Європейських ордерів на арешт (ЄОА) осіб, які розшукуються для арешту, приведення до суду або екстрадиції.

Рішення Ради (ЄС) № 2007/533/JHA про заснування, функціонування та використання Шенгенської інформаційної системи другого покоління (Рішення про SIS II) включає в себе Конвенцію № 108: «Персональні дані, що обробляються на виконання цього рішення, захищаються відповідно до Конвенції Ради Європи № 108».[277] Якщо використання персональних даних національними поліцейськими органами здійснюється на виконання Рішення про SIS II, положення Конвенції № 108 а також Рекомендації щодо використання персональних даних поліцією мають бути імплементовані в національне законодавство.

Компетентний національний наглядовий орган у кожній з держав-членів здійснює нагляд за національною N-SIS. Зокрема, він повинен перевіряти якість даних, які держава-член вносить до C-SIS через N-SIS. Національний наглядовий орган повинен забезпечувати, щоб аудит операцій з обробки даних в рамках національної N-SIS проводився хоча б один раз на чотири роки. Національні наглядові органи і ЄІЗД співпрацюють і забезпечують координований нагляд за SIS; крім того, ЄІЗД відповідає за нагляд за C-SIS. Для забезпечення прозорості Європейському парламенту, Раді (ЄС) та агенції eu-LISA один раз в два роки направляється спільний звіт про діяльність.

277 Рада Європейського Союзу (2007), Рішення Ради (ЄС) № 2007/533/JHA від 12 червня 2007 року про заснування, функціонування та використання Шенгенської інформаційної системи другого покоління, OJ 2007 L 205, ст. 57.

Права фізичних осіб на доступ до SIS II можуть здійснюватися у будь-якій з держав-членів, оскільки кожна N-SIS є точною копією C-SIS.

Приклад: У справі *«Даля проти Франції»*[278] заявнику було відмовлено у видачі візи для відвідання Франції, бо органи влади Франції повідомили Шенгенську інформаційну систему про те, що йому слід відмовити у в'їзді. Заявник безуспішно домагався від Комісії з питань захисту персональних даних Франції, а потім і від Державної ради, надати йому доступ та виправити або видалити дані. ЄСПЛ постановив, що повідомлення про заявника до Шенгенської інформаційної системи відбулося відповідно до закону і переслідувало законну мету захисту національної безпеки. Оскільки заявник не довів, що він фактично постраждав у результаті відмови у в'їзді до Шенгенської зони, і оскільки для його захисту від свавільних рішень було вжито достатніх заходів, втручання у його право на повагу до приватного життя було пропорційним. Таким чином, скаргу заявника, подану на підставі статті 8, було визнано неприйнятною.

Візова інформаційна система

Візова інформаційна система (VIS), якою також управляє агенція eu-LISA, була розроблена для підтримки реалізації спільної візової політики ЄС.[279] VIS дозволяє державам-учасницям Шенгенської угоди обмінюватися візовими даними через систему, яка з'єднує консульства шенгенських держав, розташовані у країнах, які не є членами ЄС, із зовнішніми пунктами перетину кордону всіх держав Шенгенської зони. VIS обробляє дані, що стосуються заявок на отримання короткострокових віз для відвідування Шенгенської зони або транзиту через неї. VIS дозволяє прикордонним органам перевіряти за допомогою біометричних даних, чи є особа, яка пред'являє візу, її законним власником і виявляти осіб, у яких відсутні або підроблені документи.

278 ЄСПЛ, *«Даля проти Франції»* (ріш.), № 964/07, 2 лютого 2010 р.

279 Рада Європейського Союзу (2004), Рішення Ради (ЄС) від 8 червня 2004 року про створення Візової інформаційної системи (VIS), OJ 2004 L 213; Регламент (ЄС) № 767/2008 Європейського парламенту і Ради (ЄС) від 9 липня 2008 року щодо Візової інформаційної системи (VIS) та обміну даними між державами-членами щодо короткотермінових віз, OJ 2008 L 218 (Регламент VIS); Рада Європейського Союзу (2008), Рішення Ради (ЄС) № 2008/633/JHA від 23 червня 2008 року про доступ до Візової інформаційної системи (VIS) компетентних органів держав-членів та Європолу в цілях запобігання, виявлення та розслідування терористичних та інших серйозних кримінальних правопорушень, OJ 2008 L 218.

Згідно з Регламентом № 767/2008 Європейського парламенту і Ради (ЄС) щодо Візової інформаційної системи (VIS) та обміну даними між державами-членами щодо короткотермінових віз (*Регламент VIS*), у VIS можуть бути записані тільки дані про заявника, його візи, фотографії, відбитки пальців, посилання на попередні заявки, а також інформація про осіб, які його супроводжують.[280] Доступ до VIS для внесення, зміни або видалення даних надається виключно візовим органам держав-членів, тоді як доступ для ознайомлення з даними надається візовим органам та органам, у компетенцію яких входить перевірка зовнішніх пунктів перетину кордону, імміграційний контроль і надання притулку. За певних обставин, національні компетентні поліцейські органи і Європол можуть запросити доступ до даних, внесених у VIS з метою запобігання, виявлення і розслідування тероризму і кримінальних правопорушень.[281]

Eurodac

Назва системи Eurodac походить від слова «дактилограма» або відбитки пальців. Це централізована система, що містить дані про відбитки пальців громадян третіх країн, які просять притулку в одній з держав-членів ЄС.[282] Система функціонує з січня 2003 року і її метою є надання допомоги у визначенні того, яка з держав-членів повинна відповідати за розгляд конкретної заяви про надання притулку відповідно до Регламенту Ради (ЄС) № 343/2003, що встановлює критерії та механізми визначення держави-члена, відповідальної за розгляд заяви про надання притулку, поданої в одній із держав-членів громадянином третьої країни (*Регламенту «Дублін II»*).[283] Персональні дані, що містяться в системі Eurodac, можуть використовуватися лише з метою сприян-

280 Ст. 5 Регламенту (ЄС) № 767/2008 Європейського парламенту і Ради (ЄС) від 9 липня 2008 року щодо Візової інформаційної системи (VIS) та обміну даними між державами-членами щодо короткотермінових віз (Регламент VIS), OJ 2008 L 218.

281 Рада Європейського Союзу (2008), Рішення Ради (ЄС) № 2008/633/JHA від 23 червня 2008 року про доступ до Візової інформаційної системи (VIS) компетентних органів держав-членів та Європолу в цілях запобігання, виявлення та розслідування терористичних та інших серйозних кримінальних правопорушень, OJ 2008 L 218.

282 Регламент Ради (ЄС) № 2725/2000 від 11 грудня 2000 року про заснування системи «Євродак» для порівняння відбитків пальців з метою ефективного застосування Дублінської Конвенції, OJ 2000 L 316; Регламент Ради (ЄС) № 407/2002 від 28 лютого 2002 року, що встановлює певні правила імплементації Регламенту (ЄС) № 2725/2000 про заснування системи «Євродак» для порівняння відбитків пальців з метою ефективного застосування Дублінської Конвенції, OJ 2002 L 62 (Регламенти щодо системи Євродак).

283 Регламент Ради (ЄС) № 343/2003 від 18 лютого 2003 року що встановлює критерії та механізми визначення держави-члена, відповідальної за розгляд заяви про надання притулку, поданої в одній із держав-членів громадянином третьої країни, OJ 2003 L 50 (Регламент «Дублін II»).

ня застосуванню Регламенту «Дублін II»; їх використання з будь-якою іншою метою карається.

Eurodac складається з Центрального підрозділу, яким керує агенція eu-LISA і в якому зберігаються та порівнюються відбитки пальців, та системи електронної передачі даних між державами-членами і центральною базою даних. Держави-члени беруть і передають відбитки пальців кожної особи, яка не є громадянином ЄС або не має громадянства і досягла принаймні 14-річного віку, яка просить притулку на їх території або затримана за несанкціоноване перетинання їх зовнішнього кордону. Держави-члени можуть також брати і передавати відбитки пальців осіб, що не є громадянами ЄС або не мають громадянства, якщо виявлено, що вони перебувають на їх території без дозволу.

Дані про відбитки пальців зберігаються в базі даних системи Eurodac лише в анонімній формі. У разі збігу відбитків, псевдонім разом з назвою першої держави-члена, яка передала дані про відбитки пальців, розкривається другій державі-члену. Далі ця друга держава-член звертається до першої держави-члена, тому що згідно з Регламентом «Дублін II» перша держава-член відповідає за обробку заяви про надання притулку.

Персональні дані прохачів притулку, що зберігаються в системі Eurodac, зберігаються протягом 10 років з дати взяття відбитків пальців, якщо тільки суб'єкт персональних даних не отримає громадянство держави-члена ЄС. У цьому випадку дані повинні бути негайно видалені. Дані щодо іноземних громадян, затриманих за несанкціоноване перетинання зовнішнього кордону, зберігаються протягом двох років. Ці дані повинні бути негайно видалені, якщо суб'єкт персональних даних отримує дозвіл на проживання, залишає територію ЄС чи отримує громадянство держави-члена.

Крім усіх держав-членів ЄС, Ісландія, Норвегія, Ліхтенштейн та Швейцарія також застосовують систему Eurodac на основі міжнародних угод.

Eurosur

Європейська система спостереження за кордонами (Eurosur)[284] призначена для посилення контролю на зовнішніх кордонах Шенгенської зони шляхом виявлення, запобігання та боротьби з нелегальною імміграцією і транскордонною злочинністю. Вона слугує покращенню обміну інформацією та оперативному співробітництву між національними координаційними центрами

284 Регламент (ЄС) № 1052/2013 і Європейського парламенту Ради (ЄС) від 22 жовтня 2013 року щодо створення Європейської системи прикордонного контролю (Eurosur), OJ 2013 L 295.

та Фронтексом, агенцією ЄС, що відповідає за розробку і застосування нової концепції інтегрованого управління кордонами.[285] Її загальними цілями є:

- зменшити кількість нелегальних мігрантів, які непомітно проникають до ЄС;
- зменшити кількість смертей нелегальних мігрантів, рятуючи більше життів на морі;
- посилити внутрішню безпеку ЄС в цілому, беручи участь в запобіганні транскордонній злочинності.[286]

Система почала функціонувати 2 грудня 2013 року в усіх державах-членах, які мають зовнішні кордони, а з 1 грудня 2014 року – в інших державах-членах. Її нормативні правила застосовуватимуться для спостереженням за зовнішніми кордонами на землі та морі, а також контролем за повітряними кордонами держав-членів.

Митна інформаційна система

Іншою важливою спільною інформаційною системою, створеною на рівні ЄС, є Митна інформаційна система (CIS).[287] В процесі формування внутрішнього ринку усі перевірки і формальності щодо товарів, які переміщуються по території ЄС, було скасовано, що призвело до підвищеного ризику шахрайства. Цей ризик був урівноважений посиленим співробітництвом між митними адміністраціями держав-членів. Метою CIS є надання державам-членам допомоги у запобіганні, розслідуванні та судовому переслідуванні серйозних порушень митного і сільськогосподарського права держав-членів та ЄС.

285 Регламент (ЄС) № 1168/2011 Європейського парламенту і Ради (ЄС) від 25 жовтня 2011 року щодо внесення змін до Регламенту Ради (ЄС) № 2007/2004 щодо створення Європейської агенції з питань управління оперативним співробітництвом на зовнішніх кордонах держав-членів Європейського Союзу, OJ 2011 L 394 (Регламент щодо Фронтексу).

286 Див. також: Європейська комісія (2008), Комюніке Європейської комісії до Європейського парламенту, Ради (ЄС), Європейського економічного та соціального комітету і Комітету регіонів: Вивчення можливостей створення Європейської системи спостереження за кордонами (Eurosur), COM(2008) 68 остаточна версія, Брюссель, 13 лютого 2008 року; Європейська комісія (2011), Оцінка впливу на додачу до Пропозиції щодо Регламенту Європейського парламенту і Ради (ЄС) щодо створення Європейської системи спостереження за кордонами (Eurosur), Робочий документ персоналу Комісії, SEC(2011) 1536 остаточна версія, Брюссель,12 грудня 2011 р., п. 18.

287 Рада Європейського Союзу (1995), Акт Ради (ЄС) від 26 липня 1995 року про укладення Конвенції про використання інформаційних технологій у митних цілях, OJ 1995 C 316, змінений документом: Рада Європейського Союзу (2009), Регламент № 515/97 від 13 березня 1997 року про взаємодопомогу між адміністративними органами держав-членів та співробітництво між останніми і Комісією з метою забезпечення правильного застосування законодавства з митних і сільськогосподарських питань, Рішення Ради (ЄС) № 2009/917/JHA від 30 листопада 2009 року про використання інформаційних технологій у митних цілях, OJ 2009 L 323 (Рішення про CIS).

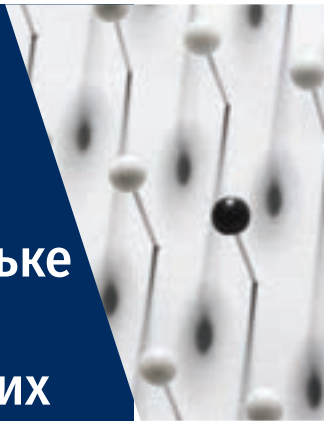
Інформація, що міститься у CIS, охоплює персональні дані стосовно сировинних матеріалів, транспортних засобів, підприємств, осіб, утриманих, заарештованих або конфіскованих товарів та коштів. Ця інформація може використовуватися виключно для цілей спостереження, звітування чи проведення конкретних перевірок або для здійснення стратегічного чи оперативного аналізу осіб, які підозрюються в порушенні митних положень.

Доступ до CIS надається національним митним, податковим і сільськогосподарським органам, органам охорони здоров'я та поліції, а також Європолу та Євроюсту.

Обробка персональних даних повинна здійснюватися у відповідності з конкретними нормами, встановленими Регламентом № 515/97 та Конвенцією CIS,[288] а також положеннями Директиви про захист персональних даних, Регламенту інституцій ЄС щодо захисту персональних даних, Конвенції № 108 і Рекомендація щодо використання персональних даних поліцією. ЄІЗД несе відповідальність за нагляд за дотриманням CIS Регламенту (ЄС) № 45/2001 і щонайменше один раз на рік скликає зустріч усіх національних наглядових органів з питань захисту персональних даних, які є компетентними у питаннях, пов'язаних з CIS.

288 Там само.

8 Інше спеціальне європейське законодавство у сфері захисту персональних даних



ЄС	питання, що висвітлюються	РЄ
Директива про захист персональних даних Директива про конфіденційність та електронні комунікації	**Електронні комунікації**	Конвенція № 108 Рекомендація щодо телекомунікаційних послуг
Директива про захист персональних даних, стаття 8 (2) (b)	**Трудові відносини**	Конвенція № 108 Рекомендація щодо даних про працевлаштування
		ЄСПЛ, *«Копланд проти Сполученого Королівства»*, № 62617/00, 3 квітня 2007 р.
Директива про захист персональних даних, стаття 8 (3)	**Медичні дані**	Конвенція № 108 Рекомендація щодо медичних даних
		ЄСПЛ, *«З. проти Фінляндії»*, № 22009/93, 25 лютого 1997 р.
Директива про клінічні випробування	**Клінічні випробування**	
Директива про захист персональних даних, стаття 6 (1) (b) і (e), стаття 13 (2)	**Статистичні дані**	Конвенція № 108 Рекомендація щодо статистичних даних

ЄС	питання, що висвітлюються	РЄ
Регламент (ЕС) № 223/2009 щодо європейської статистики Суд ЄС, C-524/06, «*Губер проти Німеччини*», 16 грудня 2008 р.	**Офіційні статистичні дані**	Конвенція № 108 Рекомендація щодо статистичних даних
Директива 2004/39/ЕС про ринки фінансових інструментів Регламент (ЕС) № 648/2012 щодо позабіржових деривативів, центральних контрагентів і торгових репозиторіїв Регламент (ЕС) № 1060/2009 щодо кредитно-рейтингових агенцій Директива 2007/64/ЕС про платіжні послуги на внутрішньому ринку	**Фінансові дані**	Конвенція № 108 Рекомендація 90(19) про захист персональних даних, що використовується при платежах та інших суміжних операціях ЄСПЛ, *«Мішо проти Франції»*, № 12323/11, 6 грудня 2012 р.

У ряді випадків на рівні ЄС були прийняті спеціальні правові документи, у яких до конкретних ситуацій більш детально застосовуються загальні норми Конвенції № 108 або Директиви про захист персональних даних.

8.1. Електронні комунікації

Ключові моменти

- Конкретні норми захисту персональних даних у сфері телекомунікацій з особливою увагою до телефонних послуг містяться у Рекомендації РЄ від 1995 року.
- Обробка персональних даних, що стосуються надання комунікаційних послуг на рівні ЄС, регулюється Директивою про конфіденційність та електронні комунікації.
- Конфіденційність електронних комунікацій стосується не лише змісту спілкування, але й таких даних щодо трафіку, як інформація про те, хто спілкувався і з ким, коли і як довго, а також даних про місцезнаходження (наприклад, звідки дані було повідомлено).

Комунікаційні мережі мають підвищений потенціал для необґрунтованого втручання в особисту сферу користувачів, оскільки вони надають додаткові технічні можливості для прослуховування і спостереження за комунікаціями, що здійснюються в таких мережах. В результаті, спеціальні регламенти щодо захисту персональних даних було визнано необхідними для подолання конкретних ризиків, які постають перед користувачами комунікаційних послуг.

В 1995 році РЄ видала Рекомендацію щодо захисту персональних даних у сфері телекомунікаційних послуг з особливими рекомендаціями щодо телефонних послуг.[289] Відповідно до цієї рекомендації цілі збирання та обробки персональних даних у контексті телекомунікацій мають обмежуватися підключенням користувача до мережі, наданням доступу до окремої телекомунікаційної послуги, виставленням рахунків, верифікацією, забезпеченням оптимальної технічної експлуатації та розвитком мережі й обслуговування.

Особливу увагу також було приділено використанню комунікаційних мереж для відправки повідомлень прямого маркетингу. Як правило, повідомлення прямого маркетингу не можуть надсилатися будь-якому абоненту, який надав чітку відмову отримувати повідомлення рекламного характеру. Автоматизовані пристрої здійснення дзвінків можуть використовуватися для передачі попередньо записаних повідомлень рекламного характеру лише за умови надання абонентом явно вираженої згоди. Національне законодавство повинно передбачати детальні норми у цій сфері.

Відносно **нормативної бази ЄС** після першої спроби, здійсненої в 1997 році з метою доповнення та конкретизації положень Директиви про захист даних у сфері телекомунікацій,[290] в 2002 році була прийнята Директива про конфіденційність та електронні комунікації, а в 2009 році до неї було внесено змі-

289 РЄ, Комітет міністрів (1995), Рекомендація Rec(95)4 щодо захисту персональних даних у сфері телекомунікаційних послуг з особливими рекомендаціями щодо телефонних послуг, 7 лютого 1995 р.

290 Директива 2002/58/ЕС Європейського парламенту і Ради (ЄС) від 12 липня 2002 року стосовно обробки персональних даних та захисту конфіденційності у секторі електронних комунікацій, OJ 2002 L 201 (Директива про конфіденційність та електронні комунікації), змінена Директивою 2009/136/ЕС Європейського парламенту і Ради (ЄС) від 25 листопада 2009 року, що вносить зміни до Директиви 2002/22/ЕС про універсальні послуги і права користувачів, що стосуються електронних комунікаційних мереж і послуг, Директиви 2002/58/ЕС стосовно обробки персональних даних та захисту конфіденційності у секторі електронних комунікацій і Регламенту (ЄС) № 2006/2004 про співробітництво між національними органами влади, відповідальними за виконання законів про захист прав споживачів, OJ 2009 L 337.

ни. Застосування Директиви про конфіденційність та електронні комунікації обмежується комунікаційними послугами в публічних електронних мережах.

Директива про конфіденційність та електронні комунікації розрізняє три основні категорії даних, вироблених в процесі комунікації:

- дані, що становлять зміст повідомлень, відправлених в процесі комунікації; ці дані є суворо конфіденційними;
- дані, необхідні для встановлення і підтримки комунікації, так звані дані щодо трафіку, такі як інформація про партнерів з комунікації, час і тривалість комунікації;
- серед даних щодо трафіку є дані, які стосуються конкретного розташування комунікаційного пристрою, так звані дані про місцезнаходження; ці дані є одночасно даними про місцезнаходження *користувачів* комунікаційних пристроїв, що особливо стосується користувачів мобільних комунікаційних пристроїв.

Дані щодо трафіку можуть використовуватися постачальником послуг лише для виставлення рахунків і технічного надання послуги. Однак за наявності згоди суб'єкта персональних даних ці дані можуть бути розкриті іншим володільцям, які пропонують такі додаткові послуги, як надання інформації про місцезнаходження користувача поблизу станції метро чи аптеки або прогнозу погоди в цьому місці.

Відповідно до статті 15 Директиви про конфіденційність та електронні комунікації, інші можливості доступу до даних про комунікацію в електронних мережах, наприклад, доступ в цілях розслідування злочинів, повинні задовольняти вимогам щодо виправданого втручання у право на захист даних, закладеним у статті 8 (2) ЄКПЛ та підтвердженим у статтях 8 і 52 Хартії.

Поправки до Директиви про конфіденційність та електронні комунікації від 2009 року[291] внесли наступні зміни:

- Обмеження на відправку електронних листів з метою прямого маркетингу було поширено на служби коротких повідомлень, служби передачі мультимедійних повідомлень та інші сфери подібного застосуван-

291 Директива 2009/136/ЕС Європейського парламенту і Ради (ЄС) від 25 листопада 2009 року, що вносить зміни до Директиви 2002/22/ЕС про універсальні послуги і права користувачів, що стосуються електронних комунікаційних мереж і послуг, Директиви 2002/58/ЕС стосовно обробки персональних даних та захисту конфіденційності у секторі електронних комунікацій і Регламенту (ЄС) № 2006/2004 про співробітництво між національними органами влади, відповідальними за виконання законів про захист прав споживачів, OJ 2009 L 337.

ня; надсилання електронних листів з метою маркетингу забороняється, якщо тільки для цього не було отримано попередню згоду. Без наявності такої згоди, електронні листи з метою маркетингу можуть надсилатися тільки попереднім клієнтам, якщо вони надали свою поштову адресу і не заперечують проти цього.

- На держав-членів було покладено зобов'язання забезпечувати засоби судового захисту від порушень заборони на розсилку незапрошених повідомлень.[292]
- Налаштування файлів «cookie» і програмних засобів, які відстежують і записують дії користувача комп'ютера, більше не допускається без згоди самого користувача комп'ютера. Національне законодавство повинно більш докладно регламентувати, як слід виражати й отримувати згоду, щоб забезпечувався достатній захист.[293]

Якщо в результаті несанкціонованого доступу, втрати або знищення даних відбувається витік даних, про це повинен бути негайно проінформований компетентний наглядовий орган. Абоненти мають бути проінформовані, якщо шкода, яку їм могло бути завдано, є наслідком витоку даних.[294]

Директива про зберігання даних[295] (втратила чинність 8 квітня 2014 року, див. приклад справи нижче) зобов'язувала постачальників комунікаційних послуг зберігати доступні дані щодо трафіку, зокрема, для цілей боротьби з тяжкими злочинами впродовж не менше шести, але не більше 24 місяців, незалежно від того, чи потрібні постачальнику ці дані для виставлення рахунків або технічного надання послуг.

Держави-члени ЄС повинні визначити незалежні державні органи, які відповідатимуть за контроль за безпекою даних, що зберігаються.

---

292 Див. змінену Директиву, ст. 13.

293 Див. там само, ст. 5; див. також: Робоча група статті 29 (2012), Висновок 04/2012 щодо згоди на вилучення файлів «cookie», WP 194, Брюссель, 7 червня 2012 р.

294 Див. також: Робоча група статті 29 (2011), Робочий документ 01/2011 щодо чинної нормативної бази ЄС з питань витоку персональних даних і рекомендацій відносно майбутніх напрацювань у політиці, WP 184, Брюссель, 5 квітня 2011 р.

295 Директива 2006/24/ЕС Європейського парламенту і Ради (ЄС) від 15 березня 2006 року про зберігання даних, що генеруються або обробляються при наданні загальнодоступних послуг електронних комунікацій або громадських мереж зв'язку, яка вносить зміни до Директиви 2002/58/ЕС, OJ 2006 L 105.

Зберігання телекомунікаційних даних є явним втручанням у право на захист персональних даних.[296] Питання про те, чи є таке втручання виправданим, оскаржувалося в декількох судових процесах у державах-членах ЄС.[297]

> Приклад: У справі *«Компанія «Digital Rights Ireland» і Зайтлінгер та інші проти Ірландії»*[298] Суд ЄС визнав Директиву про зберігання персональних даних недійсною. На думку Суду, «широке й особливо серйозне втручання директиви в основні права, про які йдеться, не є достатньо обмеженим, щоб гарантувати, що таке втручання фактично обмежується тим, що є суворо необхідним.»

Втручання з боку влади є основним питанням у контексті електронних комунікацій. Використання засобів спостереження або перехоплення повідомлень, таких, як пристрої для підслуховування або прослуховування, дозволяється лише в разі, якщо це передбачено законом і є необхідним у демократичному суспільстві в інтересах охорони державної безпеки, громадської безпеки, фінансових інтересів держави або припинення кримінальних правопорушень, чи захисту суб'єкта персональних даних або прав і свобод інших осіб.

Приклад: У справі *«Мелоун проти Сполученого Королівства»*[299] *заявника було звинувачено у вчиненні ряду правопорушень, пов'язаних з незаконним володінням вкраденими речами. В процесі розгляду справи з'ясувалося, що телефонну розмову заявника було перехоплено державним органом на підставі ордера, виданого Міністром внутрішніх справ Великої Британії. Незалежно від того, що з точки зору національного законодавства спосіб, у який було перехоплено спілкування заявника, був законним, ЄСПЛ вирішив, що не існувало жодних правових норм, які б стосувалися меж і способу здійснення державними органами їхніх дискреційних повноважень у цій сфері, та що втручання, яке відбулося в результаті дій, що оскаржувалися, «не відповідало закону». Суд постановив, що мало місце порушення статті 8 ЄКПЛ.*

---

296 ЄІЗД (2011), Висновок від 31 травня 2011 року щодо Оцінювального звіту Європейської комісії для Ради (ЄС) та Європейського парламенту стосовно Директиви про захист персональних даних (Директиви 2006/24/ЕС), 31 травня 2011 р.

297 Німеччина, Федеральний Конституційний суд (*Bundesverfassungsgericht*), 1 BvR 256/08, 2 березня 2010 р; Румунія, Федеральний Конституційний суд (*Curtea Constitutionals a Romăniei*), № 1258, 8 жовтня 2009 р.; Чеська Республіка, Конституційний суд (*Ustavnisoud Ceske republiky*), 94/2011 колективне рішення, 22 березня 2011 р.

298 Суд ЄС, Об'єднані справи C-293/12 і C-594/12, *«Компанія «Digital Rights Ireland» і Зайтлінгер та інші проти Ірландії»*, 8 квітня 2014 р., п. 65.

299 ЄСПЛ, *«Мелоун проти Сполученого Королівства»*, № 8691/79, 2 серпня 1984 р.

8.2. Дані щодо працевлаштування

Ключові моменти

- Конкретні норми захисту персональних даних у трудових відносинах містяться в Рекомендації РЄ щодо даних про працевлаштування.
- У Директиві про захист персональних даних трудові відносини конкретно згадуються лише у контексті обробки чутливих даних.
- Дійсність згоди, яка мала бути вільно надана, в якості правової основи для обробки персональних даних про працівників може бути сумнівною, враховуючи відсутність економічної рівноваги між роботодавцем і працівниками. Обставини надання згоди потрібно уважно оцінювати.

В ЄС не існує жодної конкретної нормативної бази, яка б регулювала обробку персональних даних у контексті працевлаштування. У Директиві про захист персональних даних трудові відносини конкретно згадуються тільки в статті 8 (2), яка стосується обробки чутливих даних. Щодо РЄ, то в 1989 році була видана Рекомендація щодо даних про працевлаштування, яка наразі оновлюється.[300]

Огляд найпоширеніших проблем захисту персональних даних, характерних для контексту працевлаштування, можна знайти у робочому документі робочої групи «Стаття 29».[301] Робоча група проаналізувала значення згоди як правової підстави для обробки даних про зайнятість.[302] Робоча група вирішила, що відсутність економічної рівноваги між роботодавцем, який просить згоди, і працівниками, які надають її, часто викликає сумніви щодо того, чи було цю згоду надано вільно. Тому оцінюючи дійсність згоди у контексті працевлаштування потрібно уважно розглядати умови, за яких запитується така згода.

Загальною проблемою захисту персональних даних в сьогоднішньому типовому робочому середовищі є законний ступінь контролю за електронною ко-

300 Рада Європи, Комітет міністрів (1989), Рекомендація Rec(89)2 державам-членам щодо захисту персональних даних, що використовуються для працевлаштування, 18 січня 1989 р. Див. далі: Консультативний комітет Конвенції № 108, Дослідження Рекомендації № R (89)2 щодо захисту персональних даних, що використовуються для працевлаштування, і стосовно надання пропозиції щодо перегляду вищезазначеної Рекомендації, 9 вересня 2011 р.

301 Робоча група статті 29 (2001), Висновок 8/2001 щодо обробки персональних даних у контексті працевлаштування, WP 48, Брюссель, 13 вересня 2001 р.

302 Робоча група статті 29 (2005), Робочий документ стосовно спільного тлумачення статті 26 (1) Директиви 95/46/ЕС від 24 жовтня 1995 р., WP 114, Брюссель, 25 листопада 2005 р.

мунікацією працівника на робочому місці. Часто стверджують, що цю проблему можна легко вирішити шляхом заборони використання засобів зв'язку на роботі у приватних цілях. Однак така загальна заборона може бути непропорційною і нереальною. Наступне рішення ЄСПЛ є особливо цікавим у цьому контексті:

> Приклад: У справі *«Копланд проти Сполученого Королівства»*[303] за телефоном та електронною поштою працівниці коледжу, а також за використанням нею Інтернету здійснювався таємний контроль з метою з'ясувати, чи було з її боку надмірне використання обладнання коледжу в особистих цілях. ЄСПЛ постановив, що телефонні дзвінки, здійснені у службових приміщеннях, підпадали під поняття приватного життя і кореспонденції. Тому такі дзвінки й електронні листи, надіслані з роботи, а також інформація, отримана в результаті моніторингу персонального використання Інтернету, захищалися статтею 8 ЄКПЛ. У справі заявниці не існувало жодних положень, які б регулювали обставини, за яких роботодавці можуть відстежувати використання працівниками телефону, електронної пошти та Інтернету. Таким чином, втручання не відповідало закону. Суд дійшов висновку, що мало місце порушення статті 8 ЄКПЛ.

Відповідно до Рекомендації РЄ щодо даних про працевлаштування, особисті дані, що збираються в цілях працевлаштування, повинні бути отримані безпосередньо від окремого працівника.

Особисті дані, що збираються для найму, повинні обмежуватися інформацією, необхідною для оцінки придатності кандидатів та їх кар'єрного потенціалу.

У Рекомендації також конкретно зазначено про оціночні дані, які стосуються продуктивності або потенціалу окремих працівників. Оціночні дані повинні ґрунтуватися на справедливих та чесних оцінках і не повинні бути образливими у своєму формулюванні. Цього вимагають принципи ретельної обробки і точності даних.

Особливим аспектом законодавства у сфері захисту персональних даних у відносинах між роботодавцем і працівниками є роль представників працівників. Такі представники можуть отримати персональні дані працівників лише в обсязі, необхідному, щоб мати можливість представляти інтереси працівників.

303 ЄСПЛ, *«Копланд проти Сполученого Королівства»*, № 62617/00, 3 квітня 2007 р.

Чутливі дані, зібрані в цілях працевлаштування, можуть оброблятися лише в окремих випадках і згідно з гарантіями, закладеними в національному законодавстві. Роботодавці можуть запитувати працівників або кандидатів на робоче місце про стан їх здоров'я або проводити їх медичний огляд тільки в разі, якщо це необхідно для визначення їх придатності для працевлаштування, дотримання вимог профілактичної медицини, або надання дозволу на призначення соціальних пільг. Дані про стан здоров'я не можна збирати з інших джерел, аніж у відповідного працівника, крім випадків, коли для цього було отримано явно виражену та поінформовану згоду або коли це передбачено національним законодавством.

Згідно з Рекомендацією щодо даних про працевлаштування, працівники повинні бути проінформовані про мету обробки їх персональних даних, тип персональних даних, що зберігаються, суб'єктів, яким регулярно повідомляються ці дані, мету та правову основу таких повідомлень. Роботодавці також повинні заздалегідь інформувати своїх працівників про встановлення чи адаптування автоматизованих систем обробки персональних даних працівників або контролю за переміщенням чи продуктивністю роботи працівників.

Працівники повинні мати право на доступ до своїх даних щодо працевлаштування, а також право на їх виправлення чи вилучення. Якщо обробляються оціночні дані, працівники також повинні мати право на оскарження цієї оцінки. Однак ці права можуть тимчасово обмежуватися з метою проведення внутрішніх розслідувань. Якщо працівнику було відмовлено у наданні доступу, виправленні або стиранні персональних даних щодо працевлаштування, національне законодавство має передбачати належні процедури оскарження відмови.

8.3. Медичні дані

Ключовий момент

- Медичні дані є чутливими даними, а тому їм надається особливий захист.

Відповідно до статті 8 (1) Директиви про захист персональних даних і статті 6 Конвенції № 108, персональні дані, що стосуються стану здоров'я суб'єкта персональних даних, кваліфікуються як чутливі дані. У свою чергу, медичні дані можуть підлягати суворішому режиму обробки даних, аніж нечутливі дані.

Приклад: У справі *«Z. проти Фінляндії»*[304] колишній чоловік заявниці, який був інфікований ВІЛ, скоїв ряд статевих злочинів. Згодом його було засуджено за ненавмисне вбивство на тій підставі, що він свідомо піддавав своїх жертв ризику інфікування ВІЛ-інфекцією. Національний суд розпорядився, щоб повне рішення і документи справи залишалися конфіденційними протягом 10 років, незважаючи на запити заявника щодо встановлення тривалішого періоду конфіденційності. Апеляційний суд відмовив у цих запитах, а його рішення містило повні імена заявниці та її колишнього чоловіка. ЄСПЛ постановив, що втручання не вважалося необхідним у демократичному суспільстві, оскільки захист медичних даних має фундаментальне значення для здійснення права на повагу до приватного і сімейного життя, особливо коли йдеться про інформацію щодо ВІЛ-інфекції, враховуючи стигматизацію, яка викликана цією хворобою у багатьох спільнотах. Таким чином, Суд дійшов висновку, що надання доступу до інформації про особу заявника і стан його здоров'я, як це мало місце у рішенні апеляційного суду після завершення 10-річного періоду з часу прийняття рішення, порушувало статтю 8 ЄКПЛ.

Стаття 8 (3) Директиви про захист персональних даних дозволяє обробку медичних даних, якщо вона є необхідною з метою профілактичної медицини, медичної діагностики, надання медичних послуг чи лікування або для керування служб охорони здоров'я. Проте обробка є допустимою тільки тоді, коли вона здійснюється медичним працівником, зв'язаним зобов'язанням збереження професійної таємниці, чи іншою особою, що зв'язана подібним зобов'язанням.[305]

Рекомендація РЄ щодо медичних даних від 1997 року більш докладно застосовує принципи Конвенції № 108 до обробки даних у сфері медицини.[306] Запропоновані норми відповідають нормам Директиви про захист персональних даних відносно законних цілей обробки медичних даних, існування в осіб, що використовують дані про стан здоров'я, необхідних зобов'язань збереження професійної таємниці, та прав суб'єктів персональних даних на про-

304 ЄСПЛ, *«Z. проти Фінляндії»*, № 22009/93, 25 лютого 1997 р., пп. 94 і 112; див. також: ЄСПЛ, *«M.C проти Швеції»*, № 20837/92, 27 серпня 1997 р.; ЄСПЛ, *«Л.Л. проти Франції»*, № 7508/02, 10 жовтня 2006 р.; ЄСПЛ, *«I. проти Фінляндії»*, № 20511/03, 17 липня 2008 р.; ЄСПЛ, *«К.Х. та інші проти Словаччини»*, № 32881/04, 28 квітня 2009 р.; ЄСПД, *«Жулук проти Сполученого Королівства»*, № 36936/05, 2 червня 2009 р.

305 Див. також ЄСПЛ, *«Бірюк проти Литви»*, № 23373/03, 25 листопада 2008 р.

306 РЄ, Комітет міністрів (1997), Рекомендація Rec(97)5 державам-членам щодо захисту медичних даних, 13 лютого 1997 р.

зорість і доступ, виправлення і видалення. Крім того, медичні дані, які на законних підставах обробляють медичні працівники, не можуть передаватися правоохоронним органам, якщо тільки не надано «достатні гарантії для запобігання розкриттю, несумісному з повагою до [...] приватного життя, гарантованою статтею 8 ЄКПЛ».[307]

Крім того, Рекомендація щодо медичних даних містить спеціальні положення стосовно медичних даних ненароджених дітей і недієздатних осіб, а також обробки генетичних даних. Наукові дослідження прямо визнано підставою зберігати дані довше, аніж доки вони є необхідними, хоча це зазвичай вимагає анонімізації. Стаття 12 Рекомендації щодо медичних даних пропонує детальні інструкції для ситуацій, коли дослідникам потрібні персональні дані, а анонімних даних недостатньо.

Псевдонімізація може бути доречним засобом задоволення наукових потреб і водночас захисту інтересів відповідних пацієнтів. В контексті захисту даних поняття псевдонімізації більш докладно пояснюється в підрозділі 2.1.3.

На національному та європейському рівнях відбувається інтенсивне обговорення ініціатив щодо зберігання даних про лікування пацієнта в електронному медичному записі.[308] Особливим аспектом питання про існування загальнонаціональних систем електронних медичних записів є їх доступність через кордони: ця тема становить особливий інтерес в рамках ЄС у контексті транскордонної охорони здоров'я.[309]

Ще однією сферою дискусії з приводу нових положень є клінічні випробування, інакше кажучи, перевірка нових ліків на пацієнтах у документально зафіксованому дослідницькому середовищі; крім того, ця тема має значні наслідки для захисту даних. Проведення клінічних випробувань лікарських засобів для вживання людьми регулюється Директивою 2001/20/ЕС Європейського парламенту і Ради (ЄС) від 4 квітня 2001 року щодо наближення законів, підзаконних та адміністративних актів держав-членів стосовно імплементації належної клінічної практики при проведенні клінічних випробувань лікар-

307 ЄСПЛ, № 1585/09, *«Авілкіна та інші проти Росії»*, № 1585/09, 6 червня 2013 р., п. 53 (не остаточне).

308 Робоча група статті 29 (2007), Робочий документ щодо обробки персональних даних, які стосуються стану здоров'я, в електронних медичних записах (ЕМЗ), WP 131, Брюссель, 15 лютого 2007 р.

309 Директива 2011/24/EU Європейського парламенту і Ради (ЄС) від 9 березня 2011 р. про застосування прав пацієнтів у транскордонній системі охорони здоров'я, OJ 2011 L 88.

ських засобів для вживання людьми (*Директива про клінічні випробування*).[310] У грудні 2012 року з метою зробити процедури випробування більш однорідними та ефективними Європейська комісія запропонувала регламент на заміну Директиві про клінічні випробування.[311]

На рівні ЄС очікують вирішення багато законодавчих та інших ініціатив відносно персональних даних у секторі охорони здоров'я.[312]

8.4. Обробка персональних даних у статистичних цілях

Ключові моменти

- Персональні дані, зібрані у статистичних цілях, не можуть використовуватися в будь-яких інших цілях.
- Персональні дані, зібрані на законних підставах з будь-якою метою, можуть далі використовуватися у статистичних цілях, за умови, що національне законодавство встановлює адекватні гарантії, які використовують користувачі. Для цього до передачі даних третім особам має бути передбачена, зокрема, їх анонімізація або псевдонімізація.

У Директиві про захист персональних даних обробка даних у статистичних цілях зазначається в контексті можливих винятків із принципів захисту персональних даних. Згідно зі статтею 6 (1) (b) Директиви, відповідно до національного законодавства від принципу цільового обмеження можна відмовитися на користь подальшого використання даних у статистичних цілях, хоча національне законодавство також повинно передбачати усі необхідні гарантії. Стаття 13 (2) Директиви дозволяє обмежувати право на доступ відповідно до національного законодавства, якщо дані обробляються виключно у ста-

310 Директива 2001/20/ЕС Європейського парламенту і Ради (ЄС) від 4 квітня 2001 року щодо наближення законів, підзаконних та адміністративних актів держав-членів стосовно імплементації належної клінічної практики при проведенні клінічних випробувань лікарських засобів для вживання людьми, OJ 2001 L 121.

311 Європейська комісія (2012), Пропозиція щодо Регламенту Європейського парламенту і Ради (ЄС) щодо клінічних випробувань лікарських засобів для вживання людьми і скасування Директиви 2001/20/ЕС, COM(2012) 369 остаточна версія, Брюссель, 17 липня 2012 р.

312 ЄІЗД (2013), Висновок Інспектора з захисту персональних даних щодо Комюніке Комісії стосовно Плану дій «eHealth» на 2012–2020 роки – «Інноваційна система охорони здоров'я в 21 столітті», Брюссель, 27 березня 2013 р.

тистичних цілях; знову ж, у національному законодавстві повинні існувати адекватні гарантії. В цьому контексті Директива про захист персональних даних встановлює особливу вимогу, яка передбачає, що жодні дані, одержані чи створені в процесі статистичного дослідження, не можуть використовуватися для прийняття конкретних рішень стосовно суб'єкта персональних даних.

Хоча дані, які були на законній підставі й у будь-яких цілях зібрані володільцем, можуть бути повторно використані цим володільцем у власних статистичних цілях – для так званої вторинної статистики – залежно від контексту, перед передачею цих даних третій стороні для статистичних цілей вони повинні бути анонімізовані або псевдонімізовані, якщо лише суб'єкт персональних даних не дав на це згоду чи це конкретно не передбачено національним законодавством. Це випливає з вимоги стосовно існування відповідних гарантій, передбаченої статтею 6 (1) (b) Директиви про захист персональних даних.

Найважливішими випадками використання даних у статистичних цілях є офіційна статистична діяльність, що здійснюється національним бюро статистики і бюро статистики ЄС на підставі національного права і права ЄС у сфері офіційної статистики. Відповідно до цього законодавства, громадяни і бізнес, як правило, зобов'язані розкривати персональні дані органам статистики. Посадовці, які працюють в бюро статистики, пов'язані спеціальними зобов'язаннями збереження професійної таємниці, яких вони ретельно дотримуються, оскільки це є важливим для високого рівня довіри громадян, яка є необхідною, якщо дані мають надаватися органам статистики.

Регламент (ЕС) № 223/2009 щодо європейської статистики (*Регламент щодо європейської статистики*) містить неодмінні норми захисту даних в офіційній статистичній діяльності, а тому також може вважатися таким, що стосується положень щодо офіційної статистичної діяльності на національному рівні.[313]

Положення підтримує принцип, згідно з яким офіційні статистичні операції потребують досить точної правової підстави.[314]

313 Регламент (ЄС) № 223/2009 Європейського парламенту і Ради (ЄС) від 11 березня 2009 року щодо європейської статистики і скасування Регламенту (ЄС, Євратом) № 1101/2008 Європейського парламенту і Ради (ЄС) про передачу даних, на які поширюється статистична конфіденційність, Статистичній службі Європейських Співтовариств, Регламенту Ради (ЄС) № 322/97 щодо статистики Співтовариства, і Рішення Ради (ЄС) 89/382/ЕЕС, Євратом про створення Комітету статистичних програм Європейських Співтовариств, OJ 2009 L 87.

314 Цей принцип має бути більш докладно викладеним у Кодексі практики Євростату, який відповідно до статті 11 Регламенту щодо європейської статистики наводить етичні правила здійснення офіційної статистичної діяльності, в тому числі й уважне використання персональних даних; доступно за посиланням: http://epp.eurostat.ec.europa.eu/portal/page/portal/about_eurostat/introduction.

Приклад: У справі *«Губер проти Німеччини»*[315] Суд ЄС постановив, що збирання і зберігання персональних даних державним органом у статистичних цілях не були самі по собі достатньою підставою вважати обробку правомірною. Закон, що передбачав обробку персональних даних, також мав задовольняти вимозі щодо необхідності, що не мало місце в цьому контексті.

В контексті РЄ Рекомендація щодо статистичних даних, видана в 1997 році, охоплює статистичну діяльність в державному та приватному секторах.[316] Ця рекомендація ввела принципи, які збігаються з основними нормами Директиви про захист персональних даних, описаними вище. Стосовно наступних питань наведено більш докладні норми.

У той час як дані, зібрані володільцем у статистичних цілях, не можуть використовуватися в будь-яких інших цілях, дані, які було зібрано у нестатистичних цілях, є доступними для подальшого використання в статистичних цілях. Рекомендація щодо статистичних даних навіть дозволяє повідомлення даних третім особам, якщо це робиться лише у статистичних цілях. В таких випадках сторони повинні домовитися і визначити межі подальшого законного використання даних для статистики. Оскільки це не може замінити згоду суб'єкта персональних даних, слід припустити, що повинні існувати додаткові належні гарантії, передбачені національним законодавством для мінімізації ризиків зловживання особистими даними, наприклад, зобов'язання анонімізувати або псевдонімізувати такі дані перед передачею.

Особи, які професійно займаються статистичними дослідженнями, повинні бути пов'язані спеціальними зобов'язаннями збереження професійної таємниці відповідно до національного законодавства, що є характерним для офіційної статистики. Ця вимога має поширюватися і на осіб, які проводять опитування, якщо вони працюють, збираючи дані в суб'єктів персональних даних чи інших осіб.

Якщо статистичне дослідження з використанням персональних даних не передбачене законом, суб'єкти персональних даних повинні надати згоду на використання своїх даних, щоб воно було законним чи щоб вони хоча

315 Суд ЄС, C-524/06, *«Губер проти Німеччини»*, 16 грудня 2008 р.; див., зокрема, п. 68.

316 Рада Європи, Комітет міністрів (1997), Рекомендація Rec(97)18 державам-членам щодо захисту персональних даних, які збираються й обробляються у статистичних цілях, 30 вересня 1997 р.

б мали можливість висунути заперечення. Якщо персональні дані збираються у статистичних цілях шляхом опитування осіб, ці особи повинні бути чітко проінформовані про те, чи є розкриття даних обов'язковим за національним законодавством. Чутливі дані у жодному разі не повинні збиратися у такий спосіб, щоб особу можна було ідентифікувати, якщо тільки це конкретно не дозволяється національним законодавством.

Якщо статистичне дослідження не може бути проведене без анонімних даних, а персональні дані є дійсно необхідними, дані, зібрані з цією метою, повинні бути анонімізованими, як тільки це стане можливим. Результати статистичного дослідження не повинні, принаймні, дозволяти ідентифікацію будь-якого з суб'єктів персональних даних, якщо тільки це явно не становитиме жодного ризику.

Після завершення статистичного аналізу використані персональні дані повинні або бути видаленими, або вважатися анонімними. В цьому випадку Рекомендація щодо статистичних даних пропонує зберігати ідентифікаційні дані окремо від інших персональних даних. Це означає, наприклад, що дані мають бути псевдонімізовані, а ключ шифрування чи список з ідентифікуючими синонімами – зберігатися окремо від псевдонімізованих даних.

8.5. Фінансові дані

Ключові моменти

- Хоча фінансові дані не є чутливими даними в розумінні Конвенції № 108 або Директиви про захист персональних даних, їх обробка вимагає особливих гарантій для забезпечення точності і безпеки даних.
- Електронні платіжні системи повинні мати «вбудований» захист даних, так звану заплановану конфіденційність.
- Особливі проблеми захисту даних постають у цій сфері з необхідності мати в наявності належні механізми аутентифікації.

Приклад: У справі *«Мішо проти Франції»*[317] заявник, французький юрист, оскаржував своє зобов'язання за французьким законодавством повідомля-

317 ЄСПЛ, *«Мішо проти Франції»*, № 12323/11, 6 грудня 2012 р.; див. також: ЄСПЛ, *«Німітц проти Німеччини»*, № 13710/88, 16 грудня 1992 р., п. 29, і ЄСПЛ, *«Гелфорд проти Сполученого Королівства»*, № 20605/92, 25 червня 1997 р., п. 42.

ти про підозри щодо можливої діяльності з відмивання грошей своїх клієнтів. ЄСПЛ зауважив, що вимога до адвокатів повідомляти адміністративним органам інформацію стосовно іншої особи, яка стала їм відома шляхом спілкування з цією особою, становила втручання у право адвокатів на повагу до кореспонденції і приватного життя, гарантовану статтею 8 ЄКПЛ, оскільки це поняття охоплює діяльність професійного і ділового характеру. Проте втручання здійснювалося відповідно до закону і переслідувало законну мету, а саме запобігання заворушенням та злочинності. Оскільки на адвокатів покладалося зобов'язання повідомляти про свої підозри тільки за дуже обмежених обставин, ЄСПЛ постановив, що це зобов'язання було пропорційним, та вирішив, що порушення статті 8 не було.

Застосування загальної правової системи у сфері захисту персональних даних, що міститься в Конвенції № 108, в контексті платежів було розширено РЄ у Рекомендації Rec (90) 19 від 1990 року.[318] Ця рекомендація роз'яснює питання щодо меж законного збирання і використання даних в контексті платежів, особливо за допомогою платіжних карт. Крім того, вона пропонує національним законодавцям докладні норми щодо меж повідомлення платіжних даних третім особам, строків збереження даних, прозорості, безпеки даних і транскордонної передачі даних та, нарешті, щодо нагляду і засобів правового захисту. Запропоновані рішення відповідають тому, що було пізніше передбачено в Директиві про захист персональних даних як загальна система захисту даних ЄС.

Для регулювання ринків фінансових інструментів і діяльності кредитних установ та інвестиційних компаній створюється ряд правових документів.[319] Інші правові документи допомагають у боротьбі з інсайдерськими операціями та

318 РЄ, Комітет міністрів (1990), Рекомендація № R(90)19 щодо захисту персональних даних, що використовуються для розрахункових та інших суміжних операцій, 13 вересня 1990 р.

319 Європейська комісія (2011), Пропозиція стосовно Директиви Європейського парламенту і Ради (ЄС) про ринки фінансових інструментів, яка скасовує Директиву 2004/39/ЕС Європейського парламенту і Ради (ЄС), COM(2011)656 остаточна версія, Брюссель, 20 жовтня 2011 р.; Європейська комісія (2011), Пропозиція стосовно Регламенту Європейського парламенту і Ради (ЄС) щодо ринків фінансових інструментів, який вносить зміни до Регламенту [EMIR] щодо позабіржових деривативів, центральних контрагентів і торгових репозиторіїв, COM(2011)652 остаточна версія., Брюссель, 20 жовтня 2011 р.; Європейська комісія (2011), Пропозиція стосовно Директиви Європейського парламенту і Ради (ЄС) про доступ до діяльності кредитних організацій та пруденційний нагляд за діяльністю кредитних установ та інвестиційних компаній і внесення змін до Директиви 2002/87/ЕС Європейського парламенту і Ради (ЄС) щодо додаткового нагляду за кредитними установами, страховими компаніями та інвестиційними компаніями у фінансовому конгломераті, COM(2011)453 остаточна версія, Брюссель, 20 липня 2011 р.

маніпуляціями на ринку.[320] Найважливішими проблемами у цих сферах, які впливають на захист персональних даних, є:

- збереження записів про фінансові транзакції;
- передача персональних даних третім країнам;
- запис телефонних розмов чи електронних повідомлень, в тому числі повноваження компетентних органів запитувати записи телефонних розмов і дані щодо трафіку;
- розкриття персональної інформації, включаючи публікування санкцій;
- наглядові та слідчі повноваження компетентних органів, у тому числі інспекції на місцях і вхід до приватних приміщень для конфіскації документів;
- механізми повідомлень про порушення, тобто схеми роботи інформаторів; і
- співробітництво між компетентними органами держав-членів та Європейським органом з цінних паперів та ринків (ЄОЦПР).

У цих сферах особливу увагу приділено й іншим питанням, у тому числі питанню збирання даних про фінансовий стан суб'єктів персональних даних[321] або транскордонний платіж шляхом здійснення банківських переказів, які неминуче викликають персональні потоки даних.[322]

320 Європейська комісія (2011), Пропозиція стосовно Регламенту Європейського парламенту і Ради (ЄС) про інсайдерські операції та маніпуляції на ринку (зловживання на ринку), COM(2011)651 остаточна версія, Брюссель, 20 жовтня 2011; Європейська комісія (2011), Пропозиція стосовно Директиви Європейського парламенту і Ради (ЄС) про кримінальні санкції за інсайдерські операції та маніпуляції на ринку, COM(2011)654 остаточна версія, Брюссель, 20 жовтня 2011 р.

321 Регламент (ЄС) № 1060/2009 Європейського парламенту і Ради (ЄС) від 16 вересня 2009 року щодо кредитно-рейтингових агенцій, OJ 2009 L 302; Європейська комісія, Пропозиція щодо Регламенту Європейського парламенту і Ради (ЄС), який вносить зміни до Регламенту (ЄС) № 1060/2009 щодо кредитно-рейтингових агенцій, COM(2010)289 остаточна версія, Брюссель, 2 червня 2010 р.

322 Директива 2007/64/ЕС Європейського парламенту і Ради (ЄС) від 13 листопада 2007 року про платіжні послуги на внутрішньому ринку, яка вносить зміни до Директив 97/7/ЕС, 2002/65/ЕС, 2005/60/ЕС і 2006/48/ЕС та скасовує Директиву 97/5/ЕС, OJ 2007 L 319.

Додаткові джерела інформації

Розділ 1

Араселі Манга, М. (ред.) (2008 р.), Хартія основних прав Європейського Союзу, Більбао, Фонд BBVA.

Берка, В. (2012 р.), Фундаментальне право на захист персональних даних у конфлікті між свободою і безпекою, Відень, Видавництво «Manzsche Verlags- und Universitätsbuchhandlung».

Грабенвартер, К. і Пабел, К. (2012 р.), Європейська конвенція з прав людини, Мюнхен, Видавництво «C. H. Beck».

Джарасс, Х. (2010 р.), Хартія основних прав Європейського Союзу, Мюнхен, Видавництво «C. H. Beck».

Європейські цифрові права (EDRi), Вступ до захисту персональних даних, Брюссель, доступно за посиланням: www.edri.org/files/paper06_datap.pdf.

Майєр, Дж. (2011 р.), Хартія основних прав Європейського Союзу, Баден-Баден, Видавництво «Nomos».

Моубрей, А. (2012 р.), Справи, матеріали та коментарі до Європейської конвенції з прав людини, Оксфорд, Видавництво «Oxford University Press».

Новак, М., Янушевскі, К. і Хофстеттер, Т. (2012 р.), Усі права людини для всіх – віденський посібник з прав людини, Антверпен, Видавництва «Intersentia N. V.», «Neuer Wissenschaftlicher».

Пішарель, С. і Кутрон, Л. (2010 р.), Хартія основних прав Європейського Союзу та Європейська конвенція з прав людини, Брюссель, Видавництво «Emile Bruylant».

Сімітіс, С. (1997 р.), «Директива ЄС про захист даних – застій чи стимул?», Новий юридичний тижневик (Neue Juristische Wochenschrift), № 5, С. 281–288.

Уайт, Р. і Ові, С. (2010 р.), Європейська конвенція з прав людини, Оксфорд, Видавництво «Oxford University Press».

Уоррен, С. і Брандейс, Л. (1890 р.), «Право на приватність», Гарвардський юридичний журнал (Harvard Law Review), Том 4, № 5, С. 193–220, доступно за посиланням: http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf.

Фровайн, Й. і Пойкерт, В. (2009 р.), Європейська конвенція з прав людини, Берлін, Видавництво «N. P. Engel».

Харріс, Д., О'Бойл, М., Ворбрік, Ц. і Бейтс, Е. (2009 р.), Право Європейської конвенції з прав людини, Оксфорд, Видавництво «Oxford University Press».

Розділ 2

Дельгадо, Л. (2008 р.), Конфіденційність та захист персональних даних в Європейському Союзі, Мадрид, Видавництво «Dykinson S. L.».

Десжен-Пасану, Г. (2012 р.), Захист інформації персонального характеру, Париж, Видавництво «LexisNexis».

Ді Мартіно, А. (2005 р.), Захист персональних даних у європейському праві, Баден-Баден, Видавництво «Nomos».

Кері, П. (2009 р.), Захист персональних даних: Практичний посібник з права Сполученого Королівства і ЄС, Оксфорд, Видавництво «Oxford University Press».

Марган, Р. і Бордман, Р. (2012 р.), Стратегія захисту персональних даних: Реалізація дотримання захисту персональних даних, Лондон, Видавництво «Sweet & Maxwell».

Ом, П. (2010 р.), «Невиконана обіцянка зберігати приватність: Відповідаючи на разюче недотримання анонімності», Юридичний журнал Каліфорнійського університету (UCLA Law Review), Том 57, № 6, С. 1701–1777.

Тіннефельд, М., Бухнер, Б. і Петрі, Т. (2012 р.), Вступ до захисту персональних даних: Захист даних та свобода інформації в європейській перспективі, Мюнхен, Видавництво «Oldenbourg Wissenschaftsverlag».

Управління комісара з інформації Сполученого Королівства (2012 р.), Анонімізація: управління ризиками захисту персональних даних. Кодекс практики, доступно за посиланням: www.ico.org.uk/%20for_organisations/data_protection/topic_guides/anonymisation.

Розділи 3–5

АОП (Агенція Європейського Союзу з питань основних прав) (2010 р.), Захист персональних даних у Європейському Союзі: роль національних органів з питань захисту даних (Зміцнення структури основних прав в ЄС II), Люксембург, Бюро публікацій Європейського Союзу (Бюро публікацій).

АОП (2010 р.), Розробка показників для захисту, поваги та заохочення прав дитини у Європейському Союзі (видання для конференції), Відень, АОП.

АОП (2011 р.), Доступ до правосуддя в Європі: огляд викликів та можливостей, Люксембург, Бюро публікацій.

Брюганн, У. (2012 р.), «Директива 95/46/ЕС «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» у: Грабіц, Е., Хільф, М. і Неттесхайм, М. (ред.), Право Європейського Союзу, Том IV, А. 30, Мюнхен, Видавництво «C. H. Beck».

Дамманн, У. і Сімітіс, С. (1997 р.), Директива ЄС про захист персональних даних, Баден-Баден, Видавництво «Nomos».

Конде Ортіс, К. (2008 р.), Захист персональних даних, Кадіс, Видавництво «Dykinson».

Кудре, Л. (2010 р.), Захист персональних даних у Європейському Союзі, Саарбрюкен, Видавництво «Editions universitaires europeennes».

Сімітіс, С. (2011 р.), Федеральний закон про захист персональних даних, Баден-Баден, Видавництво «Nomos«.

Управління комісара з інформації Сполученого Королівства, Оцінка впливу конфіденційності, доступно за посиланням: www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.

Розділ 6

Гутвірт, С., Пулле, У., Де Герт, П., Де Тервань, С. і Нувт, С. (2009 р.), Повторний винахід захисту персональних даних?, Берлін, Видавництво «Springer».

Кюнер, С. (2007 р.), Європейське інформаційне право, Оксфорд, Видавництво «Oxford University Press».

Кюнер, С. (2013 р.), Законодавство про транскордонну передачу персональних даних і закон про конфіденційність даних, Оксфорд, Видавництво «Oxford University Press».

Розділ 7

Гутвірт, С., Пулле, У. і Де Герт, П. (2010 р.), Захист персональних даних у профільованому світі, Дордрехт, Видавництво «Springer».

Гутвірт, С., Пулле, У., Де Герт, П. і Лінс, Р. (2011 р.), Комп'ютери, конфіденційність і захист персональних даних: Елемент вибору, Дордрехт, Видавництво «Springer».

Дрюер, Д. і Еллерманн, Дж. (2012 р.), Система захисту персональних даних Європолу як актив у боротьбі з кіберзлочинністю, Форум ERA, Том 13, № 3, С. 381–395.

Європол (2012 р.), Захист персональних даних у Європолі, Люксембург, Бюро публікацій, доступно за посиланням: www.europol.europa.eu/sites/default/files/publications/europol_dpo_book-let_0.pdf.

Євроюст, Захист персональних даних у Євроюсті: Надійний, ефективний та спеціалізований режим, Гаага, Євроюст.

Констадінідес, Т. (2011 р.), Знищення демократії під приводом її захисту? Директива про зберігання даних, стан нагляду та наша конституційна екосистема, журнал «Європейський юридичний огляд», Том 36, № 5, С. 722–776.

Сантос Вара, Х. (2013 р.), Роль Європейського парламенту в укладенні трансатлантичних угод про передачу персональних даних після Лісабонської угоди, Центр права зовнішніх зносин ЄС, Робочі матеріали ЦПЗЗ – 2013/2, доступно за посиланням: www.asser.nl/upload/documents/20130226T013310-cleer_13-2_web.pdf.

Розділ 8

Бюллесбах, А., Гійрат, С., Пулле, У. і Хакон, Р. (2010 р.), Короткий огляд європейського права у сфері інформаційних технологій, Амстердам, Видавництво «Kluwer Law International».

Гутвірт, С., Лінс, Р., Де Герт, П. і Пулле, У. (2012 р.), Європейський захист персональних даних: чи в доброму стані?, Дордрехт, Видавництво «Springer».

Гутвірт, С., Пулле, У. і Де Герт, П. (2010 р.), Захист персональних даних у профільованому світі, Дордрехт, Видавництво «Springer».

Гутвірт, С., Пулле, У., Де Герт, П. і Лінс, Р. (2011 р.), Комп'ютери, конфіденційність і захист персональних даних: Елемент вибору, Дордрехт, Видавництво «Springer».

Констадінідес, Т. (2011 р.), Знищення демократії під приводом її захисту? Директива про зберігання персональних даних, стан нагляду та наша конституційна екосистема, журнал «Європейський юридичний огляд», Том 36, № 5, С. 722–776.

Розмарі, Дж. і Гамільтон, А. (2012 р.), Законодавство і практика захисту персональних даних, Лондон, Видавництво «Sweet & Maxwell».

Судова практика

Вибрана практика Європейського суду з прав людини

Доступ до персональних даних

«Гаскін проти Сполученого Королівства» («Gaskin v. the United Kingdom»), № 10454/83, 7 липня 1989 р.

«Годеллі проти Італії» («Godelli v. Italy»), № 33783/09, 25 вересня 2012 р.

«К.Х. та інші проти Словаччини» («K.H. and Others v. Slovakia»), № 32881/04, 28 квітня 2009 р.

«Леандер проти Швеції» («Leander v. Sweden»), № 9248/81, 26 березня 1987 р.

«Одієвр проти Франції» («Odievre v. France») [GC], № 42326/98, 13 лютого 2003 р.

Баланс між захистом персональних даних та свободою вираження поглядів

«Аксель Шпрінгер АГ проти Німеччини» («Axel Springer AG v. Germany«) [GC], № 39954/08, 7 лютого 2012 р.

«Фон Ганновер проти Німеччини» («Von Hannover v. Germany»), № 59320/00, 24 червня 2004 р.

«Фон Ганновер проти Німеччини» («Von Hannover v. Germany») (№ 2) [GC], № 40660/08 і 60641/08, 7 лютого 2012 р.

Проблеми захисту персональних даних в режимі онлайн

«К.У. проти Фінляндії» («K.U. v. Finland»), № 2872/02, 2 грудня 2008 р.

Листування

«Аманн проти Швейцарії» («Amann v. Switzerland«) [GC], № 27798/95, 16 лютого 2000 р.

«Араламбіє проти Румунії» («Haralambie v. Romania»), № 21737/03, 27 жовтня 2009 р.

«Бернх Ларсен Холдинг АС» та інші проти Норвегії» («Bernh Larsen Holding AS and Others v. Norway»), № 24117/08, 14 березня 2013 р.

«Гаскін проти Сполученого Королівства» («Gaskin v. the United Kingdom»), № 10454/83, 7 липня 1989 р.

«Даля проти Франції» («Dalea v. France»), № 964/07, 2 лютого 2010 р.

«Джемалеттін Джанли проти Туреччини» («Cemalettin Canli v. Turkey»), № 22427/04, 18 листопада 2008 р.

«Леандер проти Швеції» («Leander v. Sweden»), № 9248/81, 26 березня 1987 р.

«МакМайкл проти Сполученого Королівства» («McMichael v. the United Kingdom»), № 16424/90, 24 лютого 1995 р.

«М.Г. проти Сполученого Королівства» («M.G. v. the United Kingdom»), № 39393/98, 24 вересня 2002 р.

«Мелоун проти Сполученого Королівства» («Malone v. the United Kingdom»), № 8691/79, 2 серпня 1984 р.

«Ротару проти Румунії» («Rotaru v. Romania») [GC], № 28341/95, 4 травня 2000 р.

«С. і Марпер проти Сполученого Королівства» («S. and Marper v. the United Kingdom»), №. 30562/04 і 30566/04, 4 грудня 2008 р.

«Турек проти Словаччини» («Turek v. Slovakia»), № 57986/00, 14 лютого 2006 р.

«Хелілі проти Швейцарії» («Khelili v. Switzerland»), № 16188/07, 18 жовтня 2011 р.

«Шимоволос проти Росії» («Shimovolos v. Russia»), № 30194/09, 21 червня 2011 р.

Бази даних щодо судимостей

«Б.Б. проти Франції» («B.B. v. France»), № 5335/06, 17 грудня 2009 р.

«М.М. проти Сполученого Королівства» («M.M. v. the United Kingdom»), № 24029/07, 13 листопада 2012 р.

Бази даних ДНК

«С. і Марпер проти Сполученого Королівства» («S. and Marper v. the United Kingdom»), № 30562/04 і 30566/04, 4 грудня 2008 р.

GPS-дані

«Узун проти Німеччини» («Uzun v. Germany»), № 35623/05, 2 вересня 2010 р.

Дані про стан здоров'я

«Бірюк проти Литви» («Biriuk v. Lithuania»), № 23373/03, 25 листопада 2008 р.

«Жулук проти Сполученого Королівства» («Szuluk v. the United Kingdom»), № 36936/05, 2 червня 2009 р.

«З. проти Фінляндії» («Z. v. Finland»), № 22009/93, 25 лютого 1997 р.

«І. проти Фінляндії» («I. v. Finland»), № 20511/03, 17 липня 2008 р.

«Л.Л. проти Франції» («L.L. v. France»), № 7508/02, 10 жовтня 2006 р.

«М.С. проти Швеції» («M.S. v. Sweden»), № 20837/92, 27 серпня 1997 р.

Ідентифікаційна інформація

«Годеллі проти Італії» («Godelli v. Italy»), № 33783/09, 25 вересня 2012 р.

«Одієвр проти Франції» («Odievre v. France») [GC], № 42326/98, 13 лютого 2003 р.

«Чуботару проти Молдови» («Ciubotaru v. Moldova»), № 27138/04, 27 квітня 2010 р.

Інформація про професійну діяльність

«Мішо проти Франції» («Michaud v. France»), № 12323/11, 6 грудня 2012 р.

«Німітц проти Німеччини» («Niemietz v. Germany»), № 13710/88, 16 грудня 1992 р.

Перехоплення повідомлень

«Аманн проти Швейцарії» («Amann v. Switzerland«) [GC], № 27798/95, 16 лютого 2000 р.

«Гелфорд проти Сполученого Королівства» («Halford v. the United Kingdom»), № 20605/92, 25 червня 1997 р.

«Жулук проти Сполученого Королівства» («Szuluk v. the United Kingdom»), № 36936/05, 2 червня 2009 р.

«Копланд проти Сполученого Королівства» («Copland v. the United Kingdom»), № 62617/00, 3 квітня 2007 р.

«Котлец проти Румунії» («Cotlet v. Romania»), № 38565/97, 3 червень 2003 р.

«Крюслен проти Франції» («Kruslin v. France»), № 11801/85, 24 квітень 1990 р.

«Ламберт проти Франції» («Lambert v. France»), № 23618/94, 24 серпня 1998 р.

«Ліберті» та інші проти Сполученого Королівства» («Liberty and Others v. The United Kingdom»), № 58243/00, 1 липня 2008 р.

«Мелоун проти Сполученого Королівства» («Malone v. the United Kingdom»), № 8691/79, 2 серпня 1984 р.

Обов'язки володільців

«Б.Б. проти Франції» («B.B. v. France»), № 5335/06, 17 грудня 2009 р.

«І. проти Фінляндії» («I. v. Finland»), № 20511/03, 17 липня 2008 р.

«Мослі проти Сполученого Королівства» («Mosley v. the United Kingdom»), № 48009/08, 10 травня 2011 р.

Фотографії

«Фон Ганновер проти Німеччини» («Von Hannover v. Germany»), № 59320/00, 24 червня 2004 р.

«Шіакка проти Італії» («Sciacca v. Italy»), № 50774/99, 11 січня 2005 р.

Право бути забутим

«Сегерштед-Віберг та інші проти Швеції» («Segerstedt-Wiberg and Others v. Sweden»), № 62332/00, 6 червня 2006 р.

Право на заперечення

«Леандер проти Швеції» («Leander v. Sweden»), № 9248/81, 26 березня 1987 р.

«Мослі проти Сполученого Королівства» («Mosley v. the United Kingdom»), № 48009/08, 10 травня 2011 р.

«M.C. проти Швеції» («M.S. v. Sweden»), № 20837/92, 27 серпня 1997 р.

«Ротару проти Румунії» («Rotaru v. Romania») [GC], № 28341/95, 4 травня 2000 р.

Чутливі дані

«I. проти Фінляндії» («I. v. Finland»), № 20511/03, 17 липня 2008 р.

«Мішо проти Франції» («Michaud v. France»), № 12323/11, 6 грудня 2012 р.

«C. і Марпер проти Сполученого Королівства» («S. and Marper v. the United Kingdom»), № 30562/04 і 30566/04, 4 грудня 2008 р.

Нагляд та виконання (роль різних суб'єктів, включаючи органи із захисту персональних даних)

«I. проти Фінляндії» («I. v. Finland»), № 20511/03, 17 липня 2008 р.

«K.U. проти Фінляндії» («K.U. v. Finland»), № 2872/02, 2 грудня 2008 р.

«Фон Ганновер проти Німеччини» («Von Hannover v. Germany»), № 59320/00, 24 червня 2004 р.

«Фон Ганновер проти Німеччини» («Von Hannover v. Germany») (№ 2) [GC], № 40660/08 і 60641/08, 7 лютого 2012 р.

Методи нагляду

«Аллан проти Сполученого Королівства» («Allan v. the United Kingdom»), № 48539/99, 5 листопада 2002 р.

«Асоціація «21 грудня 1989 року» та інші проти Румунії» («Association «21 Decembre 1989» and Others v. Romania»), № 33810/07 і 18817/08, 24 травня 2011 р.

«Биков проти Росії» («Bykov v. Russia») [GC], № 4378/02, 10 березня 2009 р.

«Веттер проти Франції» («Vetter v. France»), № 59842/00, 31 травня 2005 р.

«Кеннеді проти Сполученого Королівства» («Kennedy v. the United Kingdom»), № 26839/05, 18 травня 2010 р.

«Класс та інші проти Німеччини» («Klass and Others v. Germany»), № 5029/71, 6 вересня 1978 р.

«Ротару проти Румунії» («Rotaru v. Romania») [GC], № 28341/95, 4 травня 2000 р.

«Тейлор-Себорі проти Сполученого Королівства» («Taylor-Sabori v. the United Kingdom»), № 47114/99, 22 жовтня 2002 р.

«Узун проти Німеччини» («Uzun v. Germany»), № 35623/05, 2 вересня 2010 р.

Відеоспостереження

«Кьопке проти Німеччини» («Köpke v. Germany»), № 420/07, 5 жовтня 2010 р.

«Пек проти Сполученого Королівства» («Peck v. the United Kingdom»), № 44647/98, 28 січня 2003 р.

Зразки голосу

«Віcс проти Франції» («Wisse v. France»), № 71611/01, 20 грудня 2005 р.

«П.Г. і Дж.Х. проти Сполученого Королівства» («P.G. and J.H. v. the United Kingdom»), № 44787/98, 25 вересня 2001 р.

Вибрана практика Суду Європейського Союзу

Практика, пов'язана з Директивою про захист персональних даних

C-73/07, *«Уповноважений із захисту персональних даних Фінляндії проти компаній «Satakunnan Markkinapörssi Oy» і «Satamedia Oy» («Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy»)* 16 грудня 2008 р. [Концепція «журналістської діяльності» за змістом статті 9 Директиви про захист персональних даних]

Об'єднані справи C-92/09 і C-93/09, *«Товариство громадського права «Volker and Markus Schecke» та Гартмут Айферт проти землі Гессен» («Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen»)*, 9 листопада 2010 р. [Пропорційність правового зобов'язання публікувати персональні дані бенефіціарів певних сільськогосподарських фондів ЄС]

C-101/01, *«Боділ Ліндквіст» («Bodil Lindqvist»)*, 6 листопада 2003 р. [Законність публікування приватною особою даних про приватне життя інших осіб у мережі Інтернет]

C-131/12, *«ТОВ «Google Spain», компанія «Google Inc.» проти Іспанського агентства захисту даних, Маріо Костеха Гонсалеса» («Google Spain, S.L., Google Inc. v. Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez»)*, Преюдиціальний запит Національного суду (Іспанії), поданий 9 березня 2012 року, 25 травня 2012 р., перебуває на розгляді [Обов'язки постачальників пошукових систем утриматися, на прохання суб'єкта персональних даних, від показу персональних даних у результатах пошуку]

C-270/11, *«Європейська комісія проти Королівства Швеція» («European Commission v. Kingdom of Sweden»)*, 30 травня 2013 р. [Штраф за невиконання Директиви]

C-275/06, *«Музичне виробництво в Іспанії (організація «Promusicae») проти AT «Telefonica de Espana» («Productores de Musica de Espana (Promusicae) v. Telefonica de Espana SAU»)*, 29 січня 2008 р. [Обов'язок постачальників доступу до Інтернету розкривати асоціації захисту інтелектуальної власності особистість користувачів системи обміну файлами «KaZaA»]

C-288/12, *«Європейська комісія проти Угорщини» («European Commission v. Hungary»)*, 8 квітня 2014 р. [Законність звільнення з посади працівника національного наглядового органу з питань захисту персональних даних]

C-291/12, *«Майкл Шварц проти міста Бохума» («Michael Schwarz v. Stadt Bochum»)*, Висновок Генерального адвоката, 13 червня 2013 р. [Порушення первинного права ЄС Регламентом (Ради ЄС) № 2252/2004, який передбачав внесення відбитків пальців до паспортів]

Об'єднані справи C-293/12 і C-594/12, *«Компанія «Digital Rights Ireland» і Зайтлінгер та інші проти Ірландії» («Digital Rights Ireland and Seitlinger and Others v. Ireland»)*, 8 квітня 2014 р. [Порушення первинного права ЄС Директивою про зберігання персональних даних]

C-360/10, *«Компанія «SABAM» проти AT «Netlog» («SABAM v. Netlog N.V.»)*, 16 лютого 2012 р. [Зобов'язання постачальників соціальних мереж запобігати незаконному використанню музичних та аудіовізуальних творів користувачами мережі]

Об'єднані справи C-465/00, C-138/01 і C-139/01, *«Рахункова палата проти австрійської телерадіокомпанії «Österreichischer Rundfunk» та інших і Нойком та Лауерманн проти австрійської телерадіокомпанії «Österreichischer Rundfunk» («Rechnungshof v. Österreichischer Rundfunk and Others and Neukomm and Lauermann v. Österreichischer Rundfunk»)*, 20 травня 2003 р. [Пропорційність правового зобов'язання публікувати персональні дані про зарплати службовців певних категорій установ державного сектору]

Об'єднані справи C-468/10 і C-469/10, *«Національна асоціація кредитних фінансових установ (ASNEF) і Федерація електронної комерції і прямого маркетингу (FECEMD) проти Державної адміністрації» («Asociacion Nacional de Establecimientos Financieros de Credito (ASNEF) and Federation de Comercio Electronico y Marketing Directo (FECEMD) v. Administracion del Estado»)*, 24 листопада 2011 р. [Коректна імплементація положень статті 7 (f) Директиви про захист персональних даних – «законні інтереси інших осіб» – у національне законодавство]

C-518/07, *«Європейська комісія проти Федеративної Республіки Німеччина» («European Commission v. Federal Republic of Germany»)*, 9 березня 2010 р. [Незалежність національного наглядового органу]

C-524/06, *«Губер проти Федеративної Республіки Німеччина» («Huber v. Bundesrepublik Deutschland»),* 16 грудня 2008 р. [Законність зберігання даних про іноземців у статистичних реєстрах]

C-543/09, *«Компанія «Deutsche Telekom» проти Федеративної Республіки Німеччина» («Deutsche Telekom A.G. v. Bundesrepublik Deutschland»)*, 5 травня 2011 р. [Необхідність поновлення згоди]

C-553/07, *«Мер і члени міської ради Роттердаму проти М.Е.Е. Ріджкебоера» («College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer»)*, 7 травня 2009 р. [Право суб'єкта персональних даних на доступ]

C-614/10, *«Європейська комісія проти Республіки Австрія» («European Commission v. Republic of Austria»)*, 16 жовтня 2012 р. [Незалежність національного наглядового органу]

Практика, пов'язана з Регламентом інституцій ЄС щодо захисту персональних даних

C-28/08 P, *«Європейська комісія проти компанії «The Bavarian Lager Co. Ltd» («European Commission v. The Bavarian Lager Co. Ltd.»)*, 29 червня 2010 р. [Доступ до документів]

C-41/00 P, *«ТОВ «Interporc Im- und Export» проти Комісії Європейських Співтовариств» («Interporc Im- und Export GmbH v. Commission of the European Communities»)*, 6 березня 2003 р. [Доступ до документів]

F-35/08, *«Дімітрос Пахтітіс проти Європейської комісії» («Dimitrios Pachtitis v. European Commission»)*, 15 червня 2010 р. [Використання персональних даних в умовах працевлаштування в інституціях ЄС]

F-46/09, *«В. проти Європейського парламенту» («V v. European Parliament»)*, 5 липня 2011 р. [Використання персональних даних в умовах працевлаштування в інституціях ЄС]

Алфавітний покажчик

Практика Суду Європейського Союзу

Практика Європейського суду з прав людини

Практика національних судів

Агенція Європейського Союзу з питань основоположних прав
Рада Європи – Європейський суд з прав людини

Посібник з європейського права у сфері захисту персональних даних. — К.: К.І.С., 2015. — 216 с.

ISBN 978-617-684-103-6

Інформацію про Агенцію Європейського Союзу з питань основоположних прав можна знайти в мережі Інтернет, зокрема, на веб-сайті Агенції за адресою: fra.europa.eu.

Додаткову інформацію щодо практики Європейського Суду з прав людини можна знайти на веб-сайті Суду за адресою: echr.coe.int. На пошуковому порталі HUDOC розміщено англомовні та франкомовні рішення і ухвали Суду з перекладом на інші мови, щомісячні огляди судової практики, прес-релізи та інша інформація про роботу Суду.

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Швидкий розвиток інформаційних та комунікаційних технологій підкреслює зростаючу потребу в надійному захисті персональних даних – праві, яке гарантують документи Європейського Союзу (ЄС) і Ради Європи (РЄ). Технологічний прогрес розширює межі, наприклад, спостереження, перехоплення комунікацій і зберігання даних; усе це створює значні виклики для права на захист персональних даних. Цей посібник призначений для ознайомлення практикуючих юристів, які не спеціалізуються на сфері захисту персональних даних у цій галузі права. У ньому надається загальна інформація щодо застосовних нормативно-правових актів ЄС і РЄ. Він надає пояснення ключової судової практики, резюмуючи основні рішення як Європейського суду з прав людини (ЄСПЛ), так і Суду Європейського Союзу (Суду ЄС). Якщо такої судової практики не існує, наводяться практичні ілюстрації з гіпотетичними сценаріями. Одним словом, цей посібник має за мету допомогти у забезпеченні енергійного і рішучого захисту права на захист персональних даних.

АГЕНЦІЯ ЄВРОПЕЙСЬКОГО СОЮЗУ З ПИТАНЬ ОСНОВОПОЛОЖНИХ ПРАВ
Шварценбергплац, 11 - 1040 Відень - Австрія
Тел. +43 (1) 580 30-60 - Факс +43 (1) 580 30-693
fra.europa.eu - info@fra.europa.eu

РАДА ЄВРОПИ
ЄВРОПЕЙСЬКИЙ СУД З ПРАВ ЛЮДИНИ
67075 Страсбург Седекс - Франція
Тел. +33 (0) 3 88 41 20 18 – Факс +33 (0) 3 88 41 27 30
echr.coe.int - publishing@echr.coe.int

ISBN 978-617-684-103-6
9 786176 841036