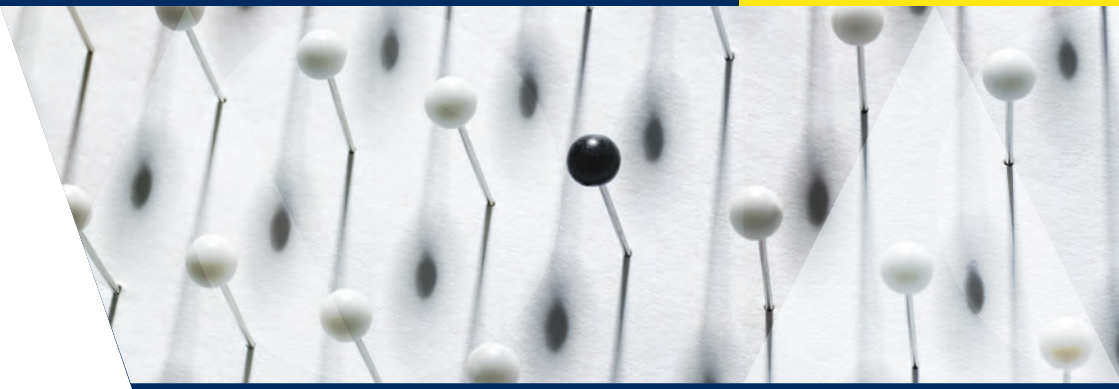
ПОСІБНИК



Посібник з європейського права у сфері захисту персональних даних

видання 2018 року

FRA
EUROPEAN UNION AGENCY

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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

Європейський Союз та Рада Європи працюють разом задля посилення операційної спроможності Омбудсмана у захисті прав людини

Фінансується Європейським Союзом та Радою Європи

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Впроваджується Радою Європи

This publication was translated and produced under the Joint Project between the European Union and the Council of Europe "European Union and Council of Europe working together to strengthen the Ombudsperson's capacity to protect human rights". 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 Спільного проєкту Європейського Союзу та Ради Європи «Європейський Союз та Рада Європи працюють разом задля посилення операційної спроможності Омбудсмана у захисті прав людини. Зміст публікації не повинен тлумачитися як такий, що відображає офіційні погляди Європейського Союзу та Ради Європи.

Роботу над цим посібником завершено в 2018 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 978-617-684-261-3 (Укр.)

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

EDPS

Посібник з європейського права у сфері захисту персональних даних

2018

Передмова

Наші суспільства стають все більш цифровими. У світлі цих змін на кожного з нас щоденно в різний спосіб впливають темпи технічного розвитку і те, як обробляються персональні дані. Нещодавно Європейський Союз (ЄС) та Рада Європи переглянули правові документи, які забезпечують захист приватного життя та персональних даних.

Європа очолює рух захисту персональних даних у світі. Стандарти ЄС у сфері захисту персональних даних ґрунтуються на положеннях Конвенції Ради Європи № 108, документів ЄС, включаючи Загальний регламент захисту персональних даних та Директиву про захист персональних даних для органів поліції та кримінальної юстиції, а також на відповідній практиці Європейського суду з прав людини та Суду Європейського Союзу.

Здійснені ЄС та Радою Європи реформи в сфері захисту персональних даних широкомасштабні та подекуди складні. Вони мають значний вплив на окремих осіб та на підприємства і надають їм багато переваг. Мета цього посібника – підвищення обізнаності та розширення знань щодо правил захисту персональних даних, особливо правників, що не є фахівцями в цій сфері, але мають справу з питаннями захисту персональних даних у своїй роботі.

Посібник підготовлено Агентством Європейського Союзу з питань основоположних прав (FRA) та Радою Європи спільно з Секретаріатом Європейського суду з прав людини та Європейським інспектором із захисту даних. Посібник доповнює видання 2014 року та становить частину серії юридичних посібників, створених спільно FRA та Радою Європи.

Ми вдячні органам захисту персональних даних Бельгії, Естонії, Франції, Грузії, Угорщини, Ірландії, Італії, Монако, Швейцарії та Сполученого Королівства за їхні коментарі стосовно проєкту посібника. Також висловлюємо подяку відділам Європейської Комісії з питань захисту персональних даних та з міжнародної передачі і захисту даних. Також дякуємо Суду Європейського Союзу за документи, надані під час підготовки цього посібника.

Крістос Джакомопулос,
Генеральний директор Директорату з прав людини та верховенства права Ради Європи

Джованні Буттареллі,
Європейський інспектор із захисту персональних даних

Майкл О'Флаерті,
Директор Агентства Європейського Союзу з питань основоположних прав

Зміст

Список скорочень

BCR	Обов'язкове корпоративне правило
CCTV	Система телебачення замкнутого контуру
CETS	Серія договорів Ради Європи
Charter	Хартія основних прав Європейського Союзу
CIS	Митна інформаційна система
CJEU	Суд Європейського Союзу (СЄС) (до грудня 2009 року – Європейський суд справедливості)
CoE	Рада Європи (РЄ)
Конвенція 108	Конвенція про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних (Рада Європи)
	Протокол про внесення змін (CETS № 223) до Конвенції 108 («Оновлена Конвенція 108») був прийнятий Комітетом міністрів Ради Європи на 128 сесії в м. Гельсінгері, Данія (17-18 травня 2018). Посилання на «Оновлену Конвенцію 108» означають посилання на Конвенцію зі змінами, внесеними Протоколом CETS № 223
CRM	Система управління зв'язками з клієнтами (CRM–система)
C-SIS	Центральна Шенгенська інформаційна система
DPO	Спеціаліст із захисту персональних даних
DPA	Орган із захисту персональних даних
EAW	Європейський ордер на арешт (ЄОА)
EDPB	Європейська рада із захисту персональних даних (ЄРЗПД)
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 персональних даних (ЄІЗПД)
EEA	Європейська економічна зона (ЄЕЗ)
EFSA	Європейський орган з безпечності харчових продуктів (ЄОБХП)
EFTA	Європейська асоціація вільної торгівлі (ЄАВТ)
ENISA	Європейське агентство з мережевої та інформаційної безпеки (ЄАМІБ)

ENU	Національний відділ Європейського поліцейського управління (НЄУ)
EPPO	Європейська прокуратура
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 ІТ-систем
FRA	Агентство Європейського Союзу із основоположних прав
GDPR	Загальний регламент про захист фізичних осіб у зв'язку з обробкою персональних даних та вільний рух таких даних (Загальний регламент захисту персональних даних (ЗРЗПД))
GPS	Спільний наглядовий орган
ICCPR	Міжнародний пакт про громадянські і політичні права (МПГПП)
ICT	Інформаційні та комунікаційні технології
ISP	Провайдер інтернет-послуг
JSB	Спільний наглядовий орган
NGO	Громадська організація (ГО)
N-SIS	Національна Шенгенська інформаційна система
OECD	Організація економічного співробітництва та розвитку (ОЕСР)
OJ	Офіційний журнал
PIN	Персональний ідентифікаційний код
PNR	Реєстраційні дані авіапасажирів
SCG	Наглядово-координаційна група
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 (ЗДПЛ)
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) з питань захисту персональних даних. Посібник підготовлено з метою надання допомоги практикам, які не спеціалізуються у сфері захисту персональних даних, включаючи адвокатів, суддів та представників інших юридичних професій, а також працівників інших органів, в тому числі й громадських організацій (ГО), перед якими можуть постати правові питання, пов'язані із захистом персональних даних.

Це – перше звернення до права ЄС і Конвенції про захист прав людини і основоположних свобод (ЄКПЛ), а також Конвенції про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108) та інших документів Ради Європи.

Кожна глава розпочинається таблицею відповідних правових норм, застосовних до теми, про яку йдеться у цій главі. Таблиця включає як право ЄС, так і Ради Європи, а також містить приклади рішень Європейського суду з прав людини (ЄСПЛ) та Суду Європейського Союзу (СЄС). Далі за тематикою один за одним наводяться приклади застосовування правових актів двох європейських систем. Це дозволяє читачеві зрозуміти їхні спільні та відмінні риси. Це допоможе користувачам знайти важливу для своєї ситуації інформацію, особливо коли вони є суб'єктами виключно права РЄ. Порядок наведених у таблицях тем може дещо відрізнятися від того порядку, у якому вони подані в самих розділах, якщо це сприяє лаконічності викладення змісту. Посібник також містить короткий огляд права Організації Об'єднаних Націй.

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 своєї країни безпосередньо із розділів, присвячених РЄ. Також необхідно пам'ятати, що з часу прийняття Загального регламенту захисту персональних даних ЄС, правила захисту персональних даних ЄС застосовуються до організацій та інших підприємств, які не зареєстровані в ЄС, якщо вони обробляють персональні дані та пропонують товари та послуги суб'єктам персональних даних в ЄС або здійснюють моніторинг поведінки таких суб'єктів.

Читачам із держав – членів ЄС потрібно буде звертатися до обох розділів, оскільки такі держави мають юридичні зобов'язання в обох правових системах. Необхідно враховувати, що реформи та модернізація правил захисту персональних даних були здійснені одночасно як у праві Ради Європи (Оновлена Конвенція 108 із змінами, внесеними Протоколом CETS № 223), так

і в праві ЄС (прийняття Загального регламенту захисту персональних даних та Директиви 2016/680/EU). Законодавці обох систем доклали максимум зусиль для забезпечення узгодженості та сумісності обох юридичних систем. Відповідно, реформи сприяли більшій сумісності права ЄС та РЄ щодо захисту персональних даних. Ті, кому потрібна детальніша інформація з певного питання, можуть звернутися до переліку спеціальних матеріалів у розділі «Додаткові матеріали». Інформація щодо положень Конвенції 108 та додаткового до неї Протоколу від 2001 р., які продовжують діяти до набрання чинності Протоколом, що вносить до них зміни, може бути знайдена читачами у виданні цього посібника 2014 року.

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

Право ЄС представлене ухваленими правовими актами, відповідними договорами, Хартією основних прав Європейського Союзу у тлумаченні Суду Європейського Союзу (СЄС). На додаток, посібник містить висновки та рекомендації, розроблені Робочою групою «Стаття 29» – дорадчим органом, який відповідно до Директиви про захист персональних даних надає експертні рекомендації державам - членам ЄС, та який з 28 травня 2018 року був замінений Європейською радою із захисту персональних даних. Висновки Європейського інспектора із захисту персональних даних також містять багато важливих напрацювань стосовно тлумачення права ЄС, тому вони також включені до цього посібника.

Приклади із судової практики, які наведено або на які даються посилання в цьому посібнику, належать до основних рішень, ухвалених ЄСПЛ та СЄС. Вказівники в кінці посібника допоможуть читачеві знайти потрібне рішення в мережі інтернет. Практика СЄС, включена до посібника, стосується нечинної Директиви про захист персональних даних. Однак тлумачення СЄС залишається застосовним до відповідних прав та обов'язків, передбачених Загальним регламентом захисту персональних даних.

На додаток до цього в текстових вікнах на блакитному тлі наведено приклади з уявним сюжетом, які пояснюють практичне застосування європейських норм захисту персональних даних, особливо з тематики, щодо якої немає рішень ЄСПЛ або СЄС. У текстових вікнах на сірому тлі наведено приклади з інших джерел, таких як нормативні документи або висновки Робочої групи «Стаття 29», а не з практики ЄСПЛ та СЄС.

На початку посібника подається короткий огляд ролі двох правових систем, утворених ЄКПЛ та правовими документами ЄС (розділ 1). У розділах 2–10 розглядаються такі питання:

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

1 Контекст та історія європейського права про захист персональних даних

ЄС	Питання, що висвітлюються	РЄ
Право на захист даних		
Договір про функціонування Європейського Союзу стаття 16 *Хартія основних прав Європейського Союзу* (Хартія), стаття 8 (право на захист персональних даних) *Директива 95/46/ЕС* про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних (Директива про захист персональних даних, OJ 1995 L 281, чинна до травня 2018 року) *Рамкове рішення Ради ЄС № 2008/977/ЈНА* про захист персональних даних, що обробляються в рамках поліцейського та судового співробітництва у кримінальних справах (OJ 2008 L 350, чинне до травня 2018 року)		*ЄКПЛ*, стаття 8 (право на повагу до приватного та сімейного життя, житла і кореспонденції) Оновлена Конвенція про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних (*Оновлена Конвенція 108*)

ЄС	Питання, що висвітлюються	РЄ
Загальний регламент (ЄС) 2016/679 захисту фізичних осіб в зв'язку з обробкою персональних даних та вільний рух таких даних і скасування Директиви 95/46/ЄК (Загальний регламент захисту персональних даних, OJ 2016 L 119) *Директива (ЄС) 2016/680* про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами влади в цілях попередження, розслідування, виявлення кримінальних правопорушень та притягнення до відповідальності за їх вчинення або виконання кримінальних покарань та про вільне переміщення таких даних, а також про скасування Рамкового рішення Ради ЄС № 2008/977/ЈНА (про захист персональних даних, що обробляються в рамках поліцейського та судового співробітництва у кримінальних справ) OJ 2016 L 119 *Директива 2002/58/ЕС* про обробку персональних даних та захист таємниці в секторі електронних комунікацій (Директива про конфіденційність та електронні комунікації) OJ 2002 L 201 *Загальний регламент (ЕС) № 45/2001* про захист фізичних осіб при обробці персональних даних інститутами і органами Співтовариства і про вільне переміщення таких даних (Загальний регламент інститутів ЄС про захист персональних даних), OJ 2001 L 8		

ЄС	Питання, що висвітлюються	РЄ
Обмеження права на захист персональних даних		
Хартія, стаття 52 (1) Загальний регламент захисту персональних даних, стаття 23 СЄС, об'єднані справи, C-92/09 та C-93/09 «"Volker und Markus Schecke GbR" та Хартмут Ейферт проти землі Гессен» (*Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*) [ВП], 2010 р.		ЄКПЛ, стаття 8 (2) Оновлена Конвенція 108, стаття 11 ЄСПЛ, «С. та Марпер проти Сполученого Королівства» (*S. and Marper v. the United Kingdom*), № 30562/04 і 30566/04, [ВП], 2008 р.
Баланс прав		
СЄС, об'єднані справи, C-92/09 та C-93/09 «"Volker und Markus Schecke GbR" та Хартмут Ейферт проти землі Гессен» (*Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*) [ВП], 2010 р. СЄС, C-73/07, «Уповноважений із захисту персональних даних Фінляндії проти "Satakunnan Markkinapörssi Oy" і "Satamedia Oy"» (*Tietosuojavaltuutettu v. Satakunnan Markkinaporssi Oy and Satamedia Oy*), [ВП], 2008р.	**Загальні** **Свобода вираження поглядів**	ЄСПЛ, «"Axel Springer AG" проти Німеччини», (*Axel Springer AG v. Germany*) № 39954/08, [ВП], 2012 р.
СЄС, C-131/12, «"Google Spain SL", "Google Inc." проти Іспанського агентства захисту даних (AEPD) та Маріо Костеха Гонсалеса» (*Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*), [ВП], 2014		ЄСПЛ, «Мослі проти Сполученого Королівства», (*Mosley v. the United Kingdom*), № 48009/08, 2011 р. ЄСПЛ, «Болен проти Німеччини» (*Bohlen v. Germany*), № 53495/09, 2015

ЄС	Питання, що висвітлюються	РЄ
СЄС, C-28/08 P, «Європейська Комісія проти “The Bavarian Lager Co. Ltd”» [ВП] (*European Commission v. The Bavarian Lager Co. Ltd*), 2010 СЄС, C-615/13P, «“ClientEarth” та “PAN Europe” проти Європейського агентства безпечності харчових продуктів» (*ClientEarth, PAN Europe v. EFSA*), 2015	**Доступ до документів**	ЄСПЛ, «Угорський Гельсінський комітет проти Угорщини» (*Magyar Helsinki Bizottság v. Hungary*) [ВП], № 18030/11, 2016
Загальний регламент захисту персональних даних, стаття 90	**Професійна таємниця**	ЄСПЛ, «Прутеану проти Румунії» (*Pruteanu v. Romania*), № 30181/05, 2015
Загальний регламент захисту персональних даних, стаття 91	**Свобода думки, совісті та релігії**	
	Свобода художньої творчості та науково - дослідницької діяльності	ЄСПЛ, «Асоціація візуальних художників проти Австрії», 2007 (*Vereinigung bildender Künstler v. Austria*), № 68345/01, 2007
СЄС, C-275/06 «Музичні продюсери Іспанії (Promusicae) проти “Telefonica de Espana SAU”» (*Productores de Musica de Espana (Promusicae) v. Telefonica de Espana SAU*), [ВП], 2008	**Захист майна**	
СЄС, C-131/12, «“Google Spain SL”, “Google Inc.“ проти Іспанського агентства захисту даних (AEPD) та Маріо Костеха Гонсалеса» («*Google Spain, S.L., Google Inc. v. Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez*»), [ВП], 2014 СЄС, C-398/15, «Торгово-промислова та сільськогосподарська палата м. Лечче проти Сальваторе Манні» (*Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*), 2017	**Економічні права**	

1.1 Право на захист персональних даних

Ключові моменти

- Згідно зі статтею 8 ЄКПЛ право на захист відносно обробки персональних даних є частиною 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. Конвенція пройшла процес оновлення, який було завершено прийняттям Протоколу про внесення змін до Конвенції CETS № 223.
- У праві ЄС право на захист персональних даних визнано як основоположне право. Це було підтверджено у статті 16 Договору про функціонування ЄС, а також у статті 8 Хартії основних права ЄС.
- Директива про захист персональних даних 1995 року була першим документом, який регулював захист персональних даних у праві ЄС.
- Враховуючи швидкі технологічні зміни, ЄС прийняв нове законодавство у 2016 році з метою адаптування правил захисту персональних даних до ери цифрових технологій. Загальний регламент захисту персональних даних набув чинності у травні 2018 року з одночасним скасуванням Директиви про захист персональних даних.
- Разом із Загальним регламентом захисту персональних даних ЄС прийняв законодавство про обробку державними органами персональних даних в цілях правоохоронної діяльності. Директива (ЄС) 2016/680 встановлює правила захисту персональних даних та принципи, які регулюють обробку персональних даних з метою попередження, розслідування, виявлення кримінальних правопорушень та притягнення до відповідальності за їх вчинення або виконання кримінальних покарань.

1.1.1 Право на повагу до приватного життя та право на захист персональних даних: стислий вступ

Право на повагу до приватного життя та право на захист персональних даних є різними правами, хоча й тісно пов'язаними. Право на приватність, на яке посилається законодавство ЄС як на право на повагу до приватного життя, вперше з'явилось у міжнародних документах з прав людини, в Загальній декларації прав людини Організації Об'єднаних Націй (ЗДПЛ) 1948 року, як одне з основоположних захищених прав. Невдовзі після прийняття Загальної

декларації прав людини Європа також підтвердила це право в Європейській Конвенції з прав людини 1950 року (ЄКПЛ), обов'язковому договорі для її Договірних Сторін. ЄКПЛ передбачає, що кожен має право на повагу до свого приватного та сімейного життя, житла та кореспонденції. Органи державної влади не можуть втручатись у здійснення цього права за винятком випадків, коли втручання здійснюється згідно із законом, переслідує важливі та легітимні суспільні інтереси і є необхідним у демократичному суспільстві.

ЗДПЛ та ЄКПЛ були прийняті задовго до ери комп'ютерів, інтернету та розвитку інформаційного суспільства. Такий прогрес приніс значні переваги окремим особам та суспільству, покращив якість життя, ефективність та продуктивність. Водночас він привніс й нові ризики стосовно права на повагу до приватного життя. У відповідь на потребу в спеціальних правилах збору та використання особистої інформації з'явилась нова концепція приватності, яку в деяких юридичних системах називають «інформаційною приватністю», в інших – «правом на інформаційне самовизначення»[1]. Ця концепція призвела до появи спеціальних правових норм для захисту персональних даних.

В Європі захист даних почався у 1970-х роках з ухвалення деякими державами законодавства про контроль за обробкою органами державної влади та великими підприємствами інформації про особу[2]. Згодом акти із захисту персональних даних були прийняті на європейському рівні[3], та з часом захист персональних даних став окремою цінністю поза межами права на повагу до приватного життя. У праві ЄС захист даних визнано основоположним правом, окремим від основоположного права на повагу до приватного життя. Це розділення постійно породжує питання щодо взаємозв'язку цих двох прав та різниці між ними.

1 7 Федеральний Конституційний суд Німеччини підтвердив право на інформаційне самовизначення в рішенні 1983 року (*Volkszählungsurteil*) , BVerfGE Bd. 65, S. 1ff. Суд вирішив, що інформаційне самовизначення виходить з основоположного права на повагу до особистості, гарантованого Конституцією Німеччини. У рішенні 2017 року ЄСПЛ визнав, що стаття 8 ЄКПЛ «передбачає право на форму інформаційного самовизначення». Див. рішення ЄСПЛ у справі «"Satakunnan Markkinapörssi Oy" та "Satamedia Oy" проти Фінляндії" (*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*), № 931/13, 27 червня 2017, п. 137.

2 Влада землі Гессен у Німеччині прийняла перший закон про захист даних у 1970 році, який застосовувався тільки на цій обмеженій території. У 1973 році Швеція прийняла перший національний закон із захисту персональних даних. До кінця 1980-х років декілька європейських держав (Франція, Німеччина, Нідерланди та Сполучене Королівство) також прийняли закони про захист персональних даних.

3 Конвенція Ради Європи про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108) була прийнята у 1981 році. 1995 року ЄС прийняв перший комплексний акт про захист персональних даних, а саме Директиву 95/46/ЕС «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних».

Право на повагу до приватного життя та право на захист персональних даних тісно пов'язані. Обидва права мають на меті захистити схожі цінності, тобто автономність та людську гідність фізичних осіб, шляхом надання їм особистої сфери, у якій вони можуть вільно розвивати свою особистість, створювати та формувати свої погляди. Таким чином, ці два права є важливими передумовами реалізації інших основоположних свобод, таких як свобода вираження поглядів, свобода мирних зібрань та об'єднань, а також свобода віросповідання.

Ці два права різняться в формулюванні та обсязі. Право на повагу до приватного життя складається із загальної заборони втручання за винятком окремих випадків наявності суспільних інтересів, які можуть виправдати втручання. Захист персональних даних розглядається як сучасне та активне право[4], яке забезпечує систему стримання та противаг для захисту фізичної особи, якщо її персональні дані обробляються. Обробка даних має відповідати базовим вимогам захисту персональних даних, а саме має бути незалежний контроль та повага до прав суб'єкта персональних даних[5].

Стаття 8 Хартії основних прав ЄС (Хартія) не тільки проголошує право на захист персональних даних, але й також вказує на ключові цінності, пов'язані з цим правом. Вона передбачає, що обробка персональних даних має бути чесною, переслідувати визначені цілі та здійснюватись або на підставі згоди суб'єкта персональних даних, або на правомірній підставі, передбаченій законом. Фізичні особи повинні мати право на доступ до своїх даних та право на їх виправлення. Дотримання цих прав має здійснюватись під контролем незалежного органу.

Право на захист персональних даних застосовується, коли персональні дані обробляються; відповідно, воно ширше, ніж право на повагу до приватного життя. Будь-яка обробка персональних даних підлягає належному захисту. Захист даних стосується всіх видів персональних даних та обробки даних незалежно від зв'язку з приватністю або впливом на неї. Обробка персональних даних може також порушити право на повагу до приватного життя, як це демонструють приклади нижче. Однак для застосування правил захисту персональних даних немає необхідності демонструвати втручання в приватне життя.

4 Генеральний адвокат Шарпстоун описала це як сполучення двох окремих прав: «класичного» права на захист приватності та більш «сучасного» права на захист персональних даних. Див. об'єднані справи № C-92/09 та № C-93/02, «"Volker und Markus Schecke GbR" та Хартмут Ейферт проти землі Гессен», Позиція генерального адвоката Шарпстоун (*Volker und Markus Schecke GbR v. Land Hessen, Opinion of Advocate General Sharpston*), від 17 червня 2010, п. 71.

5 Густінкс, П., ЄІЗПД Промови & Статті, Право ЄС з захисту персональних даних: Перегляд Директиви 95/46/ЕС та проєкт Загального регламенту про захист персональних даних, липень 2013 (*EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*).

Право на приватність стосується ситуацій, коли приватний інтерес або «приватне життя» фізичної особи зазнало обмеження. Як продемонстровано в цьому посібнику, концепція «приватного життя» була розтлумачена в судовій практиці як така, що охоплює інтимні ситуації, чутливу або конфіденційну інформацію, інформацію, яка може створити негативне ставлення суспільства до фізичної особи, навіть певні аспекти професійного життя та публічної поведінки. Втім оцінка того, чи відбулось втручання у «приватне життя» залежить від контексту та фактів кожної окремої справи.

Натомість будь-яка операція, яка включає обробку персональних даних, може потрапити до сфери правил щодо захисту даних та зумовити застосування права на захист персональних даних. Наприклад, у разі, коли роботодавець здійснює запис інформації про імена працівників та про їх виплати, сам собою запис цієї інформації не може вважатися втручанням у право на повагу до приватного життя. Про таке втручання можна говорити, наприклад, коли роботодавець передасть особисту інформацію працівників третім особам. Водночас дотримуватися правил захисту персональних даних роботодавці повинні у будь-якому разі, оскільки фіксування інформації про працівників становить обробку персональних даних.

Приклад: у справі «*Digital Rights Ireland*»[6] Суд ЄС мав вирішити питання правомірності Директиви 2006/24/ЕС в контексті основоположного права на захист персональних даних та права на повагу до приватного життя, проголошених у Хартії основних прав ЄС. Директива зобов'язувала надавачів публічно доступних електронних комунікаційних послуг або суспільних телекомунікаційних мереж зберігати дані про користування мережею громадян до двох років для забезпечення доступності даних з метою попередження, розслідування серйозних злочинів та притягнення за них до відповідальності. Захід стосувався метаданих, даних місцезнаходження та даних, необхідних для ідентифікації абонента або користувача. Директива не застосовувалася до змісту електронних комунікацій.

Суд ЄС визнав, що Директива передбачає втручання в основоположне право на захист персональних даних, «оскільки вона передбачає обробку

6 Суд ЄС, об'єднані справи C-293/12 та C-594/12, «"Digital Rights Ireland Ltd." проти Міністра зв'язку, морських та природних ресурсів та інших та Земельний уряд Каринтії та інші» (*Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [ВП]), від 08 квітня 2014.

персональних даних»[7]. Крім того, він визнав, що Директива передбачає втручання у право на повагу до приватного життя[8]. Якщо досліджувати в цілому, персональні дані, які зберігалися відповідно до Директиви та були доступними для компетентних органів влади, могли дозволити «зробити дуже чіткі висновки щодо приватного життя осіб, чиї дані зберігалися, наприклад щодо їхніх звичок у повсякденному житті, постійного або тимчасового місця проживання, щоденних або інших переміщень, їхньої діяльності, соціальних відносин з іншими особами або місць, які вони відвідували»[9]. Втручання в ці два права було широкомасштабним та вельми серйозним.

Суд ЄС визнав Директиву 2006/24/ЕС нечинною, оскільки незважаючи на мету, що переслідувалася, втручання у право на захист персональних даних та право на приватність було серйозним та виходило за межі того, що є суворо необхідним.

1.1.2 Міжнародно-правові норми: Організація Об'єднаних Націй

У правових актах ООН захист персональних даних не визнається основоположним правом, незважаючи на те, що право на приватне життя є давно визнаним основоположним правом у міжнародному правовому порядку. Стаття 12 ЗДПЛ щодо поваги до приватного та сімейного життя[10] вперше запровадила міжнародний інструмент, що передбачає право особи на захист приватної сфери від втручання інших, особливо держави. Хоча ця декларація не є обов'язковою для виконання, ЗДПЛ все ж має серйозний статус основного документа в міжнародному праві з питань прав людини та впливає на розвиток інших інструментів прав людини в Європі. Міжнародний пакт про громадянські і політичні права (МПГПП) набув чинності 1976 року. Він проголошує заборону свавільного або неправомірного втручання в приватне життя особи, житло та кореспонденцію, а також неправомірних посягань на честь та репутацію. МПГПП є міжнародним договором, який зобов'язує його 169

7 Там само, п. 36.

8 Там само, п. 32–35.

9 Там само, п. 27.

10 Організація Об'єднаних Націй (ООН), Загальна декларація прав людини (ЗДПЛ) (*Universal Declaration of Human Rights (UDHR)*), 10 грудня 1948 р.

сторін-учасниць поважати та забезпечувати реалізацію цивільних прав осіб, включно з правом на приватність.

Починаючи з 2013 року, ООН прийняла дві резолюції з питань приватного життя під назвою «право на приватність у цифрову еру»[11]. Ці резолюції були ухвалені у відповідь на розвиток нових технологій та оприлюднення фактів масового спостереження в певних державах (викриття Сноудена). У резолюціях потужно засуджується масове спостереження і наголошується на його можливому впливі на такі засадничі права, як приватне життя та свобода вираження поглядів, а також на функціонування динамічного демократичного суспільства. Хоча резолюції не є юридично обов'язковими, вони дали поштовх важливій міжнародній дискусії високого рівня щодо приватності, нових технологій та спостереження. Вони також привели до запровадження посади Спеціального доповідача щодо права на приватне життя з повноваженнями щодо популяризації та захисту цього права. Його конкретним завданням є збір інформації про підходи та досвід різних країн у питаннях приватності та про виклики, пов'язані з новими технологіями, обмін та популяризація найкращим досвідом, а також визначення потенційних перешкод.

В той час як попередні резолюції зосереджувалися на негативному впливі масового спостереження та завданні держав обмежувати повноваження розвідувальних органів, більш пізні резолюції відображають важливі події, що сталися в обговореннях питань приватності в ООН[12]. Резолюції, прийняті в 2016 та 2017 роках, повторно підкреслюють необхідність обмеження повноважень розвідувальних органів та засуджують масове спостереження. Однак у них також чітко зазначається, що «розширення можливостей бізнес компаній збирати, обробляти та використовувати персональні дані може становити ризик для реалізації права на приватність у цифрову еру». Таким чином, на додаток до відповідальності державних органів, резолюції також вказують на відповідальність приватного сектору щодо поваги до прав людини, та закликають підприємства повідомляти користувачів про збір, використання, поширення та збереження персональних даних, а також запроваджувати прозору політику обробки даних.

11 Див. ООН, Генеральна Асамблея, Резолюція про право на приватність у цифрову еру (*Resolution on the right to privacy in the digital age*), A/RES/68/167, Нью-Йорк, 18 грудня 2013 року; та ООН, Генеральна Асамблея, Переглянутий проєкт Резолюції про право на приватність у цифрову еру, A/C.3/69/L.26/Rev.1, Нью-Йорк, 19 листопада 2014 року.

12 ООН, Генеральна Асамблея, Переглянутий проєкт Резолюції про право на приватність у цифрову еру (*Revised draft resolution on the right to privacy in the digital age*), A/C.3/71/L.39/Rev.1, Нью-Йорк, 16 листопада 2016; ООН, Рада прав людини, Право на приватність у цифрову еру, A/HRC/34/L.7/Rev.1, 22 березня 2017 року.

1.1.3 Європейська Конвенція з прав людини

Раду Європи засновано після Другої світової війни з метою єднання європейських держав задля утвердження 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 (*ЄКПЛ*), яка набула чинності у 1953 році.

Договірні Сторони мають міжнародні зобов'язання щодо дотримання ЄКПЛ. Усі держави – члени РЄ вже включили норми ЄКПЛ до свого національного законодавства або ввели їх у дію, що вимагає від них дотримуватися її положень. Договірні Сторони зобов'язані поважати права, передбачені ЄКПЛ, у будь-якій діяльності або реалізації своїх повноважень. Це також включає діяльність, пов'язану з національною безпекою. Визначальні рішення Європейського суду з прав людини (ЄСПЛ) стосувалися діяльності держави в чутливих сферах права та практики, пов'язаних з національною безпекою[13]. Суд, не вагаючись, визнає спостереження втручанням у право на повагу до приватного життя[14].

З метою забезпечення виконання Договірними Сторонами їхніх зобов'язань за ЄКПЛ у 1959 році у Страсбурзі (Франція) засновано Європейський суд з 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. ЄСПЛ може також розглядати міждержавні справи, порушені однією або декількома державами – членами РЄ проти іншої держави-члена.

У 2018 році до складу Ради Європи входило 47 Договірних Сторін, 28 з яких були одночасно і державами – членами ЄС. Для того щоб подати заяву до ЄСПЛ, не потрібно бути громадянином однієї з держав-членів, хоча стверджуване порушення при цьому має бути вчинено в межах юрисдикції однієї з цих держав.

Право на захист персональних даних є частиною прав, захищених статтею 8 ЄКПЛ, яка гарантує право на повагу до приватного і сімейного життя,

13 Див., наприклад, рішення ЄСПЛ у справі «Класс та інші проти Німеччини» (*Klass and Others v. Germany*), № 5029/71, 6 вересня 1978; рішення ЄСПЛ у справі «Ротару проти Румунії» (*Rotaru v. Romania)* [ВП], № 28341/95, 4 травня 2000 та рішення ЄСПЛ у справі «Сабо та Віші проти Угорщини» (*Szabó and Vissy v. Hungary*) , № 37138/14, 12 січня 2016.

14 Там само.

житла та кореспонденції, а також визначає умови, за яких дозволяється обмежувати це право[15].

ЄСПЛ розглядав велику кількість справ, де йшлося про захист персональних даних, включно з перехопленням інформації[16], різними формами спостереження з боку як державного, так і приватного сектору[17]. та захист від зберігання персональних даних державними органами[18]. Право на повагу до приватного життя не є абсолютним правом, оскільки його реалізація може становити втручання в інші права, наприклад право на свободу вираження поглядів та доступ до інформації і, навпаки, реалізація цих прав може обмежувати право на приватність. Отже, ЄСПЛ намагається знайти баланс між різними правами. Суд 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[19]. Значна кількість цих справ детально розглядатиметься у відповідних главах.

1.1.4 Конвенція 108 Ради Європи

Із появою у 1960-х роках інформаційних технологій з'явилася потреба в розробленні більш детальних правил забезпечення захисту осіб шляхом охорони їхніх персональних даних. У середині 1970-х років Комітет міністрів Ради Європи прийняв низку резолюцій про захист персональних даних з посиланням на

15 Рада Європи, *Європейська конвенція з прав людини*, CETS № 005, 1950.

16 Див., наприклад, рішення ЄСПЛ у справі «Мелоун проти Сполученого Королівства» (*Malone v. the United Kingdom*), № 8691/79, 2 серпня 1984; рішення ЄСПЛ у справі «Копланд проти Сполученого Королівства» (*Copland v. the United Kingdom*), № 62617/00, 3 квітня 2007, або рішення ЄСПЛ у справі «Мустафа Сержін Танрікулу проти Туреччини» (*Mustafa Sezgin Tanrıkulu v. Turkey*), № 27473/06, від 18 липня 2017.

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

18 Див., наприклад, рішення ЄСПЛ у справі «Роман Захаров проти Росії» (*Roman Zakharov v. Russia*), № 47143/06, 4 грудня 2015; рішення ЄСПЛ у справі «Сабо та Віші проти Угорщини» (*Szabó and Vissy v. Hungary*), № 37138/14, 12 січня 2016.

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

статтю 8 ЄКПЛ[20]. 1981 року була відкрита для підписання *Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція 108)*[21]. Конвенція 108 була і залишається єдиним юридично зобов'язальним 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 обробці персональних даних, і водночас здійснює регулювання транскордонної передачі персональних даних. Що стосується обробки персональних даних, визначені в Конвенції принципи стосуються, зокрема, чесного і правомірного збирання та автоматизованої обробки персональних даних для визначених і легітимних цілей. Це означає, що персональні дані не мають використовуватись у спосіб, не сумісний із цими цілями, а також зберігатися довше, ніж це необхідно. Вони також стосуються якості даних, зокрема вимагається, щоб такі дані були адекватними, відповідними та не надмірними (пропорційними), а також точними.

На додаток до гарантій, що стосуються обробки персональних даних та обов'язку їх захисту, Конвенція забороняє за відсутності відповідних юридичних 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 право особи знати про факт збереження про себе інформації і про можливість її корегування за потреби. Дія закладених у Конвенції обмежень щодо здійснення прав можлива лише за умови існування загрози інтересам, які переважають (наприклад, інтересам безпеки та захисту держави). Незважаючи на те, що Конвенція передбачає вільний обмін персональними даними між державами, які є сторонами Конвенції, вона водночас накладає деякі обмеження на ті потоки, які спрямовано до держав, де правове регулювання не передбачає відповідного рівня захисту даних.

Конвенція 108 є обов'язковою для держав, які її ратифікували. ЄСПЛ не здійснює контроль над її виконанням, однак він враховує її положення у своїй

20 Рада Європи, Комітет міністрів (1973), *Резолюція (73) 22* про захист недоторканності приватного життя осіб стосовно електронних банків персональних даних у приватному секторі, 26 вересня 1973; Рада Європи, Комітет міністрів (1974), *Резолюція (74) 29* про захист недоторканності приватного життя осіб стосовно електронних банків персональних даних у приватному секторі, 20 вересня 1974.

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

практиці за статтею 8 ЄКПЛ. Протягом багатьох років ЄСПЛ вказує, що захист персональних даних є важливою частиною поваги до приватного життя (стаття 8). При цьому Суд керується принципами Конвенції 108 при визначенні того, чи мало місце втручання в це основоположне право[22].

З метою подальшого розвитку викладених у Конвенції 108 загальних принципів і правил Комітет міністрів РЄ ухвалив декілька рекомендацій, які не мають зобов'язального характеру. Ці рекомендації мають значний вплив на розвиток права із захисту даних у Європі. Наприклад, протягом багатьох років єдиним документом, який містив вказівки щодо використання даних правоохоронними органами, була Рекомендація для поліції[23]. Принципи, викладені в цій Рекомендації, наприклад, щодо засобів збереження файлів з персональними даними та необхідності встановлення чітких правил для осіб, які мають до них доступ, набули подальшого розвитку та стали частиною законодавства ЄС[24]. Нещодавні рекомендації вказують на необхідність вирішувати проблеми цифрової ери, наприклад, стосовно обробки персональних даних у трудовій сфері (див. *главу 9*).

Всі держави – члени ЄС ратифікували Конвенцію 108. 1999 року до Конвенції 108 було внесено зміни, які дозволили ЄС стати стороною Конвенції[25]. 2001 року 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[26].

Конвенція 108 відкрита для приєднання 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 підтримки захисту персональних даних на світовому рівні. Станом на сьогодні до Конвенції 108 приєдналася 51 держава, включно з усіма державами–членами

22 Див., наприклад, рішення ЄСПЛ у справі «Z. проти Фінляндії» (*Z v. Finland*), № 22009/93, 25 лютого 1997.

23 Рада Європи, Комітет міністрів (1987), Рекомендація Rec (87)15 державам-членам щодо регулювання використання персональних даних у роботі поліції, Страсбург, 17 вересня 1987. РЄ.

24 Директива 95/46/ЕС Європейського Парламенту та Ради 24 жовтня 1995 про захист фізичних осіб в зв'язку з обробкою персональних даних та вільне переміщення таких даних, OJ L 281, 23 листопада 1995.

25 Рада Європи, Зміни до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ETS No. 108), прийняті Комітетом міністрів у м. Страсбурзі 15 червня 1999.

26 Рада Європи, Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо контрольних органів та транскордонних потоків даних, CETS No. 181, 2001. З прийняттям Оновленої Конвенції 108, цей Протокол більше не застосовується, оскільки його положення були оновлені та включені до Оновленої Конвенції 108.

Ради Європи (47 держав). Уругвай, перша неєвропейська країна, приєднався у серпні 2013 року, а Республіка Маврикій, Республіка Сенегал та Туніс приєдналися у 2016 та 2017 роках.

Нещодавно Конвенцію було *оновлено*. Публічні обговорення в 2011 році визначили два головних напрямки роботи: посилення захисту приватності в цифровій сфері та зміцнення контрольного механізму Конвенції 108. Процес реформування був зосереджений на цих двох цілях та закінчився прийняттям протоколу про внесення змін до Конвенції 108 (Протокол CETS № 223). Ця робота здійснювалась паралельно з іншими реформами міжнародних інструментів захисту персональних даних та одночасно з реформуванням правил захисту даних ЄС, розпочатим у 2012 році. Законодавці на рівні Ради Європи та ЄС доклали всіх зусиль для забезпечення узгодженості та сумісності двох юридичних систем. Оновлення зберегло загальний гнучкий характер Конвенції 108 та зміцнило її потенціал універсального інструмента в праві захисту персональних даних. Внаслідок оновлення було підтверджено та закріплено важливі принципи і введено нові права фізичної особи з одночасним підвищенням відповідальності підприємств, які обробляють персональні дані, та забезпеченням більшої підзвітності. Наприклад, фізичні особи, чиї персональні дані обробляються, мають право знати підстави обробки та право заперечувати проти неї. З метою протидії збільшеному використанню профайлінгу в онлайн-світі Конвенція також встановлює право особи не бути суб'єктом рішення, прийнятого щодо неї в результаті автоматичної обробки даних без врахування її позиції. Дієве забезпечення виконання правил захисту даних незалежним наглядовим органом влади в Договірних Сторонах вважається центральним завданням практичного застосування Конвенції. Для цих цілей оновлені положення Конвенції підкреслюють необхідність надання наглядовим органам дієвих повноважень та наділення їх відповідними функціями, а також забезпечення їхньої незалежності у виконанні своєї місії.

1.1.5 Законодавство Європейського Союзу у сфері захисту персональних даних

В основі законодавства ЄС лежать договори ЄС та акти вторинного законодавства ЄС. Договори, а саме *Договір про Європейський Союз (ДфЄС)* та Договір про функціонування Європейського Союзу (ДфЄС), ратифіковано всіма державами – членами ЄС, вони формують «первинне законодавство ЄС». Регламенти, директиви та рішення ЄС ухвалюють органи ЄС, що отримали на це повноваження згідно з договорами; вони формують «вторинне законодавство ЄС».

Захист даних у первинному законодавстві ЄС

Перші договори Європейського Співтовариства не містили жодних посилань на права людини або їх захист, оскільки Європейське економічне співтовариство було започатковане як регіональна організація, спрямована на економічну інтеграцію та встановлення спільного ринку. Засадничим принципом, який був основою створення та розвитку Економічного співтовариства та який залишається чинним сьогодні, є принцип передачі повноважень. Згідно з цим принципом ЄС діє тільки в межах компетенції, яка передана йому державами-членами та яка закріплена в договорах ЄС. На противагу Раді Європи, договори ЄС не передбачають чітко визначених повноважень щодо питань основоположних прав.

Втім з надходженням до Суду ЄС справ, у яких порушуються питання прав людини в межах сфери законодавства ЄС, цей Суд надає істотне тлумачення відповідних договорів. З метою надання захисту особам Суд ЄС включив основоположні права до так званих загальних принципів європейського права. СЄС постановив, що ці загальні принципи відображають зміст захисту прав людини, який закріплений у національних конституціях і договорах з прав людини, зокрема в ЄКПЛ. СЄС заявив, що забезпечуватиме відповідність права ЄС до цих принципів.

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 (Хартію). Ця Хартія охоплює весь спектр громадянських, політичних, економічних і соціальних прав європейських громадян у поєднанні з конституційними традиціями та міжнародними зобов'язаннями, спільними для держав-членів. Описані в Хартії права розподілено за шістьма розділами: гідність, свобода, рівність, солідарність, права громадян та правосуддя.

Спочатку Хартія була лише політичним документом, але після набрання чинності Лісабонським договором 1 грудня 2009 року[27] вона стала юридично зобов'язальною[28] як первинне законодавство ЄС (див. статтю 6 (1) Договору про Європейський Союз). Положення Хартії зобов'язують інститути та органи ЄС дотримуватися передбачених у ній прав при виконанні своїх

27 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.

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

обов'язків. Положення Хартії також є обов'язковими для держав – членів ЄС при виконанні законодавства Союзу.

Хартія не лише гарантує повагу до приватного і сімейного життя (стаття 7), але й передбачає право на захист персональних даних (стаття 8), недвозначно піднімаючи рівень його захисту до рівня захисту основоположного права ЄС. Інститути та органи ЄС повинні дотримуватися і гарантувати це право, так само як і держави-члени, реалізуючи законодавство 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 існували до того часу. Таким чином, у статті 8 (1) Хартії не тільки чітко визнається право на захист персональних даних, але й вказуються основні принципи захисту персональних даних (стаття 8 (2)). І нарешті, положення статті 8 (3) Хартії вимагають здійснення незалежним органом контролю за дотриманням цих принципів.

Прийняття Лісабонського договору стало визначальним у розвитку захисту персональних даних не тільки в зв'язку з набуттям Хартією основних прав ЄС статусу юридично обов'язкового документа на рівні первинного законодавства, але й в зв'язку з проголошенням права на захист персональних даних. Це право чітко передбачається в статті 16 ДфЄС у розділі, присвяченому загальним принципам діяльності ЄС. Стаття 16 створює нову юридичну основу через надання ЄС повноважень законодавчо регулювати питання захисту персональних даних. Це важливе зрушення, оскільки правила захисту персональних даних ЄС – а саме Директива про захист персональних даних – початково спиралися на правові норми внутрішнього ринку та на необхідність гармонізації національних законів з метою забезпечення необмеженого руху даних у межах ЄС. Нині стаття 16 ДфЄС становить незалежну юридичну основу для сучасного всестороннього підходу до захисту персональних даних, який охоплює всі питання компетенції ЄС, включаючи поліцейське та судове співробітництво в питаннях кримінального права. Стаття 16 ДфЄС також передбачає, що дотримання правил захисту даних, які прийняті відповідно до неї, мають контролюватись незалежним контролюючим органом. Стаття 16 також стала юридичною основою для прийняття всебічної реформи правил захисту даних у 2016 році, а саме прийняття Загального регламенту захисту персональних даних та Директиви про захист персональних даних для органів поліції та кримінальної юстиції (див. нижче).

Загальний регламент захисту персональних даних

З 1995 року до травня 2018 року основним юридичним інструментом ЄС з питань захисту персональних даних була Директива Європейського Парламенту та Ради 95/46/ЕС від 24 жовтня 1995 року про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних (Директива про захист персональних даних)[29]. Вона була прийнята 1995 року, у час, коли декілька держав-членів вже прийняли національні закони про захист персональних даних[30]. Її прийняття було зумовлене необхідністю гармонізувати ці закони та забезпечити високий рівень захисту і вільний рух персональних даних між державами-членами. Вільний рух товарів, капіталу, послуг та людей у межах внутрішнього ринку вимагав вільного руху даних, який не міг бути забезпечений, доки держави-члени не мали уніфікованого високого рівня захисту персональних даних.

Директива про захист персональних даних передбачала принципи захисту, які вже передбачали національні закони та Конвенція 108, і часто їх розширювала. Вона використала можливість, передбачену в статті 11 Конвенції 108, стосовно доповнення інструментів захисту. Зокрема, запровадження в Директиві незалежного контролю як інструмента покращення дотримання правил захисту даних стало важливим внеском в ефективне функціонування права ЄС щодо захисту персональних даних. У подальшому цей елемент було включено до нормативно-правових документів РЄ у 2001 році додатковим протоколом до Конвенції 108. Це демонструє існування протягом років тісного взаємозв'язку та взаємного позитивного впливу цих двох інструментів.

Директива про захист персональних даних встановила деталізовану та всебічну систему захисту персональних даних у ЄС. Однак відповідно до правової системи ЄС директиви безпосередньо не застосовуються, вони мають бути імплементовані в національні закони держав-членів. Держави-члени при цьому користуються свободою розсуду щодо імплементації положень директив. Незважаючи на те, що Директива мала на меті забезпечити цілковиту

29 Директива Європейського парламенту та Ради від 24 жовтня 1995 року 95/46/ЕС про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних, OJ 1995 L 281.

30 Німецька земля Гессен прийняла у 1970 році перший у світі Закон про захист персональних даних, який застосовувався тільки на її території. Швеція прийняла Закон про дані (*Datalagen)* у 1973 році; Німеччина прийняла відповідний Закон (*Bundesdatenschutzgestez)* у 1976 році; у Франції було прийнято Закон про захист даних (*Loi relatif à l'informatique, aux fichiers et aux libertés)* у 1977 році. У Сполученому Королівстві Закон про захист даних було прийнято в 1984 році. Нарешті Нідерланди прийняли Закон про дані (*Wet Persoonregistraties*) в 1989 році.

гармонізацію[31] (та повний рівень захисту), на практиці вона була імплементована державами-членами по-різному. Це призвело до появи відмінних норм захисту персональних даних у ЄС з визначеннями та правилами, які по різному тлумачились у національних законах. Рівень реалізації та тяжкості санкцій також різнився поміж державами-членами. Нарешті, з часу проєктування Директиви в середині 1990-х відбулися значні зміни в інформаційних технологіях. Усе це в цілому зумовило проведення реформи у сфері захисту персональних даних ЄС.

Після років інтенсивних обговорень реформа призвела до прийняття Загального регламенту захисту персональних даних у квітні 2016 року. Дискусії щодо необхідності модернізувати правила захисту даних ЄС почалися 2009 року, коли Комісія ініціювала публічні обговорення щодо системи майбутнього юридичного регулювання основоположного права на захист персональних даних. Пропозиції щодо регламенту були опубліковані Комісією у січні 2012 року, таким чином розпочавши тривалий законодавчий процес переговорів між Європейським парламентом та Радою ЄС. Після прийняття Загальний регламент захисту персональних даних передбачав дворічний перехідний період. У повному обсязі він почав застосовуватися з 25 травня 2018 року, тоді ж припинила дію Директива про захист персональних даних.

Прийняття Загального регламенту захисту персональних даних у 2016 році модернізувало законодавство ЄС із захисту персональних даних, яке могло тепер забезпечити захист основоположних прав у контексті економіки та соціальних викликів цифрової ери. ЗРЗПД зберіг та розвинув ключові принципи та права суб'єкта персональних даних, які передбачалися Директивою про захист персональних даних. Крім того, він встановив нові обов'язки, які вимагають від організацій забезпечити, щоб їхні системи за замовчуванням автоматично застосовували захист персональних даних; призначити за певних умов спеціаліста із захисту персональних даних; дотримуватися нового права щодо передачі даних; та дотримуватися принципу підзвітності. Відповідно до законодавства ЄС регламентні норми застосовуються безпосередньо, для цього немає необхідності імплементувати їх до національного законодавства. Таким чином, Загальний регламент захисту персональних даних передбачає єдиний набір правил захисту персональних даних для всіх держав – членів

31 Суд ЄС, 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» CJEU, (*Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*), від 24 листопада 2011, п. 29.

ЄС. Це створює єдині узгоджені правила захисту персональних даних для всього Європейського Союзу, встановлюючи простір юридичної визначеності, з якого мають користь як суб'єкти економічної діяльності, так і фізичні особи – суб'єкти персональних даних.

Навіть при тому, що Загальний регламент захисту персональних даних застосовується безпосередньо, від держав-членів все ж очікується внесення змін до чинних законів із захисту персональних даних для забезпечення повної відповідності до регламентних норм, водночас з наданням їм свободи розсуду щодо положень статті 10. Передбачені ЗРЗПД головні правила та принципи, а також важливі права, які надаються фізичним особам, становлять більшу частину цього посібника та викладаються в наступних главах. Регламент містить комплексні правила щодо територіальної застосовності. Він застосовується до підприємств, створених у ЄС, а також до контролерів та операторів, які були створені не в ЄС, але які надають товари або послуги суб'єктам персональних даних у ЄС або моніторять їхню поведінку. Оскільки певна кількість закордонних технологічних компаній володіють значною часткою європейського ринку та мають мільйони європейських покупців, поширення на них правил ЄС із захисту персональних даних є важливим для забезпечення захисту фізичних осіб, а також для забезпечення рівних «умов гри».

Захист даних у сфері правоохоронної діяльності – Директива 2016/680

Визнана недійсною Директива про захист персональних даних передбачала всебічну систему захисту персональних даних. Ця система була надалі зміцнена прийняттям Загального регламенту про захист персональних даних. Хоча ця Директива була комплексною, сфера її застосування була обмежена діяльністю внутрішнього ринку та діяльністю державних органів, окрім правоохоронних. Таким чином, було необхідно прийняти спеціальний документ для досягнення необхідної чіткості та балансу між захистом персональних даних та іншими легітимними інтересами, а також для подолання проблем, що особливо характерні для певних секторів. Саме такою була ситуація щодо правил регулювання обробки персональних даних правоохоронними органами.

Першим юридичним актом ЄС щодо регулювання цих питань було Рамкове рішення Ради ЄС № 2008/977/ЈНА про захист персональних даних, що обробляються в рамках поліцейського та судового співробітництва в кримінальних справах. Його норми застосовувались тільки до даних поліції та судових органів при обміні між державами-членами, а обробку

персональних даних правоохоронними органами на національному рівні було виключено зі сфери її дії.

Директива (ЄС) 2016/680 про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами влади в цілях попередження, розслідування, виявлення кримінальних правопорушень та притягнення до відповідальності за їх вчинення або виконання кримінальних покарань та про вільне переміщення таких даних[32], яку називають Директивою про захист персональних даних для поліції та органів кримінальної юстиції, виправила цю ситуацію. Прийнята одночасно із Загальним регламентом захисту персональних даних, Директива замінила Рамкове рішення 2008/977/JHA та запровадила всебічну систему захисту персональних даних у контексті діяльності правоохоронних органів, водночас з визнанням особливостей обробки персональних даних, пов'язаної з національною безпекою. Як Загальний регламент захисту персональних даних передбачає загальні правила захисту фізичних осіб щодо обробки їхніх персональних даних та забезпечення вільного переміщення таких даних у межах ЄС, Директива встановлює спеціальні правила для захисту даних у сферах судового співробітництва в кримінальних справах та співпраці органів поліції. У разі, якщо компетентний орган здійснює обробку персональних даних для цілей попередження, розслідування, виявлення кримінальних правопорушень або переслідування за їх вчинення, буде застосовуватися Директива 2016/680. Якщо компетентні органи влади обробляють персональні дані для цілей інших, ніж ті, що вказано вище, застосовується загальна система захисту, що передбачена Загальним регламентом захисту персональних даних. На противагу попередньому документові (Рамкове рішення Ради 2008/977/JHA), сфера дії Директиви 2016/680 поширюється на національний рівень обробки персональних даних правоохоронними органами і не обмежується обміном такими даними між державами-членами. Крім того, Директива спрямована на досягнення балансу між правами фізичних осіб та легітимними цілями обробки, пов'язаної з національною безпекою.

Для цих цілей Директива утверджує право на захист персональних даних та ключові принципи, яким має відповідати обробка даних, чітко дотримуючись правил і принципів, передбачених Загальним регламентом захисту персональних даних. Права фізичних осіб та обов'язки, покладені на контролерів,

32 Директива (ЄС) 2016/680 про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами влади в цілях запобігання, розслідування, виявлення кримінальних правопорушень та притягнення до відповідальності за їх вчинення або виконання кримінальних покарань та про вільне переміщення таких даних, OJ L 119, від 4 травня 2016.

наприклад, щодо безпеки даних, захисту даних як елемента системи за замовчуванням і повідомлення про витік відповідають правам та обов'язкам, передбаченим Загальним регламентом захисту персональних даних. Директива також враховує та намагається надати відповідь на появу серйозних викликів, пов'язаних з технологіями, які можуть мати особливо негативний вплив на осіб, як-от використання правоохоронними органами технологій профайлінгу. Прийняття рішень виключно на підставі автоматичної обробки даних, включно з профайлінгом, в принципі має бути заборонено[33]. Крім того, рішення не мають ґрунтуватися на чутливих даних. Директива передбачає й певні винятки з дотримання цих принципів. До того ж така обробка не повинна призводити до дискримінації будь-якої особи[34].

Директива також містить правила щодо забезпечення підзвітності контролерів. Вони мають призначити спеціаліста із захисту персональних даних для здійснення моніторингу дотримання правил у цій сфері, інформування та надання рекомендацій організації і працівникам, які здійснюють обробку, щодо їхніх обов'язків та співпраці з органом. Наразі обробка персональних даних поліцією та в сфері кримінальної юстиції є об'єктом контролю незалежних контролюючих органів. Як загальна юридична система захисту персональних даних, так і спеціальна система для правоохоронних органів та системи кримінальної юстиції повинні однаковою мірою відповідати вимогам Хартії основних прав ЄС.

Спеціальна система захисту даних у контексті поліцейського та судового співробітництва, передбачена Директивою про захист персональних даних для поліції та органів кримінальної юстиції, детально описується в главі 8.

Директива про конфіденційність та електронні комунікації

Також виявилося необхідним запровадити спеціальне законодавство із захисту персональних даних у секторі електронних комунікацій. З розвитком інтернету, провідного та мобільного телефонного зв'язку було важливо забезпечити дотримання прав користувачів на приватність та конфіденційність. Директива 2002/58/ЕС[35] про обробку персональних даних та захист таємниці

33 Директива про захист персональних даних, що обробляються в рамках поліцейського та судового співробітництва в кримінальних справах, стаття 11 (1).

34 Там само, статті 11 (2) та (3).

35 Директива 2002/58/ ЄС Європейського Парламенту та Ради про обробку персональних даних та захист таємниці в секторі електронних комунікацій (Директива про конфіденційність та електронні комунікації) OJ L 201.

в секторі електронних комунікацій (Директива про конфіденційність та електронні комунікації) встановлює низку правил щодо захисту персональних даних у цих мережах, повідомлення про порушення захисту персональних даних і конфіденційність комунікацій.

Заради безпеки оператори електронних комунікаційних послуг, серед іншого, повинні забезпечити, щоб доступ до персональних даних мали тільки уповноважені особи, та вживати заходів для попередження знищення даних, втраті або неумисному їх пошкодженню[36]. Якщо існує особливий ризик порушення безпеки громадської мережі, оператори мають інформувати абонентів про такі ризики[37]. Якщо, незважаючи на вжиті заходи безпеки, порушення безпеки мало місце, оператори повинні повідомити компетентний орган влади, уповноважений виконувати директиву щодо порушення захисту персональних даних. У певних випадках оператори зобов'язані також повідомляти фізичних осіб про порушення захисту персональних даних, а саме у випадках, коли порушення може призвести до негативного впливу на їхні персональні дані або приватне життя[38]. Конфіденційність спілкування вимагає заборони прослуховування, підключення до систем, зберігання даних або будь-які інші види стеження чи перехоплення комунікацій та метаданих. Ця Директива також забороняє незапитувані повідомлення (які часто називають спамом), якщо користувачі не надали на них згоди, а також містить правила зберігання файлів «cookie» в комп'ютерах та інших пристроях. Ці ключові негативні зобов'язання чітко вказують на те, що конфіденційність комунікації суттєво пов'язана із захистом права на повагу до приватного життя, передбаченого в статті 7 Хартії, та права на захист персональних даних, передбаченого в статті 8 Хартії.

У січні 2017 року Комісія опублікувала проєкт акта стосовно поваги до приватного життя та захисту персональних даних у секторі електронних комунікацій, що означає заміну Директиви про конфіденційність та електронні комунікації. Реформа має на меті узгодження правил регулювання електронних комунікацій з новою системою регулювання захисту персональних даних, передбаченою Загальним регламентом про захист персональних даних. Нове регулювання буде безпосередньо застосовуватись у державах – членах ЄС; усі фізичні особи матимуть однаковий рівень захисту своїх електронних комунікацій; усі телекомунікаційні оператори та підприємства отримають переваги

36 Директива про конфіденційність та електронні комунікації, стаття 4 (1).

37 Там само, стаття 4 (2).

38 Там само, стаття 4 (3).

від чіткості, юридичної визначеності та існування єдиних правил для всіх держав – членів ЄС. Запропоновані норми регулювання електронних комунікацій також будуть застосовуватися до нових гравців, які надають електронні комунікаційні послуги, але які не охоплюються Директивою про конфіденційність та електронні комунікації. Ця Директива охоплює тільки традиційних надавачів телекомунікаційних послуг. Враховуючи масове використання послуг, що надаються скайпом, вотсапом, фейсбук месенджером та вайбером з направлення повідомлень або здійснення телефонних дзвінків, ці інтернет-технології (OTT послуги) тепер будуть підпадати під дію норм регулювання та будуть вимушені дотримуватися вимог захисту персональних даних, приватності та безпеки. Станом на час публікації цього посібника законодавчий процес щодо регулювання захисту приватності в секторі електронних комунікацій (e-Privacy rules) ще тривав.

Регламент № 45/2001

Оскільки Директива про захист персональних даних могла застосовуватись виключно до держав-членів ЄС, було необхідно створити додатковий юридичний інструмент захисту персональних даних при їх обробці інституціями та органами ЄС. Це завдання виконав Загальний регламент (ЄС) № 45/2001 про захист фізичних осіб при обробці персональних даних інститутами і органами Співтовариства і про вільне переміщення таких даних (Загальний регламент інститутів ЄС про захист персональних даних)[39].

Регламент № 45/2001 точно слідує принципам загальної системи ЄС щодо захисту персональних даних та застосовує ці принципи до обробки персональних даних інституціями та органами ЄС при виконанні своїх функцій. Крім того, він запроваджує незалежний контролюючий орган для моніторингу застосування його положень – Європейського інспектора із захисту персональних даних (ЄІЗПД). ЄІЗПД наділений наглядовими повноваженнями та має завдання здійснювати моніторинг обробки персональних даних інституціями та органами ЄС, а також здійснювати розгляд та розслідування скарг про стверджуване порушення правил захисту персональних даних. Він також надає рекомендації інституціям та органам ЄС щодо всіх питань, пов'язаних із захистом персональних даних – від пропозицій щодо нового законодавства до формування внутрішніх правил стосовно обробки персональних даних.

39 Загальний регламент (ЄС) № 45/2001 від 18 грудня 2000 року про захист фізичних осіб при обробці персональних даних інститутами і органами Співтовариства і про вільне переміщення таких даних, OJ 2001 L 8.

У січні 2017 року Європейська Комісія представила пропозиції щодо нового Регламенту про обробку персональних даних інституціями та органами ЄС, який замінить чинний на сьогодні Регламент. Так само як і реформа Директиви про конфідеційність та електронні комунікації, реформа Регламенту № 45/2001 модернізує та узгодить ці правила з новою системою захисту персональних даних, передбаченою Загальним регламентом про захист персональних даних.

Роль Суду Європейського Союзу

СЄС має юрисдикцію визначати, чи виконали держави-члени свої зобов'язання за законодавством ЄС у сфері захисту персональних даних, та надавати тлумачення права ЄС для забезпечення його ефективного та уніфікованого застосування всіма державами-членами. З часу прийняття Директиви про захист персональних даних у 1995 році СЄС сформував значну практику, роз'яснюючи обсяг та значення принципів захисту персональних даних та основоположного права про захист персональних даних, яке передбачено статтею 8 Хартії. Попри те, що Директива була скасована, і сьогодні діє новий юридичний акт – Загальний регламент захисту персональних даних – сформована до цього судова практика залишається релевантною та актуальною для тлумачення та застосування принципів захисту персональних даних тією мірою, якою ключові принципи та концепції Директиви про захист персональних даних були закріплені ЗРЗПД.

1.2 Обмеження права на захист персональних даних

Ключові моменти

- Право на захист персональних даних не є абсолютним; воно може бути обмежено за потреби для задоволення загального інтересу або захисту прав і свобод інших осіб.
- Умови обмеження права на повагу до приватного життя та права на захист персональних даних передбачені статтею 8 ЄКПЛ та статтею 52 (1) Хартії. Вони були розтлумачені та розвинуті у практиці ЄСПЛ та СЄС.
- Відповідно до права РЄ про захист персональних даних, обробка персональних даних є правомірним втручанням у право на повагу до приватного життя, якщо воно:

- здійснюється згідно із законом;
- переслідує легітимну мету;
- здійснюється із повагою до суті основоположних прав і свобод;
- необхідне та пропорційним в демократичному суспільстві для досягнення легітимної мети.

- Право ЄС передбачає схожі умови обмеження реалізації основоположних прав і свобод, передбачених у Хартії. Будь-яке обмеження будь-яких основоположних прав, включно із правом на захист персональних даних, може бути правомірним у разі, якщо воно:
  - здійснюється згідно із законом;
  - забезпечує дотримання суті права;
  - спирається на принцип пропорційності і застосовується лише в тому випадку, якщо є необхідним;
  - переслідує мету загального інтересу, визнаного ЄС, або є необхідним для захисту прав і свобод інших людей.

Основоположне право на захист персональних даних за статтею 8 Хартії не є абсолютним «і повинно розглядатися у зв'язку з його функцією в суспільстві»[40]. Тому в статті 52 (1) Хартії визнається, що на здійснення таких прав можуть бути накладені обмеження, наприклад, такі, які викладені в статтях 7 і 8 Хартії, тією мірою, якою вони передбачені законом, забезпечують дотримання суті цих прав і свобод, здійснюються з дотриманням принципу пропорційності і застосовуються лише в тому разі, якщо є необхідними й дійсно задовольняють цілі загального інтересу, визнаного Європейським Союзом, або необхідні для захисту прав і свобод інших людей[41]. У схожий спосіб у системі ЄКПЛ право на захист персональних даних гарантоване статтею 8, і реалізація цього права може бути обмежена в разі необхідності для досягнення легітимної мети. Ця глава присвячена умовам втручання відповідно до ЄКПЛ, тлумачення якої надано ЄСПЛ, а також умовам правомірного обмеження відповідно до статті 52 Хартії.

40 Суд ЄС, об'єднані справи, C-92/09 та C-93/09 «"Volker und Markus Schecke GbR" та Хартмут Ейферт проти землі Гессен» (*Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*) [ВП], від 9 листопада 2010,п. 48.

41 Там само, п. 50.

1.2.1 Вимоги для виправданого втручання за ЄКПЛ

Обробка персональних даних може становити втручання у право на повагу до приватного життя суб'єкта персональних даних, яке захищається статтею 8 ЄКПЛ[42]. Як пояснюється вище (див. *розділ 1.1.1.* та *розділ 1.1.4.*), на противагу законодавству ЄС, ЄКПЛ не передбачає захист персональних даних як окреме основоположне право. Захист персональних даних становить частину прав, які захищаються правом на повагу до приватного життя. Таким чином, не кожна дія, яка включає обробку персональних даних, охоплюється обсягом статті 8 ЄКПЛ. Для застосування статті 8 перш за все має бути визначено, чи було обмежено приватний інтерес або приватне життя особи. У своїй практиці ЄСПЛ тлумачить поняття «приватне життя» як широку концепцію, що охоплює навіть аспекти професійного життя та публічної поведінки. Він також вирішив, що захист персональних даних є важливим аспектом приватного життя. Однак, попри розширене тлумачення приватного життя, не всі види обробки можуть вважатись обмеженням прав, передбачених статтею 8.

Якщо ЄСПЛ визнає, що дія з обробки персональних даних, про яку йдеться, вплинула на право особи на повагу до приватного життя, він буде розглядати, чи було втручання виправданим. Право на повагу до приватного життя не є абсолютним правом, воно має бути збалансоване і узгоджене з іншими легітимними інтересами та правами, незалежно від того, чи це інтереси інших осіб (приватні інтереси), чи інтереси суспільства в цілому (суспільні інтереси).

Загалом умови, за яких втручання може бути виправдане, є такими:

Згідно із законом

Практика ЄСПЛ визнає втручання таким, що здійснено згідно із законом, якщо воно передбачено у положеннях національного законодавства, що має певні характеристики. Закон повинен бути «доступним для зацікавлених осіб і передбачуваним щодо наслідків його дії»[43]. Положення є передбачуваним, «якщо воно сформульовано з достатньою чіткістю, що дає змогу кожному, у

42 Рішення ЄСПЛ у справі «С. та Марпер проти Сполученого Королівства» (*S. and Marper v. the United Kingdom)* [ВП], №№ 30562/04 та 30566/04, 4 грудня 2008 р., п. 67.

43 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 та інші проти Молдови» (*Iordachi and Others v. Moldova*), № 25198/02 від 10 лютого 2009 р., п. 50.

разі необхідності із отриманням належного роз'яснення, вивіряти свою поведінку»[44]. «Ступінь чіткості, що вимагається від закону у зв'язку з цим залежатиме від конкретного питання»[45].

Приклад: у справі «*Ротару проти Румунії*»[46] заявник стверджував про порушення його права на повагу до приватного життя у зв'язку зі збереженням та використанням файлу, який містив інформацію про нього, Службою безпеки Румунії. ЄСПЛ встановив порушення статті 8 ЄКПЛ через той факт, що румунське законодавство дозволяє 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, яку можна обробляти, категорії людей, до яких застосовуються заходи стеження, обставини, за яких можуть бути вжиті такі заходи, або процедури, яких необхідно дотримуватися. З огляду на ці недоліки Суд дійшов висновку, що національне законодавство не відповідає вимозі передбачуваності в контексті статті 8 ЄКПЛ, і що цю статтю було порушено.

У справі «*Тейлор-Себорі проти Сполученого Королівства*»[47] за заявником було встановлено поліцейське стеження. За допомогою пейджера – клона заявника поліція змогла перехопити надіслані йому повідомлення. Згодом заявника заарештували і йому були пред'явлені обвинувачення у змові щодо постачання наркотиків. Частину доказів обвинувачення у справі становили записані сучасним способом повідомлення з пейджера,

44 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 «Мелоун проти Сполученого Королівства» (*Malone v. the United Kingdom*), № 8691/79 від 2 серпня 1984р., п. 66; рішення ЄСПЛ у справі «Сілвер та інші 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.

45 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 «Сілвер та інші 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.

46 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 «Шимоволос 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.

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

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 «згідно із законом». ЄСПЛ дійшов висновку, що було порушено статтю 8 ЄКПЛ.

Справа «*Вукота-Божич проти Швейцарії*»[48] стосується прихованого стеження за заявницею, яка вимагала виплати соціального страхування, приватними слідчими, найнятими страховою компанією. ЄСПЛ визнав, що оскільки заходи зі стеження були ініційовані приватною страховою компанією, держава надала цій компанії право отримувати вигоду від обов'язкового медичного страхування та збирати страхові виплати. Держава не може зняти з себе відповідальність за Конвенцією через делегування її обов'язків приватним організаціям або фізичним особам. Національне законодавство не передбачало достатніх гарантій від свавілля для забезпечення того, щоб втручання у права за статтею 8 ЄКПЛ здійснювалось «згідно із законом». У цій справі ЄСПЛ дійшов висновку, що мало місце порушення статті 8 ЄКПЛ, оскільки національне законодавство не визначало з достатньою чіткістю обсяг та спосіб реалізації дискреції, наданої страховим компаніям, які діяли як публічні органи влади у вирішенні страхових спорів, щодо здійснення прихованого стеження за застрахованими особами. Зокрема, національний закон не надавав достатніх гарантій проти свавілля.

Переслідування легітимної мети

Легітимна мета може бути або одним із перерахованих суспільних інтересів, або ж якимсь із захищених прав і свобод інших осіб. Легітимними інтересами, які можуть виправдати втручання відповідно до статті 8 (2) ЄКПЛ, є інтереси національної та громадської безпеки чи економічного добробуту країни, попередження заворушень чи злочинів, захист здоров'я чи моралі або захист прав і свобод інших осіб.

48 Рішення ЄСПЛ у справі «*Вукота-Божич проти Швейцарії*» (*Vukota-Bojić v. Switzerland*), № 61838/10, від 18 жовтня 2016 р., п. 77.

Приклад: у справі «*Пек проти Сполученого Королівства*»[49] 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, вони передали 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 статтю 8 ЄКПЛ було порушено.

Необхідність у демократичному суспільстві

ЄСПЛ зазначив, що «поняття необхідності означає, що втручання відповідає нагальній суспільній потребі і, зокрема, є пропорційним переслідуваній легітимній меті»[50]. При оцінці того, чи є захід необхідним для реагування на нагальну суспільну потребу, ЄСПЛ розглядає його відповідність та належність відносно мети, яка переслідується. З цією метою Суд може взяти до уваги, чи намагається втручання вирішити питання, яке, якщо його не вирішувати, може мати негативний вплив на суспільство, чи є свідчення того, що втручання може зменшити такий негативний вплив, та які існують більш широкі соціальні погляди на питання, що розглядається[51]. Наприклад, збір та зберігання службами безпеки персональних даних окремих фізичних осіб, що, як з'ясовано, мають зв'язки з терористичними рухами, становитиме втручання в право цих осіб на повагу до приватного життя, що, тим не менш буде відповідати серйозній нагальній суспільній потребі: національній безпеці та боротьбі з тероризмом. Для дотримання тесту необхідності втручання також має бути пропорційним. У практиці ЄСПЛ пропорційність розглядається в межах концепції необхідності. Пропорційність вимагає, щоб втручання в гарантовані ЄКПЛ права не було більшим, ніж це необхідно для досягнення легітимної мети, яка переслідується. Важливими факторами, які мають враховуватися

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

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

51 Робоча група «Стаття 29» (2014), Висновок щодо застосування концепцій необхідності та пропорційності та захисту персональних даних у роботі правоохоронних органів (*Opinion on the application of the necessity and proportionality concepts and data protection within the law enforcement sector*), РГ 211, Брюссель, від 27 лютого 2014 р., пп. 7–8.

при здійсненні тесту пропорційності, є обсяг втручання, кількість осіб, на яких здійснюється вплив, та гарантії або застереження, що мають на меті обмеження обсягу та негативного впливу на права осіб[52].

Приклад: у справі «*Хелілі проти Швейцарії*»[53] під час рейду поліція виявила в заявниці візитівки з номером телефону і таким текстом: «Симпатична, гарна жінка, за тридцять, хотіла б зустріти чоловіка, щоб іноді разом випити або проводити час. Номер тел. [...]». Заявниця стверджувала, що після цього поліцейські внесли в базу її ім'я як повії, якою, як вона стверджувала, вона ніколи не була. Заявниця вимагала видалити слово «повія» з комп'ютерної бази. ЄСПЛ визнав, що, загалом, 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 в 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 втручання не може розглядатися як таке, що відповідає «нагальній суспільній потребі» в розумінні статті 8 ЄКПЛ. Розглядаючи питання доведення достовірності збережених про заявницю даних як таке, що належить до повноважень органів влади, а також зважаючи на серйозне втручання в права заявниці, Суд постановив, що збереження слова «повія» у файлах поліції протягом багатьох років не було необхідним у демократичному суспільстві. Суд дійшов висновку, що було порушено статтю 8 ЄКПЛ.

Приклад: у справі «*С. та Марпер проти Сполученого Королівства*»[54] два заявника були заарештовані та обвинувачені у вчиненні кримінального порушення. Поліція відібрала в них відбитки пальців і зразки ДНК на підставі Закону про поліцію та кримінальні докази. Заявники так і не були засуджені за вчинення злочинів: один був виправданий судом, а кримінальне провадження щодо другого заявника було закрито. Однак їхні відбитки пальців, профілі ДНК та клітинні зразки зберігались поліцією в базі даних, при цьому національне законодавство дозволяло їх збереження

52 Там само, с. 9–11.

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

54 Рішення ЄСПЛ у справі «С. та Марпер проти Сполученого Королівства» (*S. and Marper v. the United Kingdom*) [ВП], №№ 30562/04 та 30566/04, 4 грудня 2008 р.

безстроково. Хоча Сполучене Королівство доводило, що збереження даних допомагає в ідентифікації майбутніх злочинців і таким чином переслідувало легітимну мету виявлення та попередження злочинів, ЄСПЛ вирішив, що втручання у право заявників на повагу до приватного життя було не виправданим. Він нагадав, що ключові принципи захисту персональних даних вимагають, щоб збереження даних було пропорційним стосовно мети їх збору та щоб період збереження даних був обмеженим. Суд погодився, що розширення бази даних і включення в них профілів ДНК не тільки засуджених осіб, але й осіб, які підозрювались, але не були засуджені, могло б сприяти виявленню та попередженню злочинів у Сполученому Королівстві. Однак, він був «вражений всеосяжним та нерозбірливим характером повноважень щодо збереження даних»[55].

Враховуючи велику кількість генетичної інформації та інформації про здоров'я, яка міститься в клітинних зразках, втручання у право заявників було особливо серйозним. Відбитки пальців та зразки могли бути відібранні в заарештованих осіб та зберігатися протягом невизначеного періоду в базі даних поліції, незалежно від характеру та серйозності порушення, навіть у випадку незначних порушень, за вчинення яких не передбачалось позбавлення волі. Більше того, можливості для виправданих осіб видалити інформацію щодо себе з бази даних були обмежені. Нарешті, ЄСПЛ також звернув увагу на вік заявника, якому під час затримання було лише 11 років. Зберігання персональних даних неповнолітніх, які не були засуджені, може бути особливо шкідливим з огляду на їхню вразливість і важливість їхнього розвитку та інтеграції у суспільство[56]. У цій справі Суд одностайно вирішив, що зберігання даних становить непропорційне втручання в право на повагу до приватного життя, яке не може бути визнано необхідним в демократичному суспільстві.

Приклад: у справі «*Леандер проти Швеції*»[57] ЄСПЛ постановив, що власне сама таємна перевірка осіб, які подають документи для працевлаштування на посади, що є важливими з точки зору національної безпеки, не суперечить вимозі необхідності в демократичному суспільстві. Існування спеціальних гарантій, які передбачені в національному законодавстві

55 Там само, п. 119.

56 Там само, п. 124.

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

для захисту інтересів суб'єктів персональних даних, наприклад, 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 наявні у неї широкі межі розсуду, держава-відповідач мала право вважати, що у справі заявника інтереси національної безпеки переважали над особистими. Суд дійшов висновку, що статтю 8 ЄКПЛ не було порушено.

1.2.2 Умови правомірних обмежень відповідно до Хартії основних прав ЄС

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

Відповідно до статті 52 (1) Хартії обмеження щодо здійснення гарантованих Хартією прав і свобод і, відповідно, щодо здійснення права на захист персональних даних, допускаються тільки, якщо вони:

- передбачені законом;
- забезпечують дотримання суті права на захист персональних даних;
- є необхідними, відповідають принципу пропорційності[58];
- відповідають цілям загального інтересу, що визнаний Європейським Союзом, або є необхідними для захисту прав і свобод інших осіб.

Оскільки право на захист персональних даних є окремим основоположним правом у системі права ЄС, яке гарантується статтею 8 Хартії, будь-яка обробка персональних даних сама собою становить втручання в це право. Неважливо, чи мають відношення персональні дані до приватного життя особи, чи є вони чутливими, або чи відчули суб'єкти персональних даних будь-які незручності. Для того, щоб бути правомірним, втручання має відповідати всім умовам, передбаченим статтею 52 (1) Хартії.

58 Посібник про оцінку необхідності заходів з обмеження основоположного права на захист персональних даних, ЄІЗПД (2017), (*Посібник з необхідності*), Брюссель, від 11 квітня 2017 р.

Передбачене законом

Обмеження права на захист персональних даних має бути передбачене законом. Ця вимога означає, що обмеження мають ґрунтуватися на правових положеннях, які належним чином доступні й передбачувані та сформульовані з належною чіткістю, щоб кожен міг розуміти свої права та регулювати свою поведінку. Правові підстави також мають чітко визначати обсяг та спосіб реалізації повноважень компетентними органами з метою захисту фізичної особи від свавільного втручання. Це тлумачення схоже на вимогу «законного втручання», яка наводиться в практиці ЄСПЛ[59], і висловлюється думка, що значення формулювання «передбачене законом», що використовується в Хартії, має розумітися так само, як у практиці ЄСПЛ[60]. Практика ЄСПЛ, особливо концепція «якості закону», яку він розвинув протягом років, є релевантною і має враховуватися СЄС при тлумаченні обсягу статті 52 (1) Хартії[61].

Дотримання суті права

Відповідно до права ЄС будь-яке обмеження основоположних прав, які захищені Хартією, має здійснюватися з дотриманням суті цих прав. Це означає, що обмеження, які є настільки серйозними та всеосяжними, що позбавляють права їхнього основного змісту, не можуть бути виправданими. Якщо суть права порушується, обмеження має визнаватися неправомірним, без необхідності подальшого аналізу щодо наявності загального інтересу, необхідності та пропорційності.

Приклад: справа «*Шремса*»[62] стосувалася захисту фізичних осіб від передання їхніх персональних даних третім державам, у даному випадку мова йшла про Сполучені Штати Америки. Шремс, громадянин Австрії,

59 ЄІЗПД (2017), Посібник з необхідності, Брюссель, від 11 квітня 2017 р., с. 4; див також Висновок Суду ЄС 1/15 (Велика Палата), (*Opinion 1/15 of the Court (Grand Chamber)* від 26 липня 2017 р.

60 Об'єднані справи Суду ЄС C-203/15 та C-698/15 «"Tele2 Sverige AB" проти Державного управління зв'язку та телекомунікації» та «Секретар внутрішніх справ проти Тома Вотсона та інших» (*Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis*), Висновок генерального адвоката Саугмандсгаард від 19 липня 2016 р., п. 140.

61 Рішення Суду ЄС у справі C-70/10 «"Scarlet Extended SA" проти Бельгійської асоціації авторів, композиторів та видавців (SABAM)» (*Scarlet Extended SA v. Société belge des auteurs compositeurs et éditeurs (SABAM)*, Висновок генерального адвоката Круза Віллалона від 14 квітня 2011 р., п. 100.

62 Рішення Суду ЄС у справі C-362/14, «Максиміліан Шремс проти Уповноваженого із захисту персональних даних» (*Maximillian Schrems v. Data Protection Commissioner*) [ВП], від 6 жовтня 2015 р.

який був користувачем Facebook декілька років, звернувся до ірландського контролюючого органу із скаргою на передання ірландською філією «Facebook» персональних даних до «Facebook Inc.» та на розташовані в Сполучених Штатах сервери, де вони оброблялись. Він стверджував, що з огляду на свідчення 2013 року американського викривача Едварда Сноудена щодо діяльності зі стеження американських спецслужб, законодавство та правозастосування Сполучених Штатів не надавали належного захисту персональних даних, які передаються на їхню територію. Сноуден навів дані, що Агентство національної безпеки безпосередньо підключалося до серверів компаній, таких як «Facebook», та могло читати вміст чатів та приватні повідомлення.

Передача даних до Сполучених Штатів відбувалася на основі рішення Комісії щодо відповідності, яке було прийняте у 2000 році та дозволяло передачу даних до компаній Сполучених Штатів, що взяли на себе зобов'язання захищати персональні дані, передані з території ЄС, та дотримуватися так званих «принципів безпечної гавані» (Safe Harbour principles). Коли справу було передано СЄС, він розглянув правомірність рішення у світлі положень Хартії. Він нагадав, що система захисту основоположних прав ЄС вимагає, щоб будь-який відступ або обмеження прав застосовувались виключно у разі гострої необхідності. СЄС визнав законодавство, яке дозволяло органам влади мати доступ за загальним правилом до змісту електронних комунікацій таким, що «порушує суть основоположного права на повагу до приватного життя, гарантованого статтею 7 Хартії». Це право не матиме сенсу, якщо органи влади Сполучених Штатів будуть мати можливість доступу до комунікацій на повсякденній основі без будь-якого об'єктивного виправдання конкретними міркуваннями національної безпеки або попередження злочину, до яких причетна конкретна особа, а також за відсутності належних запобіжників проти зловживання під час операцій зі стеження.

Більше того, СЄС зазначив, що «законодавство, яке не передбачає жодної можливості для фізичної особи скористатись юридичними засобами для отримання доступу до своїх персональних даних або вимоги їх зміни чи видалення» є несумісним з основоположним правом на ефективний судовий захист (стаття 47 Хартії). Таким чином, «принципи безпечної гавані» не забезпечували такого ж рівня захисту персональних даних в

Сполучених Штатах, як у ЄС відповідно до Директиви, розтлумаченої у світлі Хартії. Зрештою Суд ЄС визнав рішення нечинним[63].

Приклад: у справі «*Digital Rights Ireland*»[64] СЄС вирішував питання сумісності Директиви 2006/24/ЕС (Директива про зберігання даних) із статтями 7 та 8 Хартії. Директива зобов'язувала надавачів електронних комунікаційних послуг зберігати дані про трафік та дані про місцезнаходження від 6 до 24 місяців, а також надавати компетентним органам доступ до цих даних в цілях попередження, розслідування, виявлення серйозних злочинів або притягнення до відповідальності за їх вчинення. Директива не дозволяла зберігати зміст електронних комунікації. СЄС зауважив, що дані, які мали зберігати надавачі послуг відповідно до Директиви, включали дані, необхідні для відстеження та ідентифікації джерела і отримувача комунікації, дати, часу та тривалості комунікації, номера телефону, який здійснював дзвінок, номерів, на які здійснювалися дзвінки, та IP-адреси. Ці дані «загалом могли дозволити сформувати точні висновки щодо приватного життя осіб, чиї дані зберігались, наприклад звички щоденного життя, тимчасове або постійне місця проживання, щоденні або інші переміщення, діяльність, соціальні взаємозв'язки цих осіб та громадські місця, які вони відвідують».

Таким чином, збереження персональних даних на підставі Директиви становило особливо серйозне втручання у право на повагу до приватного життя та право на захист персональних даних. Однак СЄС вирішив, що це втручання не мало негативного впливу на суть цих прав. Щодо права на приватність, його суть не була порушена, оскільки Директива не дозволяла дізнаватись зміст електронних комунікацій. Суть права на захист персональних даних також не була порушена, оскільки Директива вимагала від провайдерів електронних комунікаційних послуг дотримуватися певних принципів захисту персональних даних та безпеки даних, а також запровадити належні технічні та організаційні заходи для досягнення цієї мети.

63 Рішення Суду ЄС про визнання нечинним рішення Комісії 520/2000/ЄС також ґрунтувалося на інших підставах, які будуть розглядатись у наступних розділах цього посібника. Зокрема, Суд ЄС вирішив, що рішення неправомірно обмежувало повноваження органів контролю. На додаток, режим безпечної гавані не передбачав судових засобів захисту для фізичних осіб, якщо вони бажали мати доступ до своїх персональних даних та/або домогтись їх зміни або вилучення. Таким чином, суть основоположного права на ефективний судовий захист, передбачений у статті 47 Хартії, також було порушено.

64 Рішення Суду ЄС, об'єднані справи C-293/12 та C-594/12, «"Digital Rights Ireland Ltd." проти Міністра зв'язку, морських та природних ресурсів та інших та Земельний уряд Каринтії та інші» (*Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*) [ВП], від 08 квітня 2014 р.

Необхідність та пропорційність

Стаття 52 (1) Хартії передбачає, що з урахуванням принципу пропорційності обмеження реалізації основоположних прав та свобод, передбачених Хартією, можуть здійснюватися лише, якщо вони необхідні.

Обмеження може бути **необхідним**, якщо існує потреба у здійсненні заходів в цілях відповідного суспільного інтересу, однак необхідність, як розтлумачив Суд ЄС, також передбачає, що застосовані заходи повинні мати менш серйозний ступінь втручання у порівнянні з іншими можливими заходами, які могли б бути вжиті для досягнення тої самої мети. Щодо обмежень права на повагу до приватного життя та права на захист персональних даних, СЄС застосовує суворий тест перевірки необхідності, встановлюючи, що «відступ від прав або їх обмеження може застосовуватись виключно в тій мірі, в якій це абсолютно необхідно». Якщо обмеження вбачаються суворо необхідними, також має оцінюватися, чи є вони пропорційними.

Пропорційність означає, що переваги від обмеження прав мають переважати шкоду, яке воно спричиняє для реалізації відповідних основоположних прав[65]. Для мінімізації шкоди і ризиків стосовно реалізації права на повагу до приватного життя та права на захист персональних даних важливо, щоб обмеження містили належні запобіжники.

Приклад: у справі *«"Volker und Markus Schecke GbR" та Хартмут Ейферт проти землі Гессен»*[66] СЄС дійшов висновку, що зобов'язавши опубліковувати персональні дані кожної фізичної особи, яка отримала допомогу з сільськогосподарських фондів, без розрізнення за відповідними критеріями, наприклад періодами, коли ці особи отримали таку допомогу, частотою отримання такої допомоги або її характеру та сум, Рада та Комісія вийшли за межі принципу пропорційності.

Таким чином, СЄС вирішив за необхідне визнати певні положення Регламенту Ради (ЕС) № 1290/2005 та в цілому Регламент № 259/2008 нечинними[67].

65 ЄІЗПД (2017), *Посібник з необхідності* , с. 5.

66 Суд ЄС, об'єднані справи, C-92/09 та C-93/09 «"Volker und Markus Schecke GbR" та Хартмут Ейферт проти землі Гессен» (*Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*) [ВП], від 9 листопада 2010 р., п. 89 та 86.

67 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 бенефіціарів, які отримують кошти від Європейського сільськогосподарського гарантійного фонду (EAGF) та Європейського сільськогосподарського фонду розвитку сільських територій (EAFRD), OJ 2008 L 76.

Приклад: у справі «*Digital Rights Ireland*»[68] СЄС визнав, що втручання у право на приватність, яке завдавалось Директивою про збереження даних, не порушило суті цього права, оскільки вона забороняла збереження змісту електронних комунікацій. Однак він вирішив, що Директива не була сумісною зі статтями 7 та 8 Хартії та визнав її нечинною. Оскільки дані про трафік та місце розташування, агреговані та взяті в цілому, можуть бути проаналізовані та можуть представити детальну картину приватного життя фізичних осіб, має місце серйозне втручання у ці права. СЄС взяв до уваги, що Директива вимагала збереження всіх метаданих щодо фіксованих телефонних комунікацій, мобільних комунікацій, доступу до інтернету, інтернет-пошти та інтернет-телефонії, що мало застосовуватися до всіх засобів електронних комунікацій, використання яких широко розповсюджено в щоденному житті людей. Фактично, мало місце втручання, яке зачіпало все населення Європи. Враховуючи обсяг та серйозність втручання, збереження даних трафіку та місця знаходження могло бути виправданим, на думку СЄС, тільки для боротьби з серйозними злочинами. Окрім того, Директива не містила жодних критеріїв, які б могли забезпечити обмеження доступу органів влади до збережених даних виключно у випадку жорсткої необхідності. Більше того, вона не містила субстантивних або процедурних вимог, які б регулювали доступ та використання збережених даних компетентними органами влади, що були можливі без попереднього контролю судом або іншим незалежним органом влади.

Такого ж висновку СЄС дійшов в об'єднаній справі «"*Tele2 Sverige AB" проти Державного управління зв'язку та телекомунікації*» та «*Секретар внутрішніх справ проти Тома Вотсона та інших*»[69].

Ці справи стосувалися збереження даних трафіку та місця знаходження «всіх підписників та зареєстрованих користувачів та всіх засобів електронної комунікації, а також метадані» без «розрізнення, обмеження або

68 Рішення Суду ЄС, об'єднані справи C-293/12 і C-594/12, «"Digital Rights Ireland Ltd." проти Міністра зв'язку, морських та природних ресурсів та інших та Земельний уряд Каринтії та інші» (*Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*), 8 квітня 2014 р. [ВП], 8 April 2014, п. 39.

69 Рішення Суду ЄС, об'єднані справи C-203/15 та C-698/15 «"Tele2 Sverige AB" проти Державного управління зв'язку та телекомунікації» та «Секретар внутрішніх справ проти Тома Вотсона та інших», (*Tele2 Sverige AB v. Post-och telestryrelsen and Secretary of State for the Home Department v. Tom Watson and Others*) [ВП], від 21 грудня 2016 р., пп. 105–106.

винятків відповідно до цілі, яка переслідується»[70]. У цих випадках збереження даних осіб не обумовлювалось їхнім зв'язком (прямим чи непрямим) з серйозними кримінальними правопорушеннями або зв'язком із національною безпекою. З огляду на відсутність будь-якого зв'язку між збереженими даними та загрозою громадській безпеці чи обмеженнями щодо періоду або території, СЄС дійшов висновку, що національне законодавство вийшло за межі того, що може вважатися суворо необхідним для цілей боротьби з серйозними злочинами[71].

Такий же підхід було застосовано Європейським інспектором із захисту персональних даних у «*Посібнику з питань необхідності*»[72]. Посібник було розроблено з метою надання допомоги в аналізі відповідності запропонованих заходів праву ЄС щодо захисту персональних даних. Він був написаний, щоб надати інструменти політикам та законодавцям ЄС, відповідальним за підготовку проєктів та контроль за заходами, що включають обробку персональних даних і обмежують право на захист персональних даних та інші права і свободи, передбачені Хартією.

Цілі загального інтересу

Для того щоб бути виправданими, будь-які обмеження реалізації прав, гарантованих Хартією, також мають дійсно відповідати цілям загального інтересу, визнаного Європейським Союзом, або потребі захистити права і свободи інших осіб. Щодо необхідності захистити права і свободи інших осіб необхідно пам'ятати, що право на захист персональних даних часто взаємодіє з іншими основоположними правами. Розділ 1.3 надає детальний аналіз щодо такої взаємодії. Щодо цілей загального інтересу, вони включають загальні цілі ЄС, які проголошено в статті 3 Договору про Європейський Союз (ДЄС), як-от сприяння миру та добробуту своїх народів, соціальна справедливість та захист, встановлення території свободи, безпеки та справедливості, в якій гарантується вільне переміщення осіб, у поєднанні з належними заходами з попередження та боротьби зі злочинністю, а також інші цілі та інтереси, захищені спеціальними положеннями договорів[73]. Загальний регламент захисту персональних даних у цьому аспекті уточнив статтю 52 (1) Хартії: стаття

70 Там само, п. 105.

71 Там само, п. 107.

72 ЄІЗПД (2017), Посібник з необхідності (*Necessity Toolkit*), Брюссель, 11 квітня 2017 р.

73 Коментар до Хартії основних прав (2007/C 303/02), OJ 2007, № C 303, с. 17–35.

23 (1) регламенту перелічує низку цілей загального інтересу, які вважаються легітимними для обмеження прав осіб, за умови, що обмеження зберігає дотримання суті права на захист персональних даних, є необхідним та пропорційним. Перераховані суспільні інтереси, які там зазначені, включають: національну безпеку та захист, попередження злочинів, захист важливих економічних та фінансових інтересів ЄС або держав-членів, охорону здоров'я та соціальний захист.

Важливо визначити та належним чином пояснити мету загального суспільного інтересу, яку переслідує обмеження, оскільки оцінка необхідності здійснюється з урахуванням цього пояснення. Чіткий, деталізований опис мети обмеження та запропонованих заходів є важливим для оцінки необхідності цього заходу[74]. Ціль, яку переслідують, необхідність та пропорційність обмеження тісно пов'язані.

Приклад: справа «*Шварц проти міста Бохума*»[75] стосувалася обмеження права на повагу до приватного життя та права на захист персональних даних, яке полягало у відібранні та збереженні відбитків пальців при видачі паспорта органами влади[76]. Заявник звернувся до органу влади міста Бохума по паспорт, однак відмовився надати відбитки пальців, після чого місцева влада відмовила у видачі паспорта. Він звернувся до суду Німеччини з позовом про зобов'язання видати йому паспорт без відбитків пальців. Суд звернувся до СЄС із запитом, у якому порушував питання законності статті 1 (2) Регламенту 2252/2004 щодо стандартів засобів захисту біометричних даних у паспортах та проїзних документах держав-членів.

СЄС зазначив, що відбитки пальців є **персональними даними,** оскільки вони об'єктивно містять унікальну інформацію про фізичну особу, яка дозволяє точно її ідентифікувати, при цьому відібрання та збереження відбитків є обробкою персональних даних. Така, врегульована статтею 1(2) Регламенту № 2252/2004, обробка даних становить загрозу для права на приватне життя та права на захист персональних даних[77]. Водночас стаття 52 (1) Хартії дозволяє обмеження реалізації цих прав, якщо вони встановлені законом, забезпечують дотримання суті цих прав, є пропорційними та необхідними,

74 ЄІЗПД (2017), *Посібник з необхідності* , Брюссель, 11 квітня 2017 р., с. 4.

75 Рішення Суду ЄС, C-291/12, «Міхаель Шварц проти міста Бохума» (*Michael Schwarz v. Stadt Bochum*), від 17 жовтня 2013 р.

76 Там само, пп. 33–36.

77 Там само, пп. 27–30.

а також дійсно відповідають цілям загального інтересу, визнаного ЄС, або необхідні для захисту прав і свобод інших осіб.

У цій справі Суд ЄС зазначив, що, по-перше, обмеження, яке полягає у відібранні та збереженні відбитків пальців при видачі паспорту, **передбачене законом**, оскільки ці операції передбачені статтею 1 (2) Регламенту № 2252/2004. По-друге, цей Регламент був розроблений з метою попередження підробки паспортів та їх шахрайського використання. Відповідно, Регламент має на меті, серед іншого, попередження незаконного в'їзду на територію ЄС та, відповідно, переслідує мету загального інтересу, визнаного Союзом. По-третє, з доказів, наданих ЄС, не вбачалося, що обмеження цих прав порушувало їхню суть. Цього також не стверджували сторони. По-четверте, зберігання відбитків пальців на засобі з високим ступенем безпеки, як передбачено Регламентом, вимагає сучасних розвинутих технологій. Таке збереження зменшувало ризик підроблення паспортів та сприяло роботі органів влади, відповідальних за перевірку справжності паспортів на кордонах ЄС. Той факт, що такий метод не є цілком надійним, не є вирішальним. Хоча такий метод не унеможливлює в'їзду всіх недозволених осіб, достатньо того, що він значно зменшує ризик такого в'їзду. У світлі вказаного, СЄС визнав, що відібрання та збереження відбитків пальців відповідно до статті 1 (2) Регламенту № 2252/2004 були відповідними для досягнення цілей Регламенту цього положення та, в більш широкому сенсі, цілі попередження незаконного в'їзду на територію ЄС[78].

Далі СЄС проаналізував, чи є така обробка **необхідною,** зазначаючи, що дія, яка розглядається, включає відібрання відбитків тільки двох пальців, які загалом може бачити будь-хто, що означає, що ця процедура не носить інтимний характер. Ця процедура не спричиняє відповідній особі будь-якого особливого фізичного чи психологічного дискомфорту, не більше, ніж процедура фотографування особи. Також необхідно враховувати, що під час провадження СЄС єдиною альтернативою відібранню відбитків пальців було сканування сітківки ока. Нічого з наданих матеріалів СЄС не вказувало, що ця процедура має менший ступінь втручання в права, гарантовані статтями 7 та 8 Хартії, ніж відібрання відбитків пальців. Більше того, на час провадження СЄС було загальновизнаним, що технологія розпізнання сітківки ока не була такою ж розвинутою, як технологія розпізнання відбитків пальців, вона є дорожчою у порівнянні з

78 Там само, пп. 35–45.

технологією розпізнання відбитків пальців і в зв'язку з цим менш зручною для загального використання. Відповідно, суду не надали інформацію про існування будь-якого заходу, який би був таким саме ефективним для досягнення мети захисту від використання підроблених паспортів та мав би меншу загрозу для прав, передбачених статтями 7 і 8 Хартії, у порівнянні із заходами, пов'язаними з методом використання відбитків пальців[79].

СЄС зазначив, що стаття 4 (3) Регламенту № 2252/2004 чітко встановлює, що відбитки пальців можуть використовуватися для перевірки дійсності паспорта та ідентифікації його власника. При цьому стаття 1 (2) даного регламенту не передбачає збереження відбитків пальців, крім як в самому паспорті, який належить тільки його власнику. Відповідно, Регламент не передбачає юридичної підстави для централізованого збереження даних, які відбираються відповідно до нього, або для використання даних в інших цілях, ніж попередження незаконного в'їзду на територію ЄС[80]. З огляду на вказані міркування СЄС дійшов висновку, що аналіз переданого питання не виявив жодних підстав, які могли б призвести до визнання статті 1 (2) Регламенту № 2252/2004 нечинною.

Взаємозв'язок Хартії та ЄКПЛ

Незважаючи на використання різних формулювань, умови правомірного обмеження прав, передбачені статтею 52 (1) Хартії, нагадують ті, що передбачені статтею 8 (2) ЄКПЛ щодо права на повагу до приватного життя. У своїй практиці СЄС та ЄСПЛ часто посилаються на рішення одне одного, це частина діалогу між двома судами з метою пошуку гармонізованого тлумачення правил захисту персональних даних. Стаття 52 (3) Хартії передбачає, «що в тій мірі, в якій Хартія передбачає права, які кореспондують правам, гарантованим Конвенцією про захист прав людини і основоположних свобод, значення та обсяг цих прав є такими самими, як це передбачено Конвенцією». Втім, стаття 8 Хартії не є прямо відповідною статті ЄКПЛ[81]. Стаття 52 (3) Хартії стосується змісту та обсягу прав, захищених кожною правовою системою, а не умов їх обмеження. Водночас, враховуючи ширший контекст діалогу та взаємодії двох судів, СЄС може у своєму аналізі взяти до уваги критерії правомірності

79 Рішення Суду ЄС, C-291/12, «Міхаель Шварц проти міста Бохума» (*Michael Schwarz v. Stadt Bochum*), від 17 жовтня 2013 р., пп. 46–53.

80 Там само, пп. 56–61.

81 ЄІЗПД (2017), *Посібник з необхідності*, Брюссель, від 11 квітня 2017 р., с. 6.

обмеження за статтею 8 ЄКПЛ у тлумаченні ЄСПЛ. Зворотний сценарій, за яким ЄСПЛ може посилатися на умови правомірного обмеження, передбачені Хартією, також можливий. У будь-якому разі, також необхідно враховувати, що в ЄКПЛ відсутній ідеальний еквівалент статті 8 Хартії, яка посилається на захист персональних даних, а саме права суб'єкта персональних даних, правомірні підстави для обробки та контроль незалежного органу. Деякі елементи статті 8 Хартії можна відшукати в практиці ЄСПЛ стосовно статті 8 ЄКПЛ та Конвенції 108[82]. Цей зв'язок забезпечує існування взаємного впливу між СЄС та ЄСПЛ у питаннях, що пов'язані із захистом персональних даних.

1.3 Взаємозв'язок з іншими правами та правомірними інтересами

Ключові моменти

- Право на захист даних часто взаємопов'язане з іншими правами, як-от свобода вираження поглядів та право отримувати і передавати інформацію.
- Цей взаємозв'язок є подвійним: існують ситуації, коли право на захист персональних даних є в конфронтації з певним іншим правом, але водночас існують ситуації, коли право на захист персональних даних ефективно забезпечує повагу до того ж іншого права. Наприклад, це так щодо права на свободу вираження поглядів, враховуючи, що професійна таємниця є елементом права на повагу до приватного життя.
- Потреба захисту прав та свобод інших осіб є одним із критеріїв аналізу правомірності обмеження права на захист персональних даних.
- Якщо на кону стоять різні права, суди мають збалансувати їх, використовуючи відповідні тести.
- Загальний регламент захисту персональних даних вимагає, щоб держави-члени узгоджували право на захист персональних даних зі свободою вираження поглядів та свободою інформації.
- Держави-члени також повинні прийняти ухвалити спеціальні норми в національному законодавстві для узгодження права на захист персональних даних з доступом громадськості до офіційних документів та зобов'язаннями збереження професійної таємниці.

82 Коментар до Хартії основних прав (*2007/C 303/02*), стаття 8.

Право на захист персональних даних не є абсолютним правом; умови правомірного обмеження цього права детально описуються вище. Один з критеріїв для правомірного обмеження прав, визнаний правом РЄ та ЄС, є необхідність втручання у право на захист персональних даних для захисту прав і свобод інших осіб. Застосовуючи та надаючи тлумачення статті 8 ЄКПЛ та статті 8 Хартії, як ЄСПЛ, так і СЄС неодноразово наголошували на необхідності застосування балансувального тесту в разі, якщо право на захист персональних даних взаємодіє з іншими правами[83]. Декілька важливих прикладів продемонструють, як досягається такий баланс.

На додаток до балансувального тесту, що здійснюють суди, держави повинні, де це необхідно, ухвалити законодавство, яке б узгоджувало право на захист персональних даних з іншими правами. З огляду на це Загальний регламент захисту персональних даних передбачає певні сфери, у яких держави можуть відступати від правил.

Щодо свободи вираження поглядів, ЗРЗПД вимагає від держав-членів узгодити на рівні національного законодавства «право на захист персональних даних відповідно до цього Регламенту з правом на свободу вираження поглядів та свободу інформації, включаючи обробку даних з журналістськими цілями або цілями наукової, творчої або літературної діяльності»[84]. Держави-члени можуть також ухвалити закони для узгодження права на захист персональних даних з правом на доступ до офіційних документів та зобов'язаннями зберігати професійну таємницю, що захищається як форма права на повагу до приватного життя[85].

1.3.1 Свобода вираження поглядів

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

83 Рішення ЄСПЛ у справі «Фон Ганновер проти Німеччини» (*Von Hannover v. Germany*) (№ 2) [ВП], №№ 40660/08 та 60641/08 від 7 лютого 2012 р.; Рішення Суду ЄС, 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*) від 24 листопада 2011 р., п. 48; Суд ЄС, C-275/06, «Музичні продюсери Іспанії (Promusicae) проти "Telefonica de Espana SAU"» (*Productores de Música de España (Promusicae) v. Telefónica de España SAU*) від 29 січня 2008р., [ВП], п. 68.

84 Загальний регламент захисту персональних даних, стаття 85.

85 Там само, статті 86 та 90.

Право на свободу вираження поглядів закріплене у статті 11 Хартії («Свобода вираження поглядів та свобода інформації»). Це право включає «свободу дотримуватися своїх поглядів, отримувати і розповсюджувати інформацію та ідеї без втручання органів державної влади та незалежно від державних кордонів». Свобода інформації, відповідно до статті 11 Хартії та статті 10 ЄКПЛ, захищає не тільки право надавати інформацію, але й також право *отримувати* інформацію.

Обмеження свободи вираження поглядів має відповідати умовам, визначеним у статті 52 (1) Хартії, які описані вище. Крім того, стаття 11 кореспондується із статтею 10 ЄКПЛ. Стаття 52 (3) Хартії передбачає, «що в тій мірі, в якій Хартія передбачає права, які кореспондують правам, гарантованим Конвенцією про захист прав людини і основоположних свобод, значення та обсяг цих прав є таким, як передбачає ця Конвенція». Таким чином, обмеження, які можуть правомірно накладатись на права, передбачені статтею 11 Хартії, не мають бути більшими за обсягом, ніж ті, що передбачені статтею 10 (2) ЄКПЛ, іншими словами, вони мають бути передбачені законом та бути необхідними в демократичному суспільстві «для захисту [...] репутації чи прав інших осіб». Такі права включають право на повагу до приватного життя та право на захист персональних даних.

Взаємостосунки між правом на захист персональних даних та правом на свободу вираження поглядів регулюються статтею 85 Загального регламенту захисту персональних даних під назвою «Обробка та свобода вираження поглядів і свобода інформації». Відповідно до цієї статті держави-члени мають узгоджувати право на захист персональних даних з правом на свободу вираження поглядів та свободу інформації. Зокрема, можуть існувати винятки та відступи від певних розділів Загального регламенту захисту персональних даних для цілей журналістської діяльності або наукової, художньої чи літературної діяльності в тій мірі, яка необхідна для узгодження права на захист персональних даних із свободою вираження поглядів та свободою інформації.

Приклад: у справі «*Уповноважений із захисту персональних даних Фінляндії проти "Satakunnan Markkinapörssi Oy" і "Satamedia Oy"*»[86] СЄС повинен був визначити взаємозв'язок між захистом даних та

86 Рішення Суду ЄС у справі C-73/07 «Уповноважений із захисту персональних даних Фінляндії проти "Satakunnan Markkinapörssi Oy" і "Satamedia Oy"», (*Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*) [ВП], від 16 грудня 2008 р., пп. 56, 61 та 62.

свободою преси[87]. Суд мав розглянути питання про поширення підприємством через послугу СМС інформації про податки 1,2 млн фізичних осіб, законно отриманої від фінських податкових органів. Фінський орган з контролю за дотриманням права на захист персональних даних виніс рішення, яким зобов'язав підприємство зупинити поширення цих даних. Підприємство оскаржило це рішення в національному суді, який звернувся до Суду ЄС із запитом щодо тлумачення Директиви про захист персональних даних. Зокрема, СЄС мав перевірити, чи можна вважати обробку персональних даних, які були надані податковими органами користувачам мобільних телефонів для можливості отримувати податкові дані інших фізичних осіб, діяльністю, що здійснюється виключно з журналістськими цілями. Після висновку про те, що діяльність підприємства становила «обробку персональних даних» у сенсі статті 3 (1) Директиви про захист персональних даних, СЄС здійснив аналіз статті 9 Директиви (про обробку персональних даних та свободу вираження поглядів). По-перше, він наголосив на важливості права на свободу вираження поглядів в кожному демократичному суспільстві та вирішив, що поняття, які пов'язані з цією свободою, як, наприклад, журналістика, мають тлумачитися розширено. Далі він зазначив, що для досягнення балансу між двома основоположними правами відступи від права на захист персональних даних або винятки повинні застосовуватись виключно в тій мірі, в якій це суворо необхідно. За цих обставин СЄС вирішив, що така діяльність підприємства щодо даних з документів, які були в публічному доступі відповідно до національного законодавства, може вважатися «журналістською діяльністю», якщо вона має на меті відкрити публіці інформацію, погляди або ідеї, незалежно від засобу їх передачі. Він також вирішив, що така діяльність може здійснюватися не лише засобами масової інформації, але і з метою отримання прибутку.

Та сама справа була розглянута й ЄСПЛ після того, як національний суд, спираючись на роз'яснення СЄС, прийняв рішення про виправданість втручання у право підприємства на свободу вираження поглядів, що мало місце в зв'язку з рішенням органу контролю про припинення

87 Справа стосувалася тлумачення Директиви про захист персональних даних, статті 9 – тепер заміненої статтею 85 Загального регламенту захисту персональних даних, яка передбачає: "Держави-сторони повинні передбачити винятки або відступи від положень цього Розділу, Розділу IV та Розділу VI для обробки персональних даних, що здійснюється виключно для цілей художнього та літературного вираження поглядів, тільки якщо це необхідно для узгодження права на приватність з правилами регулювання свободи вираження поглядів".

оприлюднення всієї податкової інформації. ЄСПЛ підтримав цей підхід[88]. Він вирішив, що хоча право підприємства на передання інформації зазнало втручання, воно було здійснено згідно із законом, переслідувало легітимну мету та було необхідним у демократичному суспільстві.

ЄСПЛ нагадав критерії своєї практики, якими мають керуватися національні органи та сам Суд при пошуку балансу між свободою вираження поглядів з правом на повагу до приватного життя. Якщо на кону стоять політичні висловлювання або дебати з питання суспільного інтересу, існує дуже невеликий простір для обмеження права на отримання та передання інформації, оскільки громадськість має право бути поінформованою, і «це є важливим правом в демократичному суспільстві»[89]. Однак статті, які мають на меті виключно задовольнити цікавість читачів щодо деталей приватного життя людини, не можуть вважатися внеском у дискусію суспільного інтересу. Відступ від правил захисту персональних даних в цілях здійснення журналістської діяльності має на меті дозволити журналістам мати доступ до даних, збирати їх та обробляти для здійснення ними своєї журналістської діяльності. Таким чином, дійсно існував суспільний інтерес у наданні доступу та можливості підприємствам заявника збирати та обробляти великі обсяги податкових даних, про які йшла мова. З іншого боку, Суд вирішив, що відсутній суспільний інтерес в такому масовому розповсюдженні газетами необроблених даних у незмінній формі та без будь-якого аналітичного внеску. Така інформація про податки може надати можливість допитливим членам суспільства категоризувати фізичних осіб відповідно до їхнього економічного статусу та задовольнити цікавість публіки до приватного життя інших осіб. Це не може розглядатися як сприяння обговоренню, що відповідає суспільним інтересам.

Приклад: у справі «*Google Spain*»[90] СЄС розглянув питання, чи був зобов'язаний «Google» видалити неактуальну інформацію про фінансові труднощі заявника зі списку результатів пошуку. При пошуку за допомогою системи Google з використанням імені заявника результати пошуку надавали посилання на старі газетні статті, у яких йшлося про його справу про

88 Рішення ЄСПЛ у справі «"Satakunnan Markkinapörssi Oy" та "Satamedia Oy" проти Фінляндії» (*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*), № 931/13, від 27 червня 2017 р.

89 Там само, п. 169.

90 Рішення Суду ЄС, C-131/12 «"Google Spain SL", "Google Inc." проти Іспанського агентства захисту даних (AEPD) та Маріо Костеха Гонсалеса» (*Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*), [ВП], від 13 травня 2014 р., пп. 81–83.

банкрутство. Заявник вважав, що це становило порушення його права на повагу до приватного життя та права на захист персональних даних, оскільки провадження з банкрутства було закінчено багато років тому, що робить посилання невідповідними.

СЄС роз'яснив, що пошукова система інтернету та результати пошуку з наданням персональних даних може створювати детальний профіль особи. У світлі зростання цифровізації суспільства вимога щодо точності персональних даних та їх публікації не більше, ніж це необхідно, тобто для надання інформації громадськості, є засадничою для забезпечення високого рівня захисту даних фізичних осіб. «Щодо такої обробки контролер, у межах своєї відповідальності, повноважень та спроможності, має забезпечити, щоб вона відповідала цим вимогам» права ЄС для того, щоб встановлені юридичні гарантії були повною мірою ефективними. Це означає, що право на видалення персональних даних, коли їх обробка вже не є необхідною або актуальною, також поширюється на пошукові системи, які були визнані контролерами, а не просто операторами (див. *розділ 2.3.1.*).

Розглядаючи питання, чи мав «Google» прибрати посилання, пов'язані із заявником, СЄС вирішив, що за певних обставин фізичні особи мають право на видалення своїх персональних даних з переліку результатів пошукових систем інтернету. Це право виникає, коли інформація стосовно особи є неточною, неадекватною, невідповідною або надмірною щодо цілей обробки даних. СЄС визнав, що це право не є абсолютним; його необхідно збалансувати з іншими правами, зокрема, інтересом та правом широкої публіки мати доступ до інформації. Кожний запит на видалення даних потребує оцінки з урахуванням індивідуальних обставин для встановлення балансу між основоположним правом на захист персональних даних та правом на повагу до приватного життя суб'єкта персональних даних та правомірним інтересом всіх користувачів інтернету. СЄС роз'яснив критерії, які необхідно брати до уваги під час балансування. Характер інформації, яка розглядається, є особливо важливим фактором. Якщо інформація є чутливою щодо приватного життя фізичної особи і відсутній особливий суспільний інтерес до її доступності, захист даних та приватність буде переважати над правом громадськості мати доступ до неї. І навпаки, якщо виявляється, що суб'єкт персональних даних є публічною особою, або що характер інформації виправдовує надання доступу до неї широкому загалу, тоді втручання в основоположне право на захист персональних даних та приватне життя є виправданим.

Після цього рішення Робоча група «Стаття 29» розробила рекомендації щодо виконання рішення СЄС. Цей документ містить перелік спільних критеріїв, які має використовувати орган контролю при розгляді скарг щодо вимог фізичних осіб на вилучення їхніх даних та при знаходженні балансу між цими правами[91].

Щодо узгодження права на захист персональних даних з правом на свободу вираження поглядів, ЄСПЛ прийняв декілька вагомих рішень.

Приклад: у справі «*"Axel Springer AG" проти Німеччини*»[92] ЄСПЛ визнав, що запобіжний захід, який заборонив підприємству-заявнику опублікувати статтю про арешт та засудження відомого актора, становив порушення статті 10 ЄКПЛ. ЄСПЛ нагадав про визначені у своїх рішеннях критерії балансу між правом на свободу вираження поглядів та правом на повагу до приватного життя:

- чи викликає подія, про яку опубліковано інформацію у статті, суспільний інтерес;
- чи є особа, щодо якої йдеться, публічною особою;
- як інформація була отримана, та чи є вона надійною;

ЄСПЛ визнав, що арешт актора та його засудження були публічними судовими фактами і, відповідно, викликали суспільний інтерес; актор був достатньо відомим для визнання його публічною особою; та що інформація була надана прокуратурою і її точність не оскаржувалась сторонами. Таким чином, обмеження щодо публікації, накладене на компанію-заявника, не було обґрунтовано пропорційним відносно легітимної мети захисту приватного життя. Суд дійшов висновку, що статтю 10 ЄКПЛ було порушено.

Приклад: справа «*"Coudec and Hachette Filipacchi Associés" проти Франції*»[93] стосувалася публікації інтерв'ю пані Косте в тижневому

91 Посібник Робочої групи «Стаття 29» (2014) про виконання рішення Суду ЄС «ТОВ "Google Spain", компанія "Google Inc." проти Іспанського агентства захисту даних та Маріо Костеха Гонсалеса» C-131/12 (*Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González")* , РГ 225, Брюссель, від 26 листопада 2014 р.

92 Рішення ЄСПЛ у справі «"Axel Springer AG" проти Німеччини» (*Axel Springer AG v. Germany)* [ВП], № 39954/08, від 7 лютого 2012 р., пп. 90 та 91.

93 Рішення ЄСПЛ у справі «*"Coudec and Hachette Filipacchi Associés" проти Франції*» (*Coudec and Hachette Filipacchi Associés v. France)* [ВП], № 40454/07, від 10 листопада 2015 р.

журналі. Вона стверджувала, що принц Монако Альбер був батьком її сина. В інтерв'ю йшлося про відносини пані Косте та принца, яким чином він відреагував на народження дитини. Інтерв'ю також супроводжувалося фотографією принца з дитиною. Принц Альбер звернувся до суду проти компанії-видавця щодо порушення його права на повагу до приватного життя. Французькі суди вирішили, що стаття завдала невиправної шкоди принцу Альберу та зобов'язала видавця сплатити відшкодування та опублікувати судове рішення на обкладинці журналу.

Видавці журналу звернулися до ЄСПЛ, стверджуючи, що рішення французьких судів становило невиправдане втручання у право на повагу до свободи вираження поглядів. ЄСПЛ мав збалансувати право принца Альбера на повагу до приватного життя з правом видавництва на свободу вираження поглядів і загальне право суспільства мати інформацію. Право пані Косте поділитися своєю історією та інтерес дитини в офіційному встановленні зв'язку з батьком також були важливими факторами.

ЄСПЛ визнав, що публікація інтерв'ю становила втручання у право принца на повагу до приватного життя, та розглянув, чи було таке втручання необхідним. Він дійшов висновку, що публікація стосувалася публічної особи та питання суспільного інтересу, оскільки громадяни Монако зацікавлені в тому, щоб знати про існування дитини принца, оскільки майбутнє спадкової монархії «невід'ємно пов'язане з існуванням нащадків» і, відповідно, це питання суспільного інтересу[94]. Суд також зазначив, що стаття дозволила пані Косте та її дитині реалізувати своє право на свободу вираження поглядів. Національні суди не здійснили належний розгляд принципів та критеріїв, які були розроблені в практиці ЄСПЛ, для збалансування права на повагу до приватного життя з правом на свободу вираження поглядів. Суд дійшов висновку, що Франція порушила статтю 10 ЄКПЛ щодо права на свободу вираження поглядів.

Чи сприяють висловлені погляди обговоренню суспільно важливих питань є одним із ключових критеріїв в практиці ЄСПЛ щодо пошуку балансу між цими правами.

94 Там само, пп. 104–116.

Приклад: у справі «*Мослі проти Сполученого Королівства*»[95] національна щотижнева газета надрукувала інтимні фотографії заявника, відомої особи. Заявник звернувся до судів з цивільним позовом, який був задоволений, заявнику було присуджено відшкодування шкоди. Незважаючи на присуджену грошову компенсацію, заявник стверджував, що він залишається жертвою порушення права на повагу до приватного життя, бо у нього не було можливості вимагати заборони публікації фото, оскільки газета не була юридично зобов'язана повідомляти про публікацію завчасно.

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 має приватний та інтимний характер, а також не викликає суспільного інтересу при її поширенні. Проте особливу обережність слід виявляти під час розгляду обмежень, які можуть набирати форми цензури перед здійсненням публікації. Що стосується ефекту стримування, до якого могла б призвести вимога попереднього повідомлення про публікацію, маючи сумніви щодо його ефективності та широку свободу розсуду в цій сфері, ЄСПЛ дійшов висновку, що існування юридично обов'язкової вимоги щодо попереднього повідомлення не вимагається статтею 8. Відповідно, Суд дійшов висновку, що не було порушено статтю 8.

Приклад: у справі «*Болен проти Німеччини*»[96] заявник, відомий співак та продюсер, опублікував автобіографічну збірку та в подальшому був зобов'язаний вилучити деякі частини за рішеннями суду. Історія набула широкого розголосу в національних засобах масової інформації, компанія з виробництва тютюну розробила гумористичну рекламну компанію, посилаючись на цю подію та використовуючи ім'я заявника без його згоди. Заявник вимагав присудження йому відшкодування шкоди, завданої рекламною компанією, стверджуючи про порушення його прав, гарантованих статтею 8 ЄКПЛ. ЄСПЛ повторив критерії встановлення балансу між правом на повагу до приватного життя та правом на свободу вираження поглядів та встановив, що порушення статті 8 не було. Заявник був публічною особою, реклама не посилалася на деталі його приватного

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

96 Рішення ЄСПЛ у справі «*Болен проти Німеччини*» (*Bohlen v. Germany*), № 53495/09, від 19 лютого 2015 р., пп. 45–60.

життя, вона використовувала публічну подію, про яку вже повідомляли засоби масової інформації та яка була частиною суспільної дискусії. Крім того, реклама мала гумористичний характер і не містила нічого негативного або принизливого про заявника.

Приклад: у справі «*Бірюк проти Литви*»[97] заявниця в заяві до ЄСПЛ стверджувала, що Литва не виконала своїх зобов'язань щодо забезпечення її права на повагу до приватного життя, оскільки незважаючи на серйозне порушення її приватності, яке було вчинено провідною газетою, національні суди присудили їй лише символічну суму відшкодування. Присуджуючи відшкодування моральної шкоди, національні суди застосували національний закон про поширення інформації, який встановлював дуже низький граничний рівень відшкодування моральної шкоди, завданої засобами масової інформації поширенням інформації про приватне життя особи. Справа стосувалася публікації на перших шпальтах найбільшої литовської газети інформації про те, що заявниця була ВІЛ-позитивною. Стаття також критикувала поведінку заявниці та піддавала сумніву її моральні засади.

ЄСПЛ повторив, що захист персональних даних, особливо медичних даних, має фундаментальну важливість для права на повагу до приватного життя відповідно до ЄКПЛ. Конфіденційність даних про стан здоров'я особливо важлива, оскільки відкриття медичних даних (про ВІЛ-статус у справі заявниці) може катастрофічно вплинути на приватне та сімейне життя особи, її працевлаштування та стан в суспільстві. Суд особливо відзначив, що відповідно до опублікованої інформації в газеті медичні працівники надали інформацію про ВІЛ-статус заявниці, допустивши очевидне порушення лікарської таємниці. Відповідно, мало місце неправомірне втручання у право заявниці на повагу до приватного життя.

Стаття була опублікована газетою – свобода вираження поглядів також є основоположним правом відповідно до ЄКПЛ. Однак, оцінивши, чи виправдовував наявний суспільний інтерес публікацію такого роду про заявницю, Суд вирішив, що головною метою публікації було збільшення продажу газети через задоволення цікавості читачів. Така мета не могла вважатись метою сприяння будь-якому обговоренню питань суспільного інтересу. Оскільки в даному випадку мова йшла про «надмірне

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

зловживання свободою засобів масової інформації», жорсткі обмеження щодо відшкодування шкоди та невелика сума відшкодування моральної шкоди, як було передбачено національним законодавством, призвели до порушення Литвою її позитивних зобов'язань забезпечити захист права заявниці на повагу до приватного життя. ЄСПЛ вирішив, що мало місце порушення статті 8 ЄКПЛ.

Право на свободу вираження поглядів та право на захист персональних даних не завжди перебувають у конфлікті. Існують випадки, коли ефективний захист персональних даних гарантує право на свободу вираження поглядів.

Приклад: у справі «*Tele2 Sverige*» Суд ЄС вирішив, що втручання у права за статтями 7 та 8 Хартії, спричинене Директивою 2006/24 (Директива про зберігання даних) було «всеосяжним і має вважатись особливо серйозним. Більше того, ... той факт, що дані зберігались і в подальшому використовувалися без повідомлення підписників або зареєстрованих користувачів, міг сформувати в зацікавлених осіб відчуття, що їхнє приватне життя перебуває під постійним спостереженням». СЄС також вказав, що загальне збереження даних про трафік та місцезнаходження могло вплинути на використання електронних комунікацій та «як наслідок, на реалізацію користувачами їхнього права на свободу вираження поглядів, гарантованого статтею 11 Хартії»[98]. У такому разі, вимагаючи суворих гарантій щодо неможливості збереження даних у такий загальний спосіб, правила захисту персональних даних, безперечно, сприяють реалізації свободи вираження поглядів.

Щодо права на отримання інформації, яке також є частиною права на свободу вираження поглядів, усвідомлення важливості прозорості в діяльності державних органів для функціонування демократичного суспільства постійно зростає. Прозорість є ціллю загального інтересу, яка може виправдати втручання у право на захист персональних даних, якщо воно є необхідним

98 Рішення Суду ЄС, об'єднані справи C-203/15 та C-698/15 «"Tele2 Sverige AB" проти Державного управління зв'язку та телекомунікації» та «Секретар внутрішніх справ проти Тома Вотсона та інших», (*Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others*) [ВП], від 21 грудня 2016 р., пп. 37–101; Рішення Суду ЄС, об'єднані справи C-293/12 та C-594/12, «"Digital Rights Ireland Ltd." проти Міністра зв'язку, морських та природних ресурсів та інших та Земельний уряд Каринтії та інші» (*Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [ВП]), від 08 квітня 2014 р., п. 28.

та пропорційним, як це пояснено в розділі 1.2. 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 живе 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)[99].

У праві ЄС право на доступ до документів гарантується Регламентом 1049/2001 щодо доступу громадськості до документів Європейського Парламенту, Ради та документів Комісії (Регламент щодо доступу до документів)[100]. Положеннями статті 42 Хартії та статті 15 (3) ДфЄС дію цього права було поширено на доступ «до документів інститутів, органів, служб та агентств ЄС, незалежно від їхньої форми».

Це право може вступати в конфлікт з правом на захист персональних даних, якщо у результаті доступу до документа буде розкрито персональні дані інших осіб. Стаття 86 Загального регламенту захисту персональних даних чітко передбачає, що персональні дані, які містяться в офіційних документах органів влади та установ, можуть відкриватись органом або установою у відповідності до закону Союзу[101] або держави-члена для узгодження права громадян на доступ до офіційних документів та права на захист персональних даних, прийнятого відповідно до цього регламенту.

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 «*“Volker und Markus Schecke GbR” та Хартмут Ейферт проти землі Гессен*»[102] Суд ЄС повинен був вирішити питання

99 Рада Європи, Комітет міністрів (2002), Рекомендація R (81) 19 та Рекомендація Rec(2002)2 державам-членам про доступ до офіційних документів, від 21 лютого 2002 р.; Рада Європи, Конвенція про доступ до офіційних документів, CETS № 205, від 18 червня 2009 р. Конвенція наразі не набула чинності.

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

101 Стаття 42 Хартії, стаття 15 (3) ДфЄС та Регламент 1049/2009.

102 Суд ЄС, об’єднані справи, C-92/09 та C-93/09 «Товариство цивільного права “Фолькер і Маркус Шеке” і Гартмут Айферт проти землі Гессен» (*Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*) [ВП], від 9 листопада 2010 р., пп. 47–52, 58, 66–67, 75, 86 та 92.

пропорційності оприлюднення інформації (вимога права ЄС), про імена отримувачів сільськогосподарських субсидій ЄС і отримані ними кошти. Оприлюднення мало на меті посилити прозорість та сприяти громадському контролю за належним використанням коштів адміністрації. Декілька отримувачів оскаржили пропорційність такого оприлюднення.

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

Суд вважає, що таке втручання в гарантовані статтями 7 та 8 Хартії права передбачене 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. Він визнав, що в демократичному суспільстві важливо інформувати платників податків про використання публічних коштів. Однак, оскільки «неможливо стверджувати про пріоритетність цілі забезпечення прозорості над правом на захист персональних даних»[103], інституції ЄС були зобов'язані збалансувати інтерес ЄС у прозорості та обмеження реалізації права на приватність і права на захист персональних даних, яких зазнали отримувачі коштів внаслідок оприлюднення.

СЄС вирішив, що інституції ЄС не здійснили належного балансування, оскільки було можливо передбачити заходи з меншим негативним впливом на основоположні права осіб і водночас сприяти прозорості, заради якої було оприлюднено дані. Наприклад, замість загального оприлюднення, яке впливало на всіх отримувачів, вказавши їх поіменно та отримані кожним з них точні суми, можна було розрізнити їх за певними критеріями, як-от періоди, протягом яких ці особи отримали допомогу, частота отримання або її сума чи характер[104]. Таким чином, Суд визнав

103 Там само, п. 85.

104 Там само, п. 89.

законодавство ЄС щодо оприлюднення інформації про отримувачів європейських сільськогосподарських фондів частково необґрунтованим.

Приклад: у справі «*Рахункова палата проти австрійської телерадіокомпанії "Österreichischer Rundfunk" та інших*»[105] Суд ЄС розглянув відповідність певного законодавства Австрії вимогам законодавства про захист персональних даних ЄС. Законодавство Австрії зобов'язувало державні установи збирати та передавати інформацію про доходи з метою оприлюднення прізвищ та розмірів доходу працівників різних державних підприємств у річному звіті, який був відкритим для громадськості. Деякі працівники відмовилися надавати свої дані, обґрунтовуючи це захистом персональних даних.

У своєму висновку СЄС керувався загальними принципами права ЄС щодо захисту персональних даних та статтею 8 ЄКПЛ, нагадуючи, що в той час Хартія не була обов'язковою для виконання. Він вирішив, що збір персональних даних щодо професійного доходу осіб та особливо їх передача третім особам, потрапляє до сфери дії права на повагу до приватного життя та становить втручання в це право. Втручання могло бути виправданим у разі, якщо воно здійснювалось згідно із законом, переслідувало легітимну мету та було необхідним у демократичному суспільстві для досягнення цієї мети. СЄС відзначив, що австрійське законодавство переслідувало легітимну мету, оскільки його ціллю було утримання заробітних плат працівників публічного сектору в розумних межах, що також було пов'язано з економічним добробутом країни. Однак інтерес Австрії щодо забезпечення найкращого використання державних коштів мав бути збалансованим із серйозністю втручання у право осіб на повагу до їхнього приватного життя.

Залишаючи за національними судами вирішення, чи є оприлюднення доходів фізичних осіб необхідним та пропорційним відносно мети, яка переслідувалася законодавством, СЄС закликав національні суди дослідити, чи могла така легітимна мета бути досягнута так само ефективно, але з меншим втручанням. Наприклад, дані могли передаватися тільки моніторинговим органам, а не широкій громадськості.

105 Рішення Суду ЄС C-465/00, C-138/01 та C-139/09, «Рахункова палата проти австрійської телерадіокомпанії "Österreichischer Rundfunk" та інших» та «Кріста Нойкомм і Джозеф Лауерманн проти австрійської телерадіокомпанії "Österreichischer Rundfunk"» (*Rechnungshof v. Österreichischer Rundfunk and Others and Christa Neukomm and Jospeh Lauermann v. Österreichischer Rundfunk*), від 20 травня 2003 р.

Нижченаведені справи демонструють, що балансування права на захист персональних даних та права на доступ до документів вимагає детального аналізу з урахуванням індивідуальних обставин кожної справи. Жодне з цих прав не може автоматично переважати над іншим. Суд ЄС мав можливість надати тлумачення права на доступ до документів, які містили персональні дані, у двох справах.

Приклад: у справі «*Європейська Комісія проти "The Bavarian Lager Co. Ltd"*»[106] 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 ухвалювати рішення про порушення справи проти Сполученого Королівства за невиконання зобов'язань, внаслідок чого було внесено зміни до спірних положень та узгоджено їх із правом ЄС. «Баваріан Лагер» звернулася до Комісії з проханням надати документи, серед яких вимагалася копія протоколу засідання за участі представників Комісії, органів державної влади Сполученого Королівства і Конфедерації загального ринку пивоварів (*Confédération des Brasseurs du Marché Commun* (CBMC). Комісія надала дозвіл на розкриття деяких документів, які стосуються засідання, але вилучила з протоколу імена п'ятьох учасників: дві особи чітко заявили, що заперечують проти свого розкриття, а з іншими трьома в 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 на право захисту приватного життя цих осіб, яке гарантоване 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

106 Рішення Суду ЄС C-28/08 P, «*Європейська Комісія проти "The Bavarian Lager Co. Ltd"*» (*European Commission v. The Bavarian Lager Co. Ltd.*), [ВП], від 29 червня 2010 р.

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 скасував 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 з 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 вилученими прізвищами.

Більше того, відповідно до СЄС «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 «легітимним інтересам суб'єктів персональних даних може бути завдано шкоди», що вимагається Регламентом щодо захисту персональних даних.

Приклад: у справі «*"ClientEarth" та "PAN Europe" проти Європейського агентства безпечності харчових продуктів*»[107] СЄС вирішував, чи була необхідною відмова Європейського органу з безпечності харчових продуктів (ЄОБХП) заявникам у повному доступі до документів для захисту приватності та персональних даних осіб, яким було адресовано ці документи. Документи стосувалися проєкту звіту, підготовленого робочою групою ЄОБХП у співпраці із зовнішніми експертами, щодо розміщення на ринку продуктів захисту рослин. Спочатку ЄОБХП надав частковий доступ заявникам, відмовивши в доступі до деяких робочих версій проєкту. У подальшому було надано доступ до версії проєкту, яка містила індивідуальні коментарі зовнішніх експертів. Однак імена експертів було вилучено на підставі статті 4 (1)(b) Регламенту 45/2001 про обробку персональних

107 Рішення Суду ЄС C-615/13P, «*"ClientEarth" та "PAN Europe" проти Європейського агентства безпечності харчових продуктів*» (*ClientEarth, Pesticide Action Network Europe (PAN Europe) v. European Food Safety Authority (EFSA), European Commission*), від 16 липня 2015 р.

даних інститутами та органами ЄС та у зв'язку з необхідністю захистити приватність зовнішніх експертів. Загальний суд ЄС як суд першої інстанції підтримав рішення ЄОПХБ.

У відповідь на апеляційну скаргу заявників СЄС переглянув рішення суду першої інстанції. Він дійшов висновку, що передача персональних даних у даному випадку була необхідною для забезпечення безсторонності кожного зовнішнього експерта у виконанні їхніх завдань як науковців та забезпечення прозорості процесу ухвалення рішення ЄОБХП. Відповідно до позиції СЄС, ЄОБХП не зазначив, яким чином відкриття імен зовнішніх експертів, які надавали коментарі щодо проєкту документа, могло зашкодити легітимним інтересам експертів. Загального припущення про те, що оприлюднення могло зашкодити приватності, недостатньо, якщо воно не підкріплене конкретними доказами в кожній справі.

Згідно з цими судовими рішеннями 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 скасувати право на захист персональних даних[108].

Цей підхід є схожим на підхід ЄСПЛ щодо приватності та доступу до документів. Це демонструється у рішенні у справі «*Угорський Гельсінський комітет*», у якому ЄСПЛ вказав, що стаття 10 не гарантує право на доступ до інформації, якою володіють органи влади, і не зобов'язує уряд надавати таку інформацію на запит. Однак таке право або зобов'язання може виникнути: по-перше, якщо відкриття такої інформації вимагається рішенням суду, яке набрало законної сили; по-друге, якщо доступ до інформації є інструментом для реалізації особою свого права на свободу вираження поглядів, а саме свободу отримувати і передавати інформацію, та якщо відмова в доступі є втручанням у таке право[109]. Чи становить відмова в доступі до інформації втручання у право на свободу вираження поглядів та до якої міри, має оцінюватись у кожній конкретній справі у світлі індивідуальних обставин, включаючи (i) мету отримання інформації; (ii) характер інформації, яка вимагається; (iii) роль заявника; та (iv) чи є інформація готовою та наявною.

108 Див. деталізовану позицію ЄІЗПД (2011), Публічний доступ до документів, які містять персональні дані, після рішення у справі «*Баваріан Лагер*» (*Public access to documents containing personal data after the Bavarian Lager ruling*), Брюссель, від 24 березня 2011 р.

109 Рішення ЄСПЛ у справі «*Угорський Гельсінський комітет проти Угорщини*» (*Magyar Helsinki Bizottság v. Hungary*), [ВП], № 18030/11, від 8 листопада 2016 р., п. 148.

Приклад: у справі «*Угорський Гельсінський комітет проти Угорщини*»[110] *заявник, неурядова правозахисна організація, звернулась із запитом про надання поліцією інформації про роботу призначених ex officio* захисників. Ця інформація вимагалася для закінчення дослідження функціонування системи державних захисників Угорщини. Поліція відмовила в наданні інформації, стверджуючи, що така інформація становить персональні дані, які не підлягають розкриттю. Застосувавши вищевказані критерії, ЄСПЛ вирішив, що мало місце втручання у право, гарантоване статтею 10. Точніше, заявник прагнув реалізувати своє право на передачу інформації що становила суспільний інтерес, для цих цілей просив доступу до інформації, а інформація була необхідною для реалізації права заявника на свободу вираження поглядів. Інформація про призначення захисників за кошти держави становила предмет суспільного інтересу. Відсутні підстави сумніватися, що дослідження заявника містило інформацію, яку заявник збирався повідомити громадськості, та яку громадськість мала право отримати. Суд погодився з тим, що інформація, яку запитували, була необхідною для виконання заявником його завдання. Інформація також була готова та наявна.

ЄСПЛ дійшов висновку, що відмова в наданні інформації в цій справі порушила саму суть свободи на отримання інформації. Доходячи цього висновку, Суд розглянув мету запитуваної інформації та чи сприяла вона важливим громадським обговоренням, характер інформації та чи становила вона суспільний інтерес, а також роль, яку відіграв у суспільстві запитувач у даній справі.

Обґрунтовуючи свою позицію, Суд зазначив, що дослідження, яке проводилось громадською організацією, стосувалося здійснення правосуддя та реалізації права на справедливий суд – права, яке має визначальну важливість відповідно до ЄКПЛ. Оскільки запитувана інформація містила виключно ті відомості, які перебували в публічному просторі, права на приватність суб'єкта персональних даних (публічних захисників призначених *ex officio*) не були б порушені у разі, якщо заявнику надали б інформацію. Інформація, яку запитував заявник, мала статистичний характер, вона стосувалася кількості призначень на безоплатній основі захисників для представництва обвинувачених у кримінальних провадженнях.

110 Там само, пп. 181, 187–200.

На думку Суду, враховуючи, що дослідження мало сприяти важливій дискусії з питання суспільного значення, будь-які обмеження щодо планованої громадською організацією публікації мали бути предметом суворого контролю. Інформація, яка розглядалася, була суспільно необхідною, оскільки суспільний інтерес охоплює «питання, які здатні породжувати значні суперечки, що стосуються важливої соціальної проблеми або які пов'язані з проблемою, до якої громадськість мала б інтерес, якщо б володіла такою інформацією»[111]. Без сумніву, він також включає обговорення здійснення судочинства та судових процесів, що й було предметом дослідження заявника. Збалансувавши два різних права та застосувавши принцип пропорційності, ЄСПЛ вирішив, що мало місце невиправдане порушення права заявника, гарантованого статтею 10 ЄКПЛ.

1.3.2 Професійна таємниця

У національному законодавстві певні види комунікації можуть становити професійну таємницю. Професійну таємницю можна розуміти як особливий етичний обов'язок, що приводить до юридичного обов'язку, притаманного певним професіям або функціям, які засновуються на вірі та довірі. Люди та установи, які виконують ці функції, зобов'язані не відкривати конфіденційну інформацію, отриману в ході виконання своїх завдань. Професійна таємниця особливо стосується медичної професії та таємниці спілкування адвокатів з клієнтами, а в багатьох країнах також визнається, що обов'язок дотримання професійної таємниці розповсюджується і на фінансовий сектор. Професійна таємниця не є засадничим правом, однак вона захищається як форма права на повагу до приватного життя. Наприклад, СЄС постановляв у своїх рішеннях, що в певних справах «необхідно заборонити оприлюднення певної інформації, яка визнається конфіденційною, для захисту основного права на повагу до приватного життя, гарантованого статтею 8 ЄКПЛ та статтею 7 Хартії»[112]. Як ілюструють продемонстровані приклади, ЄСПЛ також вирішував питання, чи є обмеження професійної таємниці порушенням статті 8 ЄКПЛ.

111 Там само, п. 156.

112 Рішення Суду ЄС, T-462/12 R, «"Pilkington Group Ltd" проти Європейської Комісії» (*Pilkington Group Ltd v. European Commission*), Наказ Голови Загального суду, від 11 березня 2013 р., п. 44.

Приклад: у справі «*Прутеану проти Румунії*»[113] заявник був юристом комерційного підприємства, якого було обмежено в праві здійснювати банківські трансакції з огляду на скарги про шахрайство. Протягом розслідування справи румунські суди надали дозвіл правоохоронним органам прослуховувати та записувати телефоні розмови партнерів підприємства протягом певного періоду. Записи та перехоплена інформація включала й спілкування підприємства з цим юристом.

Пан Прутеану стверджував, що це становило втручання в його право на повагу до приватного життя та кореспонденції. У своєму рішенні ЄСПЛ наголосив на статусі та важливості відносин юриста зі своїм клієнтом. Прослуховування розмов юриста з клієнтом, безперечно, є порушенням професійної таємниці, яка є основою відносин цих людей. У таких випадках юрист також може скаржитись на втручання в його право на повагу до приватного життя та кореспонденції. ЄСПЛ вирішив, що було порушено статтю 8 ЄКПЛ.

Приклад: у справі «*Брітo Феррінью Бексіга Вілла-Нова проти Португалії*»[114] заявниця, юристка, відмовилася відкривати податковим органам виписки з банківських рахунків, обґрунтовуючи це належністю інформації до професійної та банківської таємниці. Прокуратура розпочала розслідування через несплату податків і звернулась за дозволом розкрити професійну таємницю. Національні суди дозволили розкрити професійну та банківську таємницю, визнавши, що суспільний інтерес переважає приватні інтереси заявниці.

Коли справа надійшла на розгляд ЄСПЛ, Суд вирішив, що оцінка виписок з банківських рахунків становить втручання у право заявниці на повагу до професійної таємниці, що є частиною приватного життя. Втручання мало юридичну підставу, оскільки воно здійснювалося на основі кримінального процесуального кодексу та переслідувало легітимну мету. Однак, розглянувши необхідність та пропорційність втручання, ЄСПЛ вказав на той факт, що провадження стосовно зняття конфіденційності було проведено без участі чи інформування заявниці, тож вона не мала змоги навести свої аргументи. Крім того, хоча національне законодавство

113 Рішення ЄСПЛ у справі «Прутеану проти Румунії» (*Pruteanu v. Romania*), № 30181/05, від 3 лютого 2015 р.

114 Рішення ЄСПЛ у справі «*Брітo Феррінью Бексіга Вілла-Нова проти Португалії*» (*Brito Ferrinho Bexiga Villa-Nova v. Portugal*), № 69436/10, від 1 грудня 2015 р.

передбачало проведення консультацій з асоціацією юристів, у цій справі суд не вдався до такого заходу. Нарешті, заявниця не мала жодної можливості реально протидіяти скасуванню конфіденційності або оскаржити такий захід. З огляду на відсутність процедурних гарантій та ефективного судового контролю за заходом щодо скасування конфіденційності, ЄСПЛ визнав, що мало місце порушення статті 8 ЄКПЛ.

Взаємозв'язок між професійною таємницею та захистом персональних даних часто є подвійним. З одного боку, правила та гарантії захисту персональних даних, встановлені законодавством, допомагають забезпечити повагу до професійної таємниці. Наприклад, правила, які вимагають від контролерів та операторів запровадити суворі заходи безпеки даних, мають на меті запобігти, зокрема, розкриттю конфіденційності персональних даних, що становлять професійну таємницю). На додаток, Загальний регламент захисту персональних даних дозволяє обробку даних про стан здоров'я, які становлять особливу категорію персональних даних і вимагають більшого захисту, однак за умови існування прийнятних та особливих заходів захисту суб'єкта персональних даних, зокрема забезпечення професійної таємниці[115].

З іншого боку, обов'язки щодо професійної таємниці, покладені на контролерів та операторів щодо певних персональних даних, можуть обмежувати права суб'єкта персональних даних, особливо право на отримання інформації. Незважаючи навіть на те, що Загальний регламент захисту персональних даних містить широкий перелік інформації, яка в принципі має надаватися суб'єктові персональних даних, якщо дані не отримувалися від нього, така вимога щодо розкриття не поширюється на випадки, коли персональні дані мають залишатися конфіденційними у зв'язку з обов'язком збереження професійної таємниці, що вимагається національним законом або правом ЄС[116].

Загальний регламент захисту персональних даних (ЗРЗПД) надає можливість державам-членам прийняти на законодавчому рівні особливі правила для виконання обов'язку щодо захисту професійної або іншої прирівняної до неї таємниці та узгодження права на захист персональних даних з обов'язком зберігати професійну таємницю[117].

115 Загальний регламент захисту персональних даних, стаття 9 (2) (h) та 9 (3).

116 Там само, стаття 14 (5) (d).

117 Там само, частина 164 преамбули та стаття 90.

ЗРЗПД також передбачає, що держави-члени можуть прийняти особливі положення щодо повноважень контролюючого органу відносно контролерів та операторів, які мають обов'язок дотримуватися професійної таємниці. У випадку отримання відповідних персональних даних під час діяльності, до якої застосовується обов'язок збереження таємниці, спеціальні правила можуть стосуватися повноважень щодо отримання доступу до приміщень такого контролера або оператора, їхнього устаткування, за допомогою якого здійснюється обробка, до самих персональних даних. Відповідно, контролюючий орган з захисту персональних даних повинен поважати обов'язок збереження професійної таємниці, якими керуються контролери та оператори. Більше того, працівники контролюючого органу самі мають обов'язок професійної таємниці під час роботи в цій установі та після звільнення. Протягом виконання своїх обов'язків члени контролюючого органу та його працівники можуть дізнатися конфіденційну інформацію. Стаття 4 (2) Регламенту чітко передбачає, що вони зобов'язані дотримуватись обов'язку збереження професійної таємниці щодо конфіденційної інформації.

ЗРЗПД вимагає від держав-членів повідомляти Комісію про правила, які вони передбачили для узгодження захисту персональних даних і принципів, встановлених регламентом щодо обов'язку дотримання професійної таємниці.

1.3.3 Свобода релігії та переконань

Свобода релігії та переконань захищається статтею 9 ЄКПЛ (свобода думки, совісті і релігії) та статтею 10 Хартії основних прав ЄС. Персональні дані, які виявляють релігійні або філософські переконання, вважаються «чутливими даними» як відповідно до права ЄС, так і права РЄ. Їх обробка та використання підлягають посиленому захисту.

Приклад: у справі «*Сінан Ішик проти Туреччини*»[118] заявник був членом алевітської релігійної спільноти, віра якої сформувалася під впливом суфізму та інших доісламських переконань, і вважається одними спеціалістами окремою релігією, іншими – частиною ісламської релігії. Заявник поскаржився, що всупереч його бажанню документ, що посвідчував його особу, містив графу, у якій вказувалося, що його релігія «іслам», а не «алеві». Національні суди відмовили в задоволені позову про зміну

118 Рішення ЄСПЛ у справі «Сінан Ішик проти Туреччини» (*Sinan Işık v. Turkey*), № 21924/05, 2 лютого 2010 р.

документа із зазначенням «алеві» на тій підставі, що це слово означає підгрупу ісламу, а не окрему релігію. Заявник поскаржився до ЄСПЛ, що всупереч його згоді він мав відкрити інформацію про свою віру у зв'язку з обов'язковим зазначенням віри в документі, що посвідчує особу, та що це порушило його право на свободу релігії та совісті, особливо враховуючи, що визначення «іслам» у його посвідченні особи є помилковим.

ЄСПЛ повторив, що свобода релігії передбачає свободу сповідувати свою релігію спільно з іншими, прилюдно та в колі осіб, які поділяють такі самі вірування, а також самостійно та приватно. Національне законодавство, чинне на той час, зобов'язувало осіб носити з собою документ, що посвідчує особу, який підлягав пред'явленню на вимогу будь-якого органу влади або приватного підприємства і який містив інформацію про їхню релігію. Такий обов'язок не враховував, що право на сповідування релігії також передбачає зворотне, тобто право не бути зобов'язаним розкривати свою релігію. Незважаючи на твердження уряду про те, що національне законодавство було змінене і вже передбачало можливість для осіб вимагати залишити цю графу в документі не заповненою, на думку Суду, сам факт звернення з вимогою видалити інформацію про релігію може відкрити ставлення особи до релігії. Крім того, якщо документ, що посвідчує особу, має таку графу, залишення її порожньою має особливу конотацію, оскільки власники документа, який не містить інформації про релігію, можуть вирізнятися з-поміж тих, хто має в документі інформацію про свої вірування. ЄСПЛ вирішив, що національне законодавство суперечить статті 9 ЄКПЛ.

Втім функціонування церкви та релігійних об'єднань або спільнот може потребувати обробки особистої інформації про своїх членів для спілкування та організації діяльності в спільноті вірян. Через це церкви та релігійні об'єднання часто встановлюють правила щодо обробки персональних даних. Відповідно до статті 91 Загального регламенту захисту персональних даних, якщо такі правила є повними, вони можуть залишатись чинними за умови відповідності положенням регламенту. Незалежний контролюючий орган повинен мати право перевіряти такі церкви та релігійні об'єднання, які мають такі правила. Для таких суб'єктів допускається створення особливого контролюючого органу за умови, що він відповідає всім вимогам, які передбачені для такого органу Загальним регламентом захисту персональних даних[119].

119 Загальний регламент захисту персональних даних, стаття 91 (2).

Релігійні організації можуть здійснювати обробку персональних даних з декількох причин – наприклад, для підтримки контактів зі своїми парафіянами або для поширення інформації про організацію релігійних чи благодійних подій та свят. У деяких державах церкви повинні вести реєстр своїх членів для цілей оподаткування, оскільки членство у релігійних організаціях може впливати на податки фізичних осіб. У будь-якому випадку, відповідно до європейського права дані, які виявляють релігійні переконання, є чутливими даними, і церкви мають нести відповідальність за використання та обробку таких даних, особливо враховуючи, що часто інформація, яка обробляється релігійними організаціями, стосується дітей, осіб похилого віку або інших вразливих членів суспільства.

1.3.4 Свобода художньої творчості та науково-дослідницької діяльності

Ще одним правом, яке потребує 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 чітко гарантується статтею 13 Хартії основних прав ЄС. Воно переважно 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[120]. Здійснення гарантованого статтею 13 Хартії права також може підлягати обмеженням, визначеним статтею 52 (1) Хартії, які можуть тлумачитись у світлі статті 10 (2) ЄКПЛ[121].

Приклад: у справі «*Асоціація візуальних художників проти Австрії*»[122] австрійські суди заборонили заявникові (об'єднанню) продовжувати експозицію картини з фотографіями голів громадських діячів, тіла яких були зображені в сексуальних позах. Австрійський член парламенту, фото якого було використане в картині, подав позов до суду проти заявника, намагаючись отримати судову заборону на експонування картини. Національний суд видав судову заборону. ЄСПЛ нагадав, що

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

121 Коментарі до Хартії основних прав, OJ 2007, C 303.

122 Рішення ЄСПЛ у справі «Асоціація візуальних художників проти Австрії» (*Vereinigung bildender Künstler v. Austria*), № 68354/01, від 25 січня 2007 р., пп. 26 та 34.

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 в їхнє право на свободу вираження поглядів. Враховуючи, що картина – це колаж, у якому було використано лише фотокартки голів людей, і що зображення їхніх тіл було нереалістичним і перебільшеним, що навряд чи могло 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] мав би бути більш толерантним до критики». Зважуючи на 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. І Загальний регламент захисту персональних даних, і Конвенція 108 дозволяють зберігати персональні дані триваліший період часу. Більше того, незалежно від початкової мети певної обробки персональних даних, подальше їх використання з науковою метою не вважається несумісною ціллю[123]. Водночас, для захисту прав та свобод суб'єкта персональних даних мають бути передбачені належні гарантії такої обробки. ЄС або держави-члени можуть передбачити певні винятки для прав суб'єкта персональних даних, наприклад, права на доступ, зміну, обмеження обробки та права на заперечення, у випадках, коли йдеться про обробку їхніх персональних даних в наукових, історичних або статистичних цілях (див. також розділи 6.1 та 9.4).

1.3.5 Захист інтелектуальної власності

Право на захист майна закріплено в статті 1 Першого протоколу до ЄКПЛ, а також у статті 17 (1) Хартії основних прав ЄС. Одним із важливих аспектів права на мирне володіння своїм майном, який є особливо актуальним в контексті захисту персональних даних, є захист інтелектуальної власності, на що чітко

123 Загальний регламент захисту персональних даних, стаття 5 (1) (b) та Оновлена Конвенція 108, стаття 5 (4) (b).

вказується у статті 17 (2) Хартії. У правовій системі ЄС можна знайти низку директив, у яких передбачено ефективний захист інтелектуальної власності, зокрема авторського права. Інтелектуальна власність охоплює не лише питання прав на літературні та художні твори, але також патентні права, право на торгову марку і суміжні права.

Як роз'яснено в практиці Суду ЄС, захист основоположного права на володіння майном має бути узгоджений із захистом інших основоположних прав, зокрема з правом на захист персональних даних[124]. Траплялися справи, коли установи захисту авторських прав вимагали від інтернет-провайдерів розкрити особи користувачів файлообмінних інтернет-платформ. Такі платформи часто дозволяють інтернет-користувачам безоплатно завантажувати музичні твори навіть попри те, що ті захищені авторським правом.

Приклад: «*Музичні продюсери Іспанії (Promusicae) проти "Telefonica de Espana SAU"*»[125] стосувалася відмови іспанського інтернет-провайдера («Telefonica») розкрити неприбутковій організації музичних продюсерів і видавців музичних та аудіовізуальних записів «Promusicae» персональні дані про деяких осіб, яким надавалися послуги з доступу до інтернету. «Promusicae» домагалася розкриття інформації з метою подання цивільного позову проти тих осіб, що, як вона зазначала, використовували файлообмінну програму доступу до фонограм, права на експлуатацію яких належали членам «Promusicae».

Іспанський суд порушив перед Судом ЄС питання, чи потрібно відповідно до 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 в контексті статей 17 і 47 Хартії. СЄС дійшов висновку, що ці три директиви, а також Директива про конфіденційність та електронні комунікації (№ 2002/58/ЄС) не перешкоджають здійсненню державою-членом зобов'язання щодо розкриття персональних даних у контексті цивільного позову про забезпечення ефективного захисту авторських прав.

124 Рішення Суду ЄС C-275/06, «Музичні продюсери Іспанії (Promusicae) проти "Telefonica de Espana SAU"» (*Productores de Música de España (Promusicae) v. Telefónica de España SAU*), [ВП], від 29 січня 2008р., пп. 62–68.

125 Там само, пп. 54 та 60.

СЄС зазначив, що у справі порушується питання про необхідність узгодження вимог захисту різних основоположних прав, а саме права на повагу до приватного життя з правом на захист майна і на ефективний засіб юридичного захисту. Суд дійшов висновку, що «держави-члени повинні звертати увагу на необхідність брати до уваги тлумачення вказаних директив під час їх імплементації, 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 ґрунтуються на тлумаченні, яке суперечило б тим основоположним правам або іншим загальним принципам права Співтовариства, як, наприклад, принципу пропорційності»[126].

Приклад: справа «*"Bonnier Audio AB" та інші проти "Perfect Communication Sweden AB"*»[127] стосувалася балансу між правом інтелектуальної власності та правом на захист персональних даних. Заявник – п'ять компаній видавців, які володіли правом інтелектуальної власності на 27 аудіо книжок - звернулися до суду Швеції, стверджуючи про порушення їхнього права інтелектуальної власності ФОП-сервером (файлообмінний протокол, який дозволяв поширювати файли та дані через інтернет). Заявники вимагали від провайдера інтернет-послуг (ПІП) відкрити імена та адреси особи, яка використовувала IP-адресу, з якої ті файли було надіслано. ПІП – компанія ePhone – не погодився з такою вимогою, стверджуючи, що це буде порушенням Директиви № 2006/24 (Директива про зберігання даних, яку було визнано нечинною 2014 року).

Шведський суд звернувся до СЄС з питанням, чи забороняє Директива № 2006/24 застосування національного закону, що ґрунтувався на статті 8 Директиви № 2004/48 (Директива про захист прав на об'єкти інтелектуальної власності), яка дозволяє зобов'язати ПІП передати власникам авторського права інформацію про підписників, чиї IP-адреси було,

126 Там само, пп. 65–68; див. також рішення Суду ЄС, C-360/10, «Бельгійська асоціація авторів, композиторів та видавців CVBA (SABAM) проти "Netlog NV"» (*Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*), від 16 лютого 2012 р.

127 Рішення Суду ЄС, C-461/10, «*"Bonnier Audio AB" та інші проти "Perfect Communication Sweden AB"*» (*Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v. Perfect Communication Sweden AB*), від 19 квітня 2012 р.

як стверджується, використано з порушенням. Питання ґрунтувалося на припущенні, що заявник надав чіткі докази порушення певного авторського права, і що захід пропорційний.

Суд ЄС вказав, що Директива № 2006/24 стосувалася виключно обробки та збереження даних, генерованих надавачами електронних комунікаційних послуг, з метою розслідування, виявлення серйозних злочинів і притягнення до відповідальності за їх вчинення, а також передачі таких даних компетентним державним органам. Відповідно, національне законодавство, яке імплементувало Директиву про захист прав на об'єкти інтелектуальної власності, не охоплюється Директивою № 2006/24 та, відповідно, не виключається нею[128].

Щодо передачі імен та адрес, що їх вимагали заявники, СЄС вказав, що така дія становить обробку персональних даних та охоплюється Директивою № 2002/58 (Директива про конфіденційність та електронні комунікації). Він також зазначив, що передача цих даних була необхідною для ініціювання цивільного судового провадження суб'єктами авторського права для забезпечення ефективного захисту їхніх прав і, відповідно, підпадала під дію Директиви № 2004/48[129].

СЄС вирішив, що Директива № 2002/58 та Директива № 2004/48 мають тлумачитись як такі, що не виключають національне законодавство, щодо якого було порушено питання в основному провадженні, в тій мірі, в якій законодавство дозволяє національним судам, перед якими порушено питання щодо відкриття персональних даних, зважувати конфліктні інтереси на основі фактів кожної індивідуальної справи та належним чином враховувати вимоги принципу пропорційності.

128 Там само, пп. 40–41.

129 Там само, пп. 52–54. Див., також рішення Суду ЄС C-275/06, «Музичні продюсери Іспанії (Promusicae) проти "Telefonica de Espana SAU"» (*Productores de Música de España (Promusicae) v. Telefónica de España SAU*), [ВП], від 29 січня 2008р., п. 58.

1.3.6 Захист персональних даних та економічні інтереси

У цифрову еру або ж еру великих даних (big data) дані вважаються «новою нафтою» економіки для розвитку інновацій та креативності[130]. Багато компаній побудували розгалужені бізнес-моделі з використанням обробки даних, і така обробка часто включає персональні дані. Певні компанії можуть вважати, що спеціальні правила захисту персональних даних на практиці можуть становити надмірні зобов'язання, що може негативно вплинути на економічні результати. Відповідно, виникає питання, чи можуть економічні інтереси контролера чи оператора або ж інтереси громадськості загалом виправдати обмеження права на захист персональних даних.

Приклад: у справі «*Google Spain*»[131] СЄС вирішив, що за певних умов фізичні особи мають право вимагати, щоб результати пошуку було видалено з пошукового індексу систем пошуку. У своєму обґрунтуванні СЄС вказав на факт того, що використання пошукових систем і перелік результатів пошуку може надати детальний профіль фізичної особи. Ця інформація може стосуватися широкого кола аспектів приватного життя особи і не могла б бути легко знайдена або скомпонована без системи пошуку. Відповідно, має місце особливо серйозне втручання в основоположне право суб'єкта даних на повагу до приватного життя та права на захист персональних даних.

Далі СЄС розглянув, чи може таке втручання бути виправданим. Щодо економічного інтересу компаній-операторів систем пошуку у здійсненні обробки, СЄС зазначив, що «очевидно [втручання] не може бути виправдане самим лише економічним інтересом, який оператор такої системи має в такій обробці» і що «за загальним правилом» основоположні права, передбачені статтями 7 та 8 Хартії, переважують такий економічний інтерес та інтерес суспільства загалом у знайдені такої інформації за пошуком, пов'язаним з іменем суб'єкта даних»[132].

130 Див., наприклад, *Financial Times* (2016), "Дані є новою нафтою... хто збирається нею володіти?", від 16 листопада 2016 р.

131 Рішення Суду ЄС, C-131/12, «"Google Spain SL", "Google Inc." проти Іспанського агентства захисту даних (AEPD) та Маріо Костеха Гонсалеса» (*Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*), [ВП], від 13 травня 2014 р.

132 Там само., пп. 81 та 97.

Одним з ключових аспектів європейського права із захисту персональних даних є надання фізичним особам більшого контролю за їхніми персональними даними. Особливо в цифрову еру наявний дисбаланс між можливостями бізнес-компаній, які обробляють та мають доступ до великих обсягів персональних даних, та можливостями фізичних осіб, яким належать ці персональні дані, контролювати свою інформацію. Суд ЄС завжди застосовує індивідуальний підхід у справах, пов'язаних з балансом захисту даних та економічних інтересів, як-от інтереси третіх осіб щодо акціонерних товариств та товариств з обмеженою відповідальністю, як це видно з рішення у справі «*Манні*».

Приклад: справа «*Манні*»[133] стосувалася включення персональних даних особи в державний реєстр господарюючих суб'єктів. Виявивши, що потенційні клієнти, звернувшись до реєстру, можуть побачити, що він був директором компанії, яку було визнано банкрутом більше десяти років тому, пан Манні звернувся до Торгової палати м. Лечче з вимогою видалити його дані з реєстру. Ця інформація перешкоджала отриманню ним клієнтів та могла мати негативний вплив на його економічні інтереси.

У цій справі СЄС мав вирішити питання, чи передбачає законодавство ЄС право особи на видалення даних. Вирішуючи справу, СЄС збалансував правила захисту персональних даних ЄС та економічний інтерес пана Манні у видаленні інформації про його колишнє підприємство, яке стало банкрутом, з суспільним інтересом щодо доступу до цієї інформації. Він взяв до уваги, що відкриття державного реєстру компаній було передбачене законом та, зокрема, Директивою ЄС з метою забезпечення більшої доступності інформації про компанії для третіх осіб. Таке відкриття було важливим для захисту інтересів третіх осіб, які могли мати бажання вести бізнес з певними компаніями, і при цьому єдиними гарантіями, які надавалися третім особам акціонерними товариствами та товариствами з обмеженою відповідальністю, були їхні активи. Таким чином, «базові документи компанії мають бути відкриті для того, щоб треті сторони могли ознайомитися з їхнім змістом та іншою інформацією щодо компанії, особливо щодо осіб, які можуть накласти зобов'язання на компанію»[134].

133 Рішення Суду ЄС, C-398/15, «Торгово-промислова та сільськогосподарська палата м. Лечче проти Сальваторе Манні» (*Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*), від 9 березня 2017р.

134 Там само, п. 49.

З огляду на важливість легітимної мети, яка переслідувалася реєстром, СЄС вирішив, що пан Манні не мав права на видалення своїх персональних даних, оскільки необхідність захистити інтереси третіх осіб по відношенню до акціонерних товариств та товариств з обмеженою відповідальністю, а також забезпечити правову визначеність, справедливу торгівлю та, таким чином, належне функціонування внутрішнього ринку, переважували його права за законодавством про захист персональних даних. Це особливо слушно, враховуючи, що особи, які вирішують брати участь у торгівлі з використанням акціонерного товариства або товариства з обмеженою відповідальністю, знають про вимогу розкриття інформації стосовно їх особи та функцій.

Вирішивши, що підстав для видалення персональних даних у цій справі відсутні, СЄС, однак, визнав існування права на заперечення обробки даних, вказавши: «неможливо виключати, що [...] можуть існувати особливі ситуації, у яких переважні та правомірні підстави, пов'язані з особливістю справи зацікавленої особи, виправдають обмеження доступу [...] зацікавлених третіх осіб до персональних даних, внесених до реєстру, зі спливом достатньо тривалого періоду»[135].

СЄС наголосив, що оцінку в кожній справі мають здійснювати національні суди і з урахуванням усіх відповідних обставин особи встановлювати наявність або відсутність законних та переважних підстав для винятково-го обґрунтування обмеження доступу третіх осіб до персональних даних, які містяться в реєстрі суб'єктів господарювання. Водночас у справі пана Манні він визнав, що сам факт відкриття персональних даних у реєстрі з можливістю впливу на коло клієнтів не може бути визнаний такою легітимною та переважною підставою. Потенційні клієнти пана Манні мають легітимний інтерес отримати інформацію щодо банкрутства його попередньої компанії.

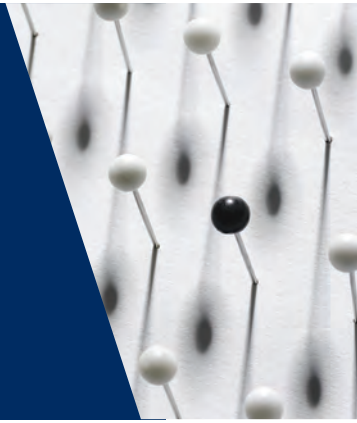
Втручання в основоположні права пана Манні та інших осіб, персональні дані яких внесено до реєстру, на повагу до приватного життя та захист персональних даних, гарантованих статтями 7 та 8 Хартії, переслідувало ціль загального інтересу та було необхідним і пропорційним.

135 Там само, п. 60.

Таким чином, у справі *Манні* СЄС вирішив, що право на повагу до приватного життя та право на захист персональних даних не переважають інтерес третіх осіб отримати доступ до інформації з реєстру компаній по відношенню до акціонерних товариств та товариств з обмеженою відповідальністю.

2

Термінологія захисту персональних даних



ЄС	Питання, що висвітлюються	РЄ
Персональні дані		
Загальний регламент захисту персональних даних, стаття 4 (1) Загальний регламент захисту персональних даних, статті 4 (5) та 5 (1) (e) Загальний регламент захисту персональних даних, стаття 9 СЄС, об'єднані справи, C-92/09 та C-93/09 «"Volker und Markus Schecke GbR" та Хартмут Ейферт проти землі Гессен» (*Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*) [ВП], 2010 р. СЄС, C-275/06 «Музичні продюсери Іспанії (Promusicae) проти "Telefonica de Espana SAU"»	**Юридичне визначення захисту персональних даних**	Оновлена Конвенція 108, стаття 2 (a) ЄСПЛ «"Бернх Ларсен Холдинг АС" та інші проти Норвегії» (*Bernh Larsen Holding AS and Others v. Norway*), № 24117/08, 2013 ЄСПЛ, «Узун проти Німеччини» (*Uzun v. Germany*) № 35623/05, 2010 ЄСПЛ, «Аманн проти Швейцарії» (*Amann v. Switzerland*) [ВП], № 27798/95, 2000

ЄС	Питання, що висвітлюються	РЄ
(*Productores de Musica de Espana (Promusicae) v. Telefonica de Espana SAU*), [ВП], 2008 СЄС, C-70/10, «"Scarlet Extended SA" проти Бельгійської асоціації авторів, композиторів та видавців (SABAM)», (*Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL*), 2011 СЄС, C-582/14, «Патрік Бреєр проти Федеративної Республіки Німеччини» (*Patrick Breyer v. Bundesrepublik Deutschland*), 2016 СЄС, об'єднані справи, C-141/12 та C-372/12, «YS проти Міністра з питань імміграції, інтеграції та притулку» та «Міністр з питань імміграції, інтеграції та притулку проти M. та S.» (*YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S*), 2014		
СЄС, C-101/01, «Кримінальне провадження проти Bodil Lindqvist» (*Criminal proceedings against Bodil Lindqvist*), 2003	**Особливі персональні дані (чутливі дані)**	Оновлена Конвенція 108, Стаття 6 (1)
СЄС, C-434/16, «Пітер Новак проти Комісара із захисту персональних даних» (*Peter Nowak v. Data Protection Commissioner*), 2017	**Анонімні дані та псевдоніми**	Оновлена Конвенція 108, Стаття 5 (4) (e) Пояснювальна записка до Оновленої Конвенції 108, Пункт 50

ЄС	Питання, що висвітлюються	РЄ
Обробка даних		
Загальний регламент захисту персональних даних, стаття 4 (2) СЄС, C-212/13, «Франтішек Ринеш проти Офісу захисту персональних даних» (*František Ryneš v. Úřad pro ochranu osobních údajů*), 2014 СЄС, C-398/15, «Торгово-промислова та сільськогосподарська палата м. Лечче проти Сальваторе Манні» (*Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*), 2017 СЄС, C-101/01, Кримінальне провадження проти Bodil Lindqvist (*Criminal proceedings against Bodil Lindqvist*), 2003 СЄС, C-131/12, «"Google Spain SL", "Google Inc." проти Іспанського агентства захисту даних (AEPD) та Маріо Костеха Гонсалеса» (*Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*) [ВП], 2014	**Визначення**	Оновлена Конвенція 108, Стаття 2 (b) та (c)
Користувачі даних		
Загальний регламент захисту персональних даних, стаття 4 (7)	**Контролер**	Оновлена Конвенція 108, стаття 2 (d) *Рекомендація щодо профайлінгу*, стаття 1 (g)*

ЄС	Питання, що висвітлюються	РЄ
СЄС, C-212/13, «Франтішек Ринеш проти Офісу захисту персональних даних» (*František Ryneš v. Úřad pro ochranu osobních údajů*), 2014 СЄС, C-1318/12, «“Google Spain SL”, “Google Inc.“ проти Іспанського агентства захисту даних (AEPD) та Маріо Костеха Гонсалеса» (*Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*) [ВП], 2014		
Загальний регламент захисту персональних даних, стаття 4 (8)	**Оператор**	Оновлена Конвенція 108, стаття 2 (f) *Рекомендація щодо профайлінгу*, стаття 1 (h)
Загальний регламент захисту персональних даних, стаття 4 (9)	**Одержувач**	Оновлена Конвенція 108, стаття 2 (e)
Загальний регламент захисту персональних даних, стаття 4 (10)	**Третя сторона**	
Згода		
Загальний регламент захисту персональних даних, статті 4 (11) та 7 СЄС, C-543/09, «“Deutsche Telekom” проти Федеративної Республіки Німеччини» (*Deutsche Telekom AG v. Bundesrepublik Deutschland*), 2011	**Визначення та вимоги чинної згоди**	Оновлена Конвенція 108, стаття 5 (2) *Рекомендація щодо захисту медичних даних*, стаття 6, та ряд наступних рекомендацій ЄСПЛ, «Елберте проти Латвії» (*Elberte v. Latvia*), № 61243/08, 2015

ЄС	Питання, що висвітлюються	РЄ
СЄС, C-536/15, «“Tele2 (Netherlands) BV” та інші проти Управління споживачів та ринку (УСР)» *(Tele2 (Netherlands) BV and Others v. Autoriteit Consument en Markt (AMC)*, 2017		

*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) (Рекомендація щодо профайлінгу), 23 листопада 2010 р.*

2.1 Персональні дані

Ключові моменти

- Дані є персональними даними, коли в них йдеться про ідентифіковану особу чи принаймні особу, яку можна ідентифікувати, “суб’єкт персональних даних”.
- Для визначення, чи можна ідентифікувати особу, контролер або інша особа має врахувати всі раціональні засоби, які можуть бути використанні – такі як виокремлення – для прямої чи непрямої ідентифікації фізичної особи.
- Автентифікація означає підтвердження, що певна особа має певну ідентичність та/або уповноважена здійснювати певну діяльність.
- Існують особливі категорії даних, так звані чутливі дані, перелік яких наводиться в Оновленій Конвенції 108 і в законодавстві ЄС із захисту персональних даних. Вони потребують посиленого захисту, а отже є предметом особливого правового режиму.
- Анонімні дані – це ті, які більше не стосуються жодної ідентифікованої особи або особи, яку можна ідентифікувати.
- Псевдонімізація – це захід, за допомогою якого персональні дані не мають зв’язку з суб’єктом персональних даних без додаткової інформації, яка зберігається окремо. “Ключ”, який надає можливість повторної ідентифікації (реідентифікації) суб’єкта даних, має зберігатись окремо та в безпеці. Дані, які були псевдонімізовані, залишаються персональними даними. Законодавство ЄС не містить концепції «псевдонімізованих даних».
- Принципи та правила захисту персональних даних не застосовуються до анонімізованої інформації, однак вони застосовуються до псевдонімізованих даних.

2.1.1 Головні аспекти концепції персональних даних

Відповідно до **права ЄС,** як і **права РЄ,** «персональні дані» визначаються як інформація, що стосується ідентифікованої фізичної особи або фізичної особи, яку можна ідентифікувати[136]. Йдеться про інформацію про фізичну особи, ідентичність якої чітко встановлено або може бути встановлено за допомогою додаткової інформації. Для визначення, чи можна особу ідентифікувати, контролер або інша особа повинна розглянути всі раціональні засоби, які можуть бути використанні для прямої чи не прямої ідентифікації фізичної особи, такі, як, наприклад, виокремлення, що дає можливість відрізнити одну людину від іншої[137].

Якщо дані такої особи обробляються, така особа називається «суб'єктом персональних даних».

Суб'єкт персональних даних

Відповідно до **права ЄС** вигодонабувачами правил захисту персональних даних[138] можуть бути тільки фізичні особи, і тільки живі фізичні особи перебувають під захистом права із захисту персональних даних ЄС[139]. Загальний регламент захисту персональних даних (ЗГЗПД) визначає персональні дані як будь-яку інформацію про ідентифіковану фізичну особу або фізичну особу, яку можна ідентифікувати.

Право РЄ, а саме Оновлена Конвенція 108 також вказує на захист фізичних осіб стосовно обробки їхніх персональних даних. У ній так само персональні дані означають інформацію стосовно ідентифікованої фізичної особи або фізичної особи, яку можливо ідентифікувати. Ця фізична особа або індивід, як визначає ЗГЗПД та Оновлена Конвенція 108, називається в праві із захисту персональних даних суб'єктом персональних даних.

Юридичні особи також мають певний захист. У своїй практиці ЄСПЛ виносить рішення за заявами юридичних осіб, які стверджують про порушення їхнього

136 Загальний регламент захисту персональних даних, стаття 4 (1); Оновлена Конвенція 108, стаття 2 (a).

137 Загальний регламент захисту персональних даних, п. 26 преамбули.

138 Там само, стаття 1.

139 Там само, положення 27. Див. також Робоча група «Стаття 29» (2007), Висновок 4/2007 про концепцію персональних даних. РГ 136, від 20 червня 2007 р., с. 22.

права на захист від використання їхніх даних за статтею 8 ЄКПЛ. Стаття 8 ЄКПЛ поширюється як на право на повагу до приватного і сімейного життя, так і на право на повагу до житла і кореспонденції. Таким чином, Суд може розглядати справи під кутом цього другого права, а не права на повагу до приватного життя.

Приклад: справа «"*Бернг Ларсен Холдінг АС" та інші проти Норвегії*»[140] стосувалася скарги трьох норвезьких компаній щодо наказу податкових органів про зобов'язання компаній надати податковим аудиторам копію даних, які зберігалися на комп'ютерному сервері, що був у їхньому спільному користуванні.

ЄСПЛ вирішив, що таке зобов'язання, покладене на компанії-заявників, становить втручання в їхні права на повагу до «житла» та «кореспонденції» за статтею 8 ЄКПЛ. Однак Суд встановив, що податкові органи вжили ефективних та належних гарантій проти свавілля: заявникам повідомили про це завчасно, вони були присутні та могли робити зауваження під час здійснення оперативного заходу, інформацію мало бути знищено, як тільки перевірку податковими органами буде закінчено. За таких обставин Суд вирішив, що було встановлено справедливий баланс між правом компаній-заявників на повагу до «житла» та «кореспонденції» і їхнім інтересом щодо захисту приватності осіб, які на них працювали, та суспільним інтересом у забезпеченні ефективної перевірки для цілей податкового аналізу. Суд дійшов висновку, що порушення статті 8 не було.

Відповідно до Оновленої Конвенції 108 захист персональних даних насамперед стосується захисту фізичних осіб. Однак держави-члени можуть поширити своїм законодавством правила захисту даних на юридичних осіб, таких як компанії та об'єднання. У пояснювальній записці до Оновленої Конвенції зазначається, що національний закон може захищати інтереси юридичних осіб шляхом поширення Конвенції на таких осіб[141]. **Право із захисту персональних даних ЄС** не поширюється на обробку даних, які стосуються юридичних осіб, зокрема підприємств, зареєстрованих як юридичні особи, включаючи назву

140 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. Див. також рішення ЄСПЛ у справі «Либерті та інші проти Сполученого Королівства» (*Liberty and Others v. the United Kingdom*), № 58243/00, від 1 липня 2008 р.

141 Пояснювальна записка до Оновленої Конвенції 108, п. 30.

та форму юридичної особи та їхні контактні даних[142]. Водночас Директива про конфіденційність та електронні комунікації дійсно захищає конфіденційність комунікації та легітимний інтерес юридичних осіб щодо збільшення спроможності автоматичного збереження та обробки даних, що стосуються підписників та користувачів[143]. Так само й проєкт нової Директиви про конфіденційність та електронні комунікації поширює захист на юридичних осіб.

Приклад: у справі «*"Volker und Markus Schecke GbR" та Хартмут Ейферт проти землі Гессен*»[144] у контексті оприлюднення персональних даних відносно отримувачів допомоги з сільськогосподарських фондів СЄС зазначив, що «юридичні особи можуть вимагати захисту за статтями 7 та 8 Хартії щодо такої ідентифікації тільки в тій мірі, в якій офіційна назва юридичної особи ідентифікує одну або більше фізичних осіб. [...] Право на повагу до приватного життя в контексті обробки персональних даних за статтями 7 та 8 Хартії стосується будь-якої інформації про ідентифіковану фізичну особу або особу, яку може бути ідентифіковано [...]"[145].

При встановленні балансу між інтересом ЄС щодо забезпечення прозорості надання субсидій з одного боку, та, з іншого боку - основоположним правом на приватність та правом на захист персональних даних фізичних осіб, які отримали ці субсидії, Суд ЄС визнав, що втручання в ці основоположні права було непропорційним. Він вирішив, що досягнення мети прозорості могло забезпечуватися заходами з менш серйозними наслідками для прав осіб, яких це стосувалося. Водночас, вивчаючи питання пропорційності оприлюднення інформації стосовно юридичних осіб, які отримали субсидію, СЄС дійшов іншого висновку про те, що таке оприлюднення не вийшло за межі принципу пропорційності. Він вказав, що «серйозність порушення права на захист персональних даних проявляє себе для юридичних і фізичних осіб по-різному»[146]. Юридичні особи мають більш широкі обов'язки щодо оприлюднення інформації про них. СЄС вирішив, що вимагати від національних органів досліджувати перед

142 Загальний регламент захисту персональних даних, п. 14 преамбули.

143 Директива про конфіденційність та електронні комунікації, п. 7 преамбули та стаття 1 (2).

144 Рішення Суду ЄС, об'єднані справи C-92/09 and C-93/09, «"Volker und Markus Schecke GbR" та Хартмут Ейферт проти землі Гессен» (*Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*) [ВП], від 9 листопада 2010 р., п. 53.

145 Там само., пп. 52–53.

146 Там само, п. 87.

оприлюдненням, чи ідентифікують дані кожної юридичної особи, яка отримала субсидію, будь-яку пов'язану фізичну особу, означало б покласти на ці органи необґрунтований адміністративний тягар. Таким чином, законодавство, яке вимагає загальне оприлюднення даних юридичних осіб, встановило справедливий баланс між конкурентними інтересами.

Характер даних

Будь-який вид інформації може бути персональними даними за умови, що інформація стосується ідентифікованої особи або особи, яку можна ідентифікувати.

Приклад: персональними даними стосовно працівника є оцінка з боку інспектора діяльності працівника на роботі, збережена в особистій справі працівника. Це є персональними даними, навіть якщо інформація відображає частково чи загалом особисту думку інспектора, як-от «працівник не відповідає займаній посаді», а не фактичну інформацію, наприклад, «працівник був відсутній на роботі п'ять тижнів протягом останніх шести місяців».

Персональні дані включають інформацію стосовно приватного життя особи, яка також охоплює професійне життя та інформацію про її або його публічне життя.

У справі *Аманн*[147] ЄСПЛ розтлумачив поняття «персональні дані» як таке, що не обмежується питаннями приватної сфери життя фізичної особи. Таке значення поняття «персональні дані» також відповідає ЗРЗПД.

Приклад: у справі «*"Volker und Markus Schecke GbR" та Хартмут Ейферт проти землі Гессен*»[148] СЄС зазначив, що «в цьому контексті немає значення, що персональні дані не стосуються діяльності професійного характеру [...]. Європейський суд з прав людини з посиланням на статтю 8

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

148 Рішення Суду ЄС, об'єднані справи C-92/09 and C-93/09, «"Volker und Markus Schecke GbR" та Хартмут Ейферт проти землі Гессен» (*Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*) [ВП], від 9 листопада 2010 р., п. 59.

Конвенції [ЄКПЛ] вирішив, що поняття «приватне життя» не може тлумачитися вузько, і що відсутні принципові причини виправдовувати виключення діяльності професійного характеру з поняття приватного життя."

Приклад: у об'єднаних справах «*YS проти Міністра з питань імміграції, інтеграції та притулку» та «Міністр з питань імміграції, інтеграції та притулку проти M. та S.*»[149] СЄС встановив, що юридичний аналіз, який міститься в проєкті рішення Служби імміграції та натуралізації про розгляд заяв на надання дозволу на проживання, сам собою не становить персональні дані, хоча він може включати певні персональні дані.

Практика ЄСПЛ стосовно статті 8 ЄКПЛ підтверджує, що може бути складно повністю відокремити питання приватного та професійного життя[150].

Приклад: у справі «*Барбулеску проти Румунії*»[151] заявника було звільнено за використання інтернету його роботодавця протягом робочих годин, що було порушенням внутрішніх правил. Роботодавець моніторив його спілкування та записи, які містили повідомлення виключно приватного характеру. Ці повідомлення були надані національному суду під час провадження. Визнаючи застосовність статті 8 ЄКПЛ, ЄСПЛ залишив відкритим питання, чи надавали заявнику обмежувальні правила, встановлені роботодавцем, обґрунтовані очікування приватності, але в будь-якому разі він вирішив, що інструкції роботодавця не можуть звести до нуля приватне соціальне життя, коли людина перебуває на робочому місці. Щодо суті справи, Договірні Сторони мають користуватися широкими межами розсуду в оцінці необхідності встановлення законодавчого регулювання умов, за яких роботодавець міг би регулювати спілкування – електронне або в іншій формі – своїх працівників на робочому місці, але не пов'язане з роботою. Однак національні органи влади мають забезпечити, щоб запровадженні роботодавцем заходи з моніторингу

149 Рішення Суду ЄС, об'єднані справи «YS проти Міністра з питань імміграції, інтеграції та притулку» та «Міністр з питань імміграції, інтеграції та притулку проти M. та S.» (*YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S*), від 17 липня 2014 р., п. 39.

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

151 Рішення ЄСПЛ у справі «Барбулеску проти Румунії» (*Bărbulescu v. Romania*) [ВП], № 61496/08, від 5 вересня 2017 р., п. 121.

кореспонденції та іншої комунікації, незалежно він обсягу та тривалості таких заходів, супроводжувались адекватними та належними гарантіями проти зловживання. Пропорційність та процедурні гарантії проти свавілля були суттєвими, тож ЄСПЛ ідентифікував низку важливих за даними обставинами справи факторів. Такі фактори включали, наприклад, обсяг моніторингу працівників роботодавцем та ступінь втручання у приватність працівника, наслідки для працівника, та чи надавалися належні гарантії. Крім того, національні органи мали забезпечити, щоб працівник, чия комунікація підлягала моніторингу, мав можливість захисту в суді, який би мав повноваження визначати, принаймні за суттю, як ті визначені критерії були дотримані та чи був оскаржуваний захід правомірним. У цій справі ЄСПЛ встановив порушення статті 8, оскільки національні органи не надали належного захисту праву заявника на повагу до приватного життя та кореспонденції і в результаті не встановили справедливий баланс між конфліктними інтересами.

Відповідно до **права ЄС** та **права РЄ** інформація містить дані про особу, якщо:

- особа є ідентифікованою або може бути ідентифікованою завдяки цій інформації;
- особа, хоча і не є ідентифікованою, однак може бути виокремлена завдяки цій інформації так, що за допомогою додаткового пошуку є можливість встановити, хто є суб'єктом персональних даних

Обидва види інформації захищені в однаковий спосіб відповідно до європейського права із захисту персональних даних. Пряма чи непряма можливість ідентифікації особи потребує постійної оцінки, «враховуючи наявні на час провадження технології та технологічні розробки»[152]. ЄСПЛ неодноразово заявляв, що поняття «персональні дані» відповідно до ЄКПЛ є таким як і в Конвенції 108, особливо щодо умов відносно ідентифікованої особи або особи, яку може бути ідентифіковано[153].

ЗРЗПД передбачає, що фізичну особу можна ідентифікувати, якщо її «можливо ідентифікувати, прямо чи опосередковано, зокрема, за такими показниками як ім'я/прізвище, ідентифікаційний номер, дані про місцезнаходження, онлайн-ідентифікатор, або за одним чи декількома факторами, що є

152 Загальний регламент захисту персональних даних, п. 26 преамбули.

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

визначальними для фізичної, фізіологічної, генетичної, розумової, економічної, культурної чи соціальної ідентичності такої фізичної особи»[154]. Таким чином, ідентифікація потребує елементів, які описують особу у такий спосіб, що її можливо відрізнити від всіх інших осіб та впізнати як індивіда. Ім'я/прізвище особи є першим прикладом таких елементів опису і може прямо ідентифікувати особу. У певних випадках інші характеристики можуть приводити до такого ж результату, уможливлюючи пряму ідентифікацію особи. Телефонний номер, номер соціального страхування та номерний знак автомобіля є прикладами інформації, яка може призвести до ідентифікації особи. Також можна використовувати такі атрибути, як комп'ютеризовані файли, файли *cookies* та засоби спостереження за веб-трафіком для того, щоб виокремити осіб через ідентифікацію їхньої поведінки та звичок. Як пояснюється у висновку Робочої групи «Стаття 29», «навіть без знання прізвища та адреси особи можливо віднести цю особу до певної категорії на підставі соціоекономічних, психологічних, філософських та інших критеріїв та приймати щодо неї певні рішення, оскільки її індивідуальна точка контакту (комп'ютер) більше не вимагає відкриття її ідентичності у вузькому сенсі»[155]. Визначення персональних даних як відповідно до права РЄ, так і відповідно до права ЄС є достатньо широким, щоб охопити всі можливості ідентифікації (та, таким чином, всі рівні можливої ідентифікації).

Приклад: у справі «*Музичні продюсери Іспанії (Promusicae) проти "Telefonica de Espana SAU"*»[156] СЄС вказав, що «безперечно, інформація про комунікацію, яку вимагала організація "Promusicae" щодо імен та адрес певних користувачів [певних інтернет-платформ обміну файлами] включає можливість отримання персональних даних, тобто інформації, що стосується ідентифікованої фізичної особи або фізичної особи, яку може бути ідентифіковано, відповідно до визначення статті 2 (a) Директиви 95/46 [станом на сьогодні стаття 4 (1) ЗРЗПД]. Ця комунікаційна інформація, як зазначила організація "Promusicae" та не заперечувалося компанією "Telefónica", становить обробку персональних даних»[157].

154 Загальний регламент захисту персональних даних, стаття 4 (1).

155 Робача група «Стаття 29» (2007), *Висновок 4/2007 про концепцію персональних даних*. РГ 136, від 20 червня 2007 р., с. 15.

156 Рішення Суду ЄС C-275/06, «Музичні продюсери Іспанії (Promusicae) проти "Telefonica de Espana SAU"» (*Productores de Música de España (Promusicae) v. Telefónica de España SAU),* [ВП], від 29 січня 2008р., п. 45.

157 Колишня Директива 95/46, стаття. 2 (b), тепер Загальний регламент захисту персональних даних, стаття 4 (2).

Приклад: «*"Scarlet Extended SA" проти Бельгійської асоціації авторів, композиторів та видавців (SABAM)*»[158] стосувалася відмови надавача інтернет-послуг «Scarlet» встановити систему фільтрів електронних комунікацій, які використовували програмне забезпечення обміну файлами, для попередження обміну файлами в порушення авторського права, захищеного SABAM, менеджерською компанією, яка представляє авторів, композиторів та видавців. СЄС вирішив, що IP-адреси користувачів є «захищеними персональними даними, оскільки вони дозволяють точно ідентифікувати цих користувачів».

Оскільки багато імен не є унікальними, встановлення ідентичності особи може вимагати додаткових характеристик для з'ясування того, що особа не є кимось іншим. Інколи прямі або непрямі характеристики можуть бути поєднані для ідентифікації особи, якої стосується ця інформація. Часто використовується дата та місце народження. Крім того, деякі держави запровадили персональні номери для кращого розрізнення громадян. Переміщені податкові дані[159], також дані, пов'язані з дозволом на проживання, які містяться в адміністративних документах[160], документи щодо банківських відносин та відносин з управління активами[161] можуть бути персональними даними. Такі біометричні дані, як відбитки пальців, цифрові фото або сканована сітківка ока, дані про місцезнаходження та онлайн-характеристики все більше використовуються для ідентифікації особи в наш час технологій.

Водночас для застосовності права із захисту персональних даних ЄС не потрібна фактична ідентифікація суб'єкта персональних даних, достатньо того, що зацікавлена особа може бути ідентифікованою. Особа вважається такою, яка може бути ідентифікована, якщо наявні достатні елементи, за допомогою яких особу можливо прямо або непрямо ідентифікувати[162]. Чи ймовірно, що

158 Рішення Суду ЄС, C-70/10, «"Scarlet Extended SA" проти Бельгійської асоціації авторів, композиторів та видавців (SABAM)», (*Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, від 24 листопада 2011р., п. 51.

159 Рішення Суду ЄС, C-201/14, «Смаранда Бара та інші проти Національного фонду медичного страхування та інших» (*Smaranda Bara and Others v. Casa Naţională de Asigurări de Sănătate and Others*), від 1 жовтня 2015 р.

160 Рішення Суду ЄС, об'єднані справи «YS проти Міністра з питань імміграції, інтеграції та притулку» та «Міністр з питань імміграції, інтеграції та притулку проти M. та S.» (*YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S*), від 17 липня 2014 р.

161 Рішеня ЄСПЛ у справі «M. N. та інші проти Сан-Марино» (*M.N. and Others v. San Marino*), № 28005/12, від 07 липня 2015 р.

162 Загальний регламент захисту персональних даних, стаття 4 (1).

існуватимуть достатні засоби для ідентифікації та використання їх передбачуваними користувачами, є визначальним критерієм відповідно до пункту 26 преамбули ЗРЗПД; це також включає інформацію, якою володіють треті особи-отримувачі (див. *розділ 2.3.2.*).

Приклад: місцева влада вирішила збирати дані про швидкість автомобілів на місцевих дорогах. Пристрої фотографували авто, автоматично фіксуючи час та місцезнаходження для передачі даних компетентному органу, щоб він міг накласти штраф на порушників правил з обмеження швидкості. Суб'єкти даних звернулись зі скаргою, стверджуючи, що місцева влада не має юридичних підстав для збору таких даних відповідно до закону про захист персональних даних. Місцева влада стверджувала, що вона не збирає персональні дані. Номерні знаки, як вони стверджували, є анонімізовані. Місцевий орган влади не мав жодних юридичних підстав для доступу до загального реєстру автомобілів для встановлення власника авто або його водія.

Це обґрунтування не відповідає пункту 26 преамбули ЗРЗПД. Враховуючи те, що метою збирання даних є потреба чітко ідентифікувати та оштрафувати порушників обмеження швидкості, можна передбачити, що ідентифікація буде досягнута. Хоча місцеві органи влади не мають засобів ідентифікації, які були б їм прямо доступні, вони передадуть дані компетентному органу, поліції, яка дійсно має такі засоби. Пункт 26 преамбули також явно передбачає сценарій, за яким існує можливість допускати, що подальші отримувачі, інші особи, ніж ті, що здійснюють негайне або перше використання даних, можуть спробувати ідентифікувати фізичну особу. Відповідно до пункту 26, дії органів місцевої влади прирівнювалися до збирання персональних даних щодо фізичної особи, яку можливо ідентифікувати, і, відповідно, вони повинні були мати юридичні підстави за законом про захист персональних даних.

Для «встановлення достатньої ймовірності використання засобів для ідентифікації фізичної особи, необхідно взяти до уваги всі об'єктивні фактори, якот витрати та період часу, необхідні для ідентифікації, враховуючи технології, наявні станом на момент обробки, і технологічні розробки»[163].

163 Там само, п. 26 преамбули.

Приклад: у справі «*Бреєр проти Федеративної Республіки Німеччини*»[164] СЄС розглянув поняття непрямої ідентифікації суб'єктів даних. Справа стосувалася динамічних IP-адрес, які постійно змінюються при новому підключенні до інтернету. Вебсайт, який адмініструвався федеральними німецькими установами, реєстрував та зберігав динамічні IP-адреси для попередження кібератак та ініціювання кримінальних проваджень у разі необхідності. Тільки провайдер інтернет-послуг, яким користувався пан Бреєр, мав додаткову інформацію, необхідну для його ідентифікації. СЄС вирішив, що динамічна IP-адреса, яка реєструється провайдером онлайн-медіа послуг у випадку під'єднання особи до відкритого для доступу провайдером вебсайту, є персональними даними, якщо третя сторона – у цьому випадку провайдер інтернет-послуг – має необхідні додаткові дані для ідентифікації особи[165]. СЄС зазначив, що для того, щоб інформація становила персональні дані, «немає необхідності, щоб уся інформація, яка уможливлює ідентифікацію суб'єкта даних, була в руках однієї особи». Користувачі динамічних IP-адрес, зареєстровані провайдером інтернет-послуг, можуть бути ідентифіковані в певних ситуаціях, наприклад, за допомогою інших осіб у ході кримінального провадження у випадку кібератак»[166]. Відповідно до позиції СЄС, коли провайдер «має юридичні засоби, які йому надають можливість ідентифікувати суб'єкта персональних даних за допомогою інших даних, які провайдер має про таку особу», це становить «засіб, який, імовірно, може бути використаний для ідентифікації суб'єкта даних». Відповідно, такі дані вважаються персональними даними.

У праві РЄ особа, яку можливо ідентифікувати, розуміється схожим чином. Пояснювальна записка до Оновленої Конвенції 108 містить схожий опис: поняття «можливо ідентифікувати» охоплює не тільки цивільну або юридичну ідентичність особи як таку, але й також те, що може дозволити персоніфікувати особу або виокремити її з-поміж інших і в результаті потенційно ставитись до неї по-іншому. Ця «персоніфікація» можлива, наприклад, через пряме

164 Рішення Суду ЄС C-582/14, «Патрік Бреєр проти Федеративної Республіки Німеччини» (*Patrick Breyer v. Bundesrepublik Deutschland)*, від 19 жовтня 2016 р., п. 43.

165 Колишня Директива Європейського парламенту та Ради від 24 жовтня 1995 року 95/46/ЕС про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних, стаття 2 (a).

166 Рішення Суду ЄС, C-70/10, «"Scarlet Extended SA" проти Бельгійської асоціації авторів, композиторів та видавців (SABAM)», (*Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, від 24 листопада 2011 р., пп. 47–48.

посилання на особу або на пристрій чи комбінацію пристроїв (комп'ютер, мобільний телефон, камеру, гральні пристрої тощо), які пов'язані з ідентифікаційним номером, псевдонімом, біометричними або генетичними даними, місцезнаходженням, IP-адресами або іншими ідентифікаторами[167]. Особа не вважається такою, яка «може бути ідентифікованою», якщо її або його ідентифікація вимагає багато часу, зусиль або ресурсів. Наприклад, це має місце, коли ідентифікація суб'єкта персональних даних вимагає надмірно складних, тривалих і дорогих операцій. Необґрунтованість часу, зусиль і ресурсів має бути оцінена в кожній індивідуальній справі з врахуванням таких факторів, як мета обробки, витрати на ідентифікацію та вигоди від неї, тип контролера та технології, які використовуються[168].

Щодо форми, у якій зберігаються або використовуються персональні дані, важливо зазначити, що це неважливо для застосовності права із захисту персональних даних. Письмове або усне спілкування може містити персональні дані, а також їх може містити зображення[169], включаючи відео[170] або аудіо[171] системи охоронного спостереження. Зафіксована електронними засобами та паперова інформація також можуть бути персональними даними. Навіть клітинні зразки людських тканин, які містять ДНК особи, можуть бути джерелом, з якого можуть бути вилучені біометричні дані[172], оскільки ці дані стосуються успадкованих або набутих генетичних характеристик, надають унікальну інформацію про здоров'я або фізіологію особи та можуть бути результатом аналізу біологічних зразків такої особи[173].

---

167 Пояснювальна записка до Оновленої Конвенції 108, п. 18.

168 Там само, п. 17.

169 Рішення ЄСПЛ у справі «Фон Ганновер проти Німеччини» (*Von Hannover v. Germany*), № 59320/00 від 24 червня 2004 р.; рішення ЄСПЛ у справі «Шякка проти Італії» (*Sciacca v. Italy*), № 50774/99 від 11 січня 2005 р.; рішення Суду ЄС, C-212/13, «Франтішек Ринеш проти Офісу захисту персональних даних» (*František Ryneš v. Úřad pro ochranu osobních údajů*), від 11 грудня 2014 р.

170 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» (*Köpke v. Germany*), № 420/07 від 5 жовтня 2010 р.; ЄІЗПД (2010), Посібник ЄДПС з питань відеоспостереження (*The EDPS video-surveillance guidelines*), від 17 березня 2010 р.

171 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 «Віс проти Франції» (*Wisse v. France*), № 71611/01 від 20 грудня 2005 р. (французькою мовою).

172 Робоча група «Стаття 29» (2007), Висновок 4/2007 про концепцію персональних даних. (*Opinion 4/2007 on the concept of personal data*) РГ 136, від 20 червня 2007 р., с. 9; Рада Європи, Рекомендація Комітету міністрів Rec. (2006)4 про дослідження біологічних матеріалів людського походження (*Recommendation No. Rec(2006)4 of the Committee of Ministers to member states on research on biological materials of human origin*), від 15 березня 2006 р.

173 Загальний регламент захисту персональних даних, стаття 4 (13).

Знеособлення (анонімізація)

Відповідно до принципу обмеження зберігання даних, що передбачається як ЗРЗПД, так й Оновленою Конвенцією 108 (більш детально описаного у главі 3), дані мають зберігатись «у формі, яка дозволяє ідентифікацію суб'єкта персональних даних не довше, ніж це необхідно для цілей, заради яких вони оброблялись»[174]. Відповідно, дані мають бути видалені або знеособлені, якщо контролер хоче зберігати їх після того, як вони вже більше не потрібні або більше не служать початковій меті.

Процес знеособлення даних означає, що всі елементи ідентифікації вилучено з набору персональних даних такою мірою, що суб'єкт даних вже більш не може бути ідентифікованим[175]. У своєму Висновку № 05/2014 Робоча група «Стаття 29» аналізувала ефективність та обмеження різних технік знеособлення[176]. У висновку визнавалася потенційна цінність таких технік, однак підкреслювалося, що певні підходи не обов'язково працюють у всіх справах. Для того, щоб віднайти оптимальне рішення конкретній ситуації, рішення щодо належного процесу знеособлення має бути прийнято з урахування індивідуальних обставин. Незалежно від того, яка техніка використовується, неможливість ідентифікації має бути забезпечена безповоротно. Це означає, що для знеособлення даних, не може бути залишено жодного елементу в інформації, який шляхом докладення певних зусиль міг би допомогти повторно ідентифікувати зацікавлену особу або осіб[177]. Ризик повторної ідентифікації може бути оцінений, беручи до уваги «час, зусилля або ресурси, необхідні з огляду на характер даних, контекст їх використання, наявних технологій повторної ідентифікації та відповідних витрат»[178].

Якщо дані успішно знеособлено, вони більше не є персональними та законодавство із захисту персональних даних більше не застосовується.

ЗРЗПД передбачає, що особа або організація, яка контролює обробку персональних даних, не може бути зобов'язана зберігати, набувати або обробляти додаткову інформацію для ідентифікації суб'єкта персональних даних лише

174 Там само, стаття 5 (1) (e); Оновлена Конвенція 108, стаття 5 (4) (e).

175 Загальний регламент захисту персональних даних, п. 26 преамбули.

176 Робоча група «Стаття 29» (2014), Висновок 05/2014 щодо технік анонімізації (*Opinion 05/2014 on Anonymization Techniques*), РГ 216, від 10 квітня 2014 р.

177 Загальний регламент захисту персональних даних, п. 26 преамбула.

178 Рада Європи, Комітет Конвенції 108 (2017), Посібник із захисту осіб щодо обробки персональних даних у світі Великих даних (*Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*), від 23 січня 2017 р., п. 6.2.

з метою дотримання правил. Водночас це правило має важливий виняток: як тільки суб'єкт персональних даних для цілей реалізації права на доступ, виправлення, видалення, обмеження обробки та можливість переміщення даних надає контролеру додаткову інформацію, яка уможливлює ідентифікацію, тоді дані, які до цього були знеособлені, стають персональними даними знову[179].

Псевдонімізація

У персональній інформації є такі ідентифікатори, як ім'я, дата народження, стать і адреса або інші елементи, які можуть призвести до ідентифікації. Процес псевдонімізації персональних даних означає, що ці елементи замінюються псевдонімом.

Право ЄС визначає «псевдонімізацію» як «обробку персональних даних у такий спосіб, що персональні дані більше не можна віднести до конкретного суб'єкта даних без використання додаткової інформації, за умови, що таку додаткову інформацію зберігають окремо, і на неї поширюється застосування технічних і організаційних інструментів для забезпечення того, що персональні дані не стосуються фізичної особи, яку ідентифіковано чи можна ідентифікувати»[180]. На відміну від анонімізованих даних, псевдонімізовані дані ще залишаються персональними даними та, відповідно, на них поширюється законодавство про захист персональних даних. Хоча псевдонімізація може зменшити ризик для суб'єктів персональних даних, вона не виключена з-під сфери ЗРЗПД.

ЗРЗПД визнає різні сфери застосування псевдонімізації як належний технічний засіб для підсилення захисту персональних даних, також окремо наголошується, що це є засобом організації та захисту обробки персональних даних[181]. Це є також належним запобіжником, що може бути використаний для обробки персональних даних в інших цілях, ніж ті, для яких вони початково були зібрані[182].

Псевдонімізація безпосередньо не вказується в юридичних визначеннях Оновленої Конвенції 108 **РЄ**. Однак пояснювальна записка до Оновленої Конвенції 108 чітко вказує, що «використання псевдонімів або будь-яких

179 Загальний регламент захисту персональних даних, стаття 11.

180 Там само, стаття 4 (5).

181 Там само, стаття 25 (1).

182 Там само, стаття 6 (4).

цифрових ідентифікаторів/цифрової ідентичності не призводить до анонімізації персональних даних, оскільки залишається можливість ідентифікувати суб'єкта даних або індивідуалізувати його»[183]. Одним із способів псевдонімізації даних є їх шифрування. Якщо дані були псевдонімізовані, зв'язок з ідентичністю існує у формі псевдоніма плюс ключа дешифрування. Без такого ключа складно ідентифікувати псевдоніми даних. Водночас для тих, хто має ключ дешифрування, повторна ідентифікація можлива без будь-яких труднощів. Необхідно особливо стежити, щоб ключ дешифрування не використовувався неуповноваженими особами. Таким чином, «дані-псевдоніми [...] вважаються персональними даними [...]», які охоплюються Оновленою Конвенцією 108[184].

Автентифікація

Це процедура, за допомогою якої особа може підтвердити, що вона володіє певною ідентичністю та/або уповноважена на здійснення певних дій, таких як вхід на територію, що охороняється, або зняття грошей з банківського рахунку. Автентифікація може бути досягнута шляхом порівняння біометричних даних, таких як фото або відбитки пальців у паспорті при проходженні суб'єктом персональних даних, наприклад, паспортного контролю[185]; або шляхом пропозиції надати інформацію, яка має бути відома тільки особі з відповідною ідентичністю або дозволом, наприклад особистий ідентифікаційний номер (PIN) або пароль; або через надання певного знака (ключа), володіти яким може лише особа з певною ідентичністю або дозволом, як-от спеціальна картка-чіп або ключ від банківського сейфа. Крім пароля або карток-чипів, електронні підписи, інколи разом із PIN, можуть бути спеціальними інструментами для ідентифікації або автентифікації особи в електронній комунікації.

2.1.2 Особливі категорії персональних даних

Відповідно до права ЄС та **права РЄ** існують особливі категорії персональних даних, обробка яких, з огляду на їхню природу, може становити ризик для суб'єкта персональних даних при обробці. Вони вимагають особливого захисту. До таких даних застосовується принцип заборони обробки, та існує обмежена кількість умов, за яких така обробка вважається правомірною.

183 Пояснювальна записка до Оновленої Конвенції 108, п. 18.

184 Там само.

185 Там само, пп. 56–57.

Відповідно до Оновленої Конвенції 108 (стаття 6) та ЗРЗПД (стаття 9) наступні категорії вважаються чутливими даними:

- персональні дані, які вказують на расу та етнічне походження;
- персональні дані, які вказують на політичні погляди, релігійні та інші переконання, включаючи філософські переконання;
- персональні дані, які вказують на членство в профспілці
- генетичні дані та біометричні дані, які обробляються для цілей ідентифікації особи;
- персональні дані щодо стану здоров'я, сексуального життя або сексуальної орієнтації.

Приклад: справа «*Боділ Ліндквіст*»[186] стосувалася посилання на різних осіб, шляхом зазначення їхніх імен або іншим чином, наприклад шляхом зазначення їхніх телефонних номерів або інформації про їхні звички на вебсторінці. Суд ЄС вирішив, що «посилання на той факт, що особа травмувала ногу і працює за медичними показаннями скорочений день, становить персональні дані щодо стану здоров'я»[187].

Персональні дані про судимість і злочини

Оновлена Конвенція 108 включає персональні дані про судимість і злочини або пов'язані заходи безпеки до списку особливих категорій персональних даних[188]. ЗРЗПД не включає дані про судимість і злочини або пов'язані питання безпеки до списку особливих категорій персональних даних, однак про них йдеться в окремій статті. Стаття 10 ЗРЗПД передбачає, що обробка таких даних може здійснюватись виключно «під контролем офіційного органу або у разі, якщо обробка дозволена законодавством Союзу або держави-члена, що передбачають належні гарантії для прав і свобод суб'єктів даних». Будь-який комплексний реєстр, що містить дані про судимості, необхідно вести лише під контролем офіційного органу[189]. У ЄС обробку персональних даних у кон-

186 Суд ЄС, C-101/01, Кримінальне провадження проти Bodil Lindqvist (*Criminal proceedings against Bodil Lindqvist*), від 6 листопада 2003 р., п. 51.

187 Колишня Директива 95/46/ЄС, стаття 8 (1), тепер Загальний регламент захисту персональних даних, стаття 9 (1).

188 Оновлена Конвенція 108, стаття 6 (1).

189 Загальний регламент захисту персональних даних, стаття 10.

тексті діяльності правоохоронних органів регулює спеціальний правовий акт Директива 2016/680/ЄС[190]. Директива передбачає спеціальні правила для захисту даних, які є обов'язковими для компетентних органів при обробці персональних даних з метою попередження, розслідування, виявлення кримінальних правопорушень та переслідування за їх вчинення (див. *розділ 8.2.1.*).

2.2 Обробка даних

Ключові моменти

- «Обробка даних» стосується будь-яких операцій, які здійснюються із персональними даними.
- Поняття «обробка» охоплює автоматичну та не автоматичну обробку.
- Відповідно до права ЄС «обробка» також включає обробку структурованих картотек даних вручну.
- Відповідно до права РЄ значення поняття «обробка» може бути розповсюджене національним законом на обробку ручними засобами.

2.2.1 Концепція обробки персональних даних

Концепція обробки персональних даних, відповідно як до права ЄС, так і до права РЄ, є комплексною: «"обробка персональних даних" [...] означає будь-яку операцію, здійснювану з персональними даними [...] такі, як збір, реєстрація, організація, структурування, зберігання, адаптація чи зміна, пошук, ознайомлення, використання, розкриття через передавання, розповсюдження чи надання іншим чином, упорядкування чи комбінування, обмеження, видалення чи знищення»[191]. Оновлена Конвенція 108 додає до визначення збереження персональних даних[192].

190 Директива Європейського Парламенту та Ради (ЄС) 2016/680 27 квітня 2016 р. про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами влади в цілях попередження, розслідування, виявлення кримінальних правопорушень та притягнення до відповідальності за їх вчинення або виконання кримінальних покарань та про вільне переміщення таких даних та скасування Рамкового рішення Ради 2008/977/JHA, OJ 2016 L 119.

191 Загальний регламент захисту персональних даних, стаття 4 (2). Див. також Оновлену Конвенцію 108, стаття 2 (b).

192 Оновлена Конвенція 108, стаття 2 (b).

Приклад: у справі «*Франтішек Ринеш*»[193] пан Ринеш за допомогою домашньої системи ТВ-спостереження записав зображення двох осіб, які розбили вікна в його будинку. СЄС вирішив, що відеонагляд, включно із записом та збереженням персональних даних, становить автоматичну обробку даних, яка охоплюється законодавством із захисту персональних даних ЄС.

Приклад: у справі *«Торгово-промислова та сільськогосподарська палата м. Лечче проти Сальваторе Манні»*[194] пан Манні вимагав вилучити його персональні дані з реєстру рейтингової компанії, які пов'язували його з ліквідацією підприємства з нерухомості і, відповідно, мали негативний вплив на його репутацію. СЄС вирішив, що «розшифровуючи та зберігаючи таку інформацію в реєстрі та надаючи доступ для ознайомлення у разі необхідності на запит третім сторонам, органи влади, відповідальні за ведення реєстру, здійснюють "обробку персональних даних", відносно якої вони є "контролерами"».

Приклад: роботодавці збирають та обробляють дані про своїх працівників, включаючи інформацію стосовно їхніх зарплат. Їхні трудові договори є юридичної підставою для правомірності таких дій.

Роботодавці далі мають передати відомості про заробітну плату працівників податковим органам. Така передача також становитиме «обробку» в сенсі цього поняття за Оновленою Конвенцією 108 та ЗРЗПД. Однак для такого відкриття даних трудовий договір вже не є юридичною підставою. Мають існувати додаткові юридичні підстави для операцій з обробки, які в результаті призводять до передачі даних про заробітню плату працівників до податкових органів. Як правило, юридична підстава для такої обробки міститься в національних законах про податки. Без таких положень та за відсутності будь-яких інших підстав для обробки така передача персональних даних буде незаконною обробкою.

193 Рішення Суду ЄС, C-212/13, «Франтішек Ринеш проти Офісу захисту персональних даних» (*František Ryneš v. Úřad pro ochranu osobních údajů*), від 11 грудня 2014 р., п. 25.

194 Рішення Суду ЄС, C-398/15, «Торгово-промислова та сільськогосподарська палата м. Лечче проти Сальваторе Манні», (*Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*), від 9 березня 2017 р., п. 35.

2.2.2 Автоматизована обробка даних

Правила захисту персональних даних відповідно до Оновленої Конвенції 108 та ЗРЗПД повністю застосовуються до автоматизованої обробки даних.

Відповідно до **права ЄС** автоматизована обробка даних стосується операцій, здійснених «щодо персональних даних повністю або частково автоматизованими засобами»[195]. Оновлена Конвенція 108 містить подібне визначення[196]. У практичному вимірі це означає, що будь-яка обробка персональних даних за допомогою автоматизованих засобів, наприклад, персонального комп'ютера, мобільного додатку або роутера охоплюється як правилами захисту персональних даних ЄС, так і правилами РЄ.

Приклад: справа «*Боділ Ліндквіст*»[197] стосувалася посилання на веб-сторінці на різних осіб шляхом зазначення їхніх імен або іншим чином, наприклад шляхом зазначення їхніх телефонних номерів або інформації про їхні хобі. СЄС вирішив, що «дія у формі посилання на інтернет-сторінці на різних осіб та їх ідентифікація за ім'ям або іншими засобами, наприклад, надаючи їхні номери телефонів або інформацію щодо робочих умов або хобі, становить «обробку персональних даних повністю або частково автоматизованими засобами» в сенсі статті 3 (1) Директиви 95/46[198].

Приклад: у справі «*"Google Spain SL", "Google Inc." проти Іспанського агентства захисту даних (AEPD) та Маріо Костеха Гонсалеса*»[199] пан Гонсалес вимагав прибрати або змінити зв'язок між його ім'ям у пошуковій системі Google та двома газетними сторінками, у яких оголошувався аукціон нерухомості для стягнення боргів у системі соціального страхування. СЄС встановив, що «досліджуючи інтернет автоматично, постійно та систематично у пошуку інформації, яку там опубліковано, постачальник пошукових систем «збирає» такі дані, які в подальшому він «витягує», «записує» та «організовує» в межах своїх програм індексації,

195 Загальний регламент захисту персональних даних, стаття 2 (1) та 4 (2).

196 Оновлена Конвенція 108, стаття 2 (b) та (c); Пояснювальна записка до Оновленої Конвенції 108, п. 21.

197 Суд ЄС, C-101/01, Кримінальне провадження проти Bodil Lindqvist (*Criminal proceedings against Bodil Lindqvist*), від 6 листопада 2003 р., п. 27.

198 Загальний регламент захисту персональних даних, стаття 2 (1).

199 Рішення Суду ЄС, C-131/12, «"Google Spain SL", "Google Inc." проти Іспанського агентства захисту даних (AEPD) та Маріо Костеха Гонсалеса» (*Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*), [ВП], від 13 травня 2014 р.

«зберігає» на своїх серверах і, за певних обставин, «відкриває» або «робить доступними» його користувачам у формі результатів у пошуковому списку[200]. СЄС дійшов висновку, що такі дії становлять «обробку» «незалежно від того, що постачальник пошукових систем здійснює такі самі операції щодо інших типів інформації та не розрізняє між такою інформацією та персональними даними».

2.2.3 Неавтоматизована обробка даних

Процедура ручної обробки даних також потребує захисту персональних даних.

Відповідно до **права ЄС** захист персональних даних жодним чином не зводиться до автоматизованої обробки. Тому у праві ЄС захист даних застосовується до обробки персональних даних, які зберігаються в неавтоматизованій картотеці, тобто у спеціально структурованій паперовій картотеці[201]. Структурована картотека організовує за категоріями набори персональних даних, таким чином роблячи їх доступними за певними критеріями. Наприклад, якщо роботодавець зберігає паперовий файл під назвою «відпустка працівника», який містить усі деталі відпусток працівників за останній рік в алфавітному порядку, файл буде становити неавтоматизовану картотеку, яка підпадає під правила захисту персональних даних ЄС. Причиною такого розширення сфери дії захисту даних є те, що:

- паперові картотеки структуровано у спосіб, який пришвидшує і полегшує пошук інформації;
- зберігання персональних даних у структурованих паперових картотеках допомагає обійти обмеження, які стосуються процесу автоматизованої обробки даних[202].

У визначенні поняття «автоматизована обробка» у **праві РЄ** визнається, що між автоматизованими операціями може виникати потреба в застосуванні певних етапів ручної обробки персональних даних[203]. Стаття 2 (c) Оновленої Конвенції 108 вказує, що «у випадках, коли не використовується автоматизована обробка, обробка даних означає операцію або набір операцій, що виконуються стосовно персональних даних у структурованому наборі таких даних, які є доступними або такими, які можна отримати відповідно до чітких критеріїв».

200 Там само, п. 28.

201 Загальний регламент захисту персональних даних, стаття 2 (1).

202 Загальний регламент захисту персональних даних, п. 15 преамбули.

203 Оновлена Конвенція 108, стаття 2 (b) та (c).

2.3 Користувачі персональних даних

Ключові моменти

- Той, хто визначає засоби та цілі обробки персональних даних інших осіб, є «контролером» відповідно до законодавства про захист персональних даних; якщо таке рішення приймається декількома особами, вони можуть бути «спільними контролерами».
- «Оператор» – це фізична або юридична особа, яка обробляє персональні дані від імені контролера.
- Оператор стає контролером, якщо він або вона самостійно визначає засоби або цілі обробки даних.
- Будь-яка особа, якій відкриваються персональні дані, є «одержувачем».
- Третя особа – це фізична або юридична особа, крім суб'єкта персональних даних, контролера, оператора, а також інших осіб, які уповноважені обробляти персональні дані під безпосереднім керівництвом такого контролера або оператора.
- Згода на обробку персональних даних як юридична підстава для обробки персональних даних є будь-яке вільне, чітке, поінформоване та однозначне волевиявлення суб'єкта персональних даних, виражене у формі заяви та/або чіткої стверджувальної дії, яким він дозволяє обробку своїх персональних даних.
- Обробка особливих категорій даних на підставі згоди вимагає ясно висловленої згоди.

2.3.1 Контролери та оператори

Найбільш важливим наслідком роботи контролера або оператора є правова відповідальність за дотримання передбачених законодавством про захист персональних даних відповідних зобов'язань. У приватному секторі це зазвичай фізична або юридична особа; у державному – орган. Існує значна різниця між контролером даних та оператором даних: перший – фізична або юридична особа, яка визначає цілі та засоби обробки, другий – фізична або юридична особа, яка здійснює обробку даних від імені контролера відповідно до чітких інструкцій. За загальним правилом, саме контролер має здійснювати контроль над обробкою та нести відповідальність за це, включно з юридичною відповідальністю. Однак, згідно з реформою правил захисту персональних даних зараз оператор має обов'язок дотримуватися багатьох вимог,

які застосовуються до контролера. Наприклад, відповідно до ЗРЗПД оператори мають вести запис усіх видів діяльності з обробки даних, щоб продемонструвати дотримання своїх обов'язків за регламентом[204]. Від операторів також вимагається вживати необхідних технічних і організаційних заходів для забезпечення безпеки обробки[205], за певних умов призначити спеціаліста із захисту персональних даних[206] та повідомляти контролера про витік[207].

Чи має особа можливість вирішувати і визначати мету та засоби обробки, буде залежати від фактичних елементів або обставин справи. Відповідно до визначення контролера, наданого в ЗРЗПД, фізична особа, юридична особа або інший орган можуть бути контролером. Водночас Робоча група «Стаття 29» підкреслила, що для забезпечення особам більш стабільної основи для реалізації їхніх прав «перевага при визначенні контролером має надаватися компанії або органу, а не окремій особі в компанії або органі»[208]. Наприклад, компанія, яка продає медичні товари спеціалістам, є контролером створення та ведення переліку спеціалістів, яким надходить продукція в певних сферах, контролером не є менеджер з продажу, який фактично використовує та веде цей перелік.

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

Фізичні особи можуть бути контролерами як відповідно до права ЄС, так і права РЄ. Втім, коли мова йде про обробку даних інших осіб виключно стосовно їхньої особистої або побутової діяльності, фізичні особи не підпадають під сферу дії правил ЗРЗПД та Оновленої Конвенції 108 та не вважаються контролерами[209]. Фізична особа, яка веде свою кореспонденцію,

204 Загальний регламент захисту персональних даних, стаття 30 (2).

205 Там само, стаття 32.

206 Там само, стаття 37.

207 Там само, стаття 33 (2).

208 Робоча група «Стаття 29» (2010), *Висновок 1/2010 про поняття «контролер» та «оператор»*, РГ 169, Брюссель, від 16 лютого 2010 р.

209 Загальний регламент захисту персональних даних, п. 18 преамбули та стаття 2 (2) (c); Оновлена Конвенція 108, стаття 3 (2).

особистий щоденник, описуючи в ньому події з друзями та колегами, та записи щодо стану здоров'я членів сім'ї, може бути виключена з-під дії правил захисту персональних даних, оскільки ця діяльність може бути виключно особистою та побутовою. ЗРЗПД далі зазначає, що особиста та побутова діяльність також може включати соціальні контакти та діяльність в інтернеті, якщо вона здійснюється в контексті такої діяльності[210]. На противагу цьому, правила захисту персональних даних повністю застосовуються до контролерів та операторів, які надають засоби для обробки персональних даних в особистій або побутовій діяльності (наприклад, платформи соціальних мереж)[211].

Доступ громадян до інтернету та можливість використання платформ електронної комерції, соціальних мереж та сайтів блогів для поширення особистої інформації про себе або інших фізичних осіб призводить до все складнішого відокремлення особистої обробки інформації від неособистої[212]. Чи є діяльність виключно особистою чи побутовою, залежить від обставин[213]. Діяльність, яка має професійний або комерційний аспект, не може вважатися винятком, яким є побутова діяльність[214]. Таким чином, якщо масштаб та частота обробки даних передбачає професійну діяльність або повну зайнятість, приватна особа може вважатися контролером. Чи відкриваються персональні дані великій кількості людей, які вочевидь не входять до приватного кола даної особи, є ще одним фактором, який має братися до уваги, крім професійного або комерційного характеру діяльності. Практика застосування Директиви про захист персональних даних свідчить, що законодавство про захист персональних даних застосовується у випадку, коли приватна особа, використовуючи інтернет, публікує дані про інших осіб на публічному вебсайті. СЄС поки не вирішував схожі питання за ЗРЗПД, що надає більш детальні рекомендації з питань, на які не поширюється законодавство із захисту персональних даних через належність до «побутових винятків» таких, як використання соціальних мереж в особистих цілях.

---

210 Загальний регламент захисту персональних даних, п. 18 преамбули.

211 Там само, п. 18 преамбули; Пояснювальна записка до Оновленої Конвенції 108, п. 29.

212 Див. позицію Робочої групи «Стаття 29» щодо обговорення пакету реформ у сфері захисту персональних даних (2013), *Додаток 2: Пропозиції та зміни щодо винятку для особистої чи побутової діяльності*, від 27 лютого 2013 р.

213 Пояснювальна записка до Оновленої Конвенції 108, п. 28.

214 Див. Загальний регламент захисту персональних даних, п. 18 преамбули та Пояснювальну записку до Оновленої Конвенції 108, п. 27.

Приклад: справа «*Боділ Ліндквіст*»[215] стосувалася посилання на вебсторінці на імена різних осіб або іншим чином, наприклад на їхні телефонні номери або інформацію про їхні хобі. СЄС вирішив, що «посилання на інтернет-сторінці на різних осіб та їхня ідентифікація за іменем або за допомогою інших засобів [...] становить процес "обробки персональних даних за допомогою повного чи часткового використання автоматизованих засобів"» у розумінні статті 3 (1) Директиви про захист персональних даних[216].

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, що, безумовно, не так у випадку обробки персональних даних, які містяться в інтернет-публікації і є доступними для невизначеного кола осіб»[217].

Відповідно до практики СЄС за певних обставин візуальні записи приватної охоронної камери також можуть охоплюватися законодавством із захисту персональних даних ЄС.

Приклад: у справі «*Франтішек Ринеш*»[218] пан Ринеш за допомогою домашньої системи ТВ-спостереження записав зображення двох осіб, які розбили вікна в його будинку. Далі запис було передано поліції, на нього здійснювалось посилання протягом кримінального провадження.

СЄС вирішив, що «в тій мірі, в якій відео спостереження [...] навіть частково охоплює публічний простір і, відповідно, спрямоване за межі приватного середовища особи, яка обробляє дані у такий спосіб, воно не може вважатись діяльністю, яка є виключно "особистою або побутовою"[...]»[219].

215 Суд ЄС, C-101/01, Кримінальне провадження проти Bodil Lindqvist (*Criminal proceedings against Bodil Lindqvist*), від 6 листопада 2003 р.

216 Там само, п. 27; Колишня Директива 95/46/ЄС, стаття 3 (1), тепер Загальний регламент захисту персональних даних, стаття 2 (1).

217 Суд ЄС, C-101/01, Кримінальне провадження проти Bodil Lindqvist (*Criminal proceedings against Bodil Lindqvist*), від 6 листопада 2003 р., п. 47.

218 Рішення Суду ЄС, C-212/13, «Франтішек Ринеш проти Офісу захисту персональних даних» (*František Ryneš v. Úřad pro ochranu osobních údajů*), від 11 грудня 2014 р., п. 33.

219 Колишня Директива 95/46/ЄС, стаття 3 (2), тепер Загальний регламент захисту персональних даних, стаття 2 (2) (c).

Контролер

У **праві ЄС** «контролер» – це той, «хто окремо чи разом з іншими визначає мету і засоби обробки персональних даних»[220]. Контролер вирішує, чому і як персональні дані оброблятимуться.

У **праві РЄ** Оновлена Конвенція 108 визначає «контролера» як фізичну або юридичну особу, орган влади, службу, установу чи будь-який інший орган (установу), що самостійно або спільно з іншими має право приймати рішення щодо обробки даних[221]. Таке право вирішувати стосується цілей та засобів обробки, а також категорій даних, які мають оброблятись, та питань доступу до даних[222]. Чи ґрунтується таке право на законодавстві або випливає із фактичних обставин, має вирішуватись у кожній конкретній справі в залежності від обставин[223].

Приклад: справа «*Google Spain*»[224] була ініційована громадянином Іспанії, який вимагав видалити з пошукової системи Google посилання на старі газетні публікації щодо його фінансової історії.

СЄС мав вирішити, чи є «Google» як оператор пошукової системи контролером персональних даних у розумінні статті 2 (d) Директиви про захист персональних даних[225]. СЄС вирішив, що поняття «контролер» має тлумачитися широко для забезпечення «ефективного та повного захисту суб'єкта персональних даних»[226]. СЄС дійшов висновку, що оператор інформаційно-пошукової системи визначає цілі та засоби діяльності та робить інформацію, завантажену видавцями на інтернет-сторінки, доступною для будь-якого інтернет-користувача, який здійснює пошук через

220 Загальний регламент захисту персональних даних, стаття 4 (7).

221 Оновлена Конвенція 108, стаття 2 (d).

222 Пояснювальна записка до Оновленої Конвенції 108, п. 22.

223 Там само.

224 Рішення Суду ЄС, C-131/12, «"Google Spain SL", "Google Inc." проти Іспанського агентства захисту даних (AEPD) та Маріо Костеха Гонсалеса» (*Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*), [ВП], від 13 травня 2014 р.

225 Загальний регламент захисту персональних даних, стаття 4 (7); Рішення Суду ЄС, C-131/12, «"Google Spain SL", "Google Inc." проти Іспанського агентства захисту даних (AEPD) та Маріо Костеха Гонсалеса» (*Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*) [ВП], від 13 травня 2014 р., п. 21.

226 Рішення Суду ЄС, C-131/12, «"Google Spain SL", "Google Inc." проти Іспанського агентства захисту даних (AEPD) та Маріо Костеха Гонсалеса» (*Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*), [ВП], від 13 травня 2014 р., п. 34.

ім'я суб'єкта персональних даних[227]. Відповідно, СЄС вирішив, що «Google» може вважатися «контролером»[228].

Коли контролер або оператор зареєстровані поза межами ЄС, така компанія повинна в письмовій формі призначити представника в межах ЄС[229]. ЗРЗПД підкреслює, що представник «повинен мати осідок в одній з держав-членів, де перебувають суб'єкти даних, чиї персональні дані опрацьовують у зв'язку з постачанням їм товарів чи послуг, або чию поведінку моніторять»[230]. Якщо представника не призначено, до контролера або оператора все одно може бути пред'явлено судовий позов[231].

Спільне контролювання

ЗРЗПД передбачає, що якщо цілі та засоби обробки персональних даних визначаються двома або більше контролерами спільно, вони вважаються спільними контролерами. Це означає, що вони вирішують разом обробляти персональні дані для спільних цілей[232]. Пояснювальна записка до Оновленої Конвенції 108 також вказує на можливість існування множинного контролера або співконтролювання в нормативно-правових **документах РЄ**[233].

Робоча група «Стаття 29» вказує, що спільне контролювання може мати різні форми, і що участь різних контролерів у контрольній діяльності може бути не рівною[234]. Така гнучкість уможливлює реагування на все складніші реалії обробки персональних даних[235]. Спільні контролери повинні визначити свою відповідальність за дотримання обов'язків, вказаних у регламенті, у відповідній спеціальній угоді[236].

227 Там само, пп. 35–40.

228 Там само, пп. 41.

229 Загальний регламент захисту персональних даних, стаття 27 (1).

230 Там само, стаття 27 (3).

231 Там само, стаття 27 (5).

232 Там само, стаття 4 (7) та стаття 26.

233 Оновлена Конвенція 108, стаття 2 (d); Пояснювальна записка до Оновленої Конвенції 108, п. 22.

234 Робоча група «Стаття 29» (2010), *Висновок 1/2010 про поняття «контролер» та «оператор»*, РГ 169, Брюссель, від 16 лютого 2010 р.

235 Там само.

236 Загальний регламент захисту персональних даних, п. 79 преамбули.

Спільне контролювання призводить до спільної відповідальності за дії з обробки[237]. У межах **законодавства ЄС** це означає, що кожен контролер або оператор може бути притягнутий до відповідальності за всю можливу шкоду, завдану обробкою даних під спільним контролюванням, для забезпечення ефективної компенсації суб'єкту персональних даних[238].

Приклад: база даних клієнтів неплатників, яка ведеться спільно кількома кредитними установами, є розповсюдженим прикладом такого спільного контролювання. Коли хтось звертається по кредит до банку, який є одним з контролерів, банк перевіряє базу даних, щоб прийняти поінформоване рішення щодо кредитоспроможності заявника.

У юридичних документах прямо не зазначено, чи потребує спільне контролювання наявності загальної мети для всіх контролерів, чи досить того, що їхня мета лише частково співпадає. На жаль, на європейському рівні поки немає відповідної судової практики з цього питання. У висновку 2010 року щодо контролерів та операторів Робоча група «Стаття 29» заявила, що спільні контролери можуть поділяти всі цілі та засоби обробки або поділяти тільки певні цілі чи засоби або їхню частину[239]. Перший варіант означатиме дуже тісні стосунки між різними учасниками, другий – менш тісні.

Робоча група «Стаття 29» виступає за більш широке тлумачення поняття «спільне контролювання», яке б додало деякої гнучкості у реагування на все складнішу реальність обробки персональних даних[240]. Справа «Спільноти всесвітніх міжбанківських фінансових телекомунікацій (SWIFT)» доводить позицію робочої групи.

Приклад: у так званій справі «*СВІФТ*» європейські банківські установи користувалися системою СВІФТ (спочатку як оператора) для управління передачею даних у ході банківських операцій. Не маючи прямої вказівки європейських банківських установ, які наймали цю спільноту, СВІФТ розкрив Міністерству фінансів США інформацію про банківську трансакцію, що

237 Там само, п. 21.

238 Там само, стаття 82 (4).

239 Робоча група «Стаття 29» (2010), *Висновок 1/2010 про поняття «контролер» та «оператор»,* РГ 169, Брюссель, від 16 лютого 2010 р., с 19.

240 Там само.

зберігалася в обчислювальному сервісному центрі в Сполучених Штатах Америки (США). Робоча група «Стаття 29», оцінюючи законність цієї ситуації, дійшла висновку, що європейські банківські установи, які користувалися системою СВІФТ, а також саму спільноту СВІФТ слід було б вважати спільними контролерами, які б несли відповідальність перед європейськими клієнтами за розкриття органам влади США їхніх персональних даних[241].

Оператор

Відповідно до **законодавства ЄС** оператор – це той, хто здійснює обробку персональних даних від імені контролера[242]. Доручена оператору діяльність може бути обмежена дуже конкретним завданням чи контекстом або може бути досить загальною і широкою. У **нормативно-правових документах РЄ** визначення «оператор» має те ж саме значення, що й у законодавстві ЄС[243].

Окрім обробки персональних даних для третіх осіб оператори також мають право бути контролерами персональних даних у зв'язку з обробкою, яку 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 оператором обробки. Якщо ж «Евереді» обробляє дані своїх власних співробітників, тоді вона – контролер персональних даних для здійснення своїх зобов'язань як роботодавця.

Зв'язок між контролером та оператором

Як можна побачити, контролер – це той, хто визначає цілі та засоби обробки. ЗРЗПД чітко встановлює, що оператор може обробляти дані лише за дорученням контролера, якщо тільки законодавство ЄС або держави-члена не

241 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.

242 Загальний регламент захисту персональних даних, стаття 4 (8).

243 Оновлена Конвенція 108, стаття 2 (f).

уповноважує оператора це робити[244]. Угода між контролером та оператором є важливим елементом їхніх відносин та юридичною вимогою[245].

Приклад: директор компанії «Саншайн» вирішує, що компанія «Клауд», яка є спеціалістом з питань хмарних сервісів для збереження даних, має управляти даними клієнтів компанії «Саншайн». Компанія «Саншайн» залишається контролером, а «Клауд» – лише оператором, оскільки у відповідності до угоди «Клауд» може використовувати дані про клієнтів компанії «Саншайн» тільки для цілей, які визначить «Саншайн».

Якщо право визначати засоби обробки делегуються оператору, контролер тим не менш має бути здатним здійснювати належний рівень контролю за рішеннями оператора щодо засобів обробки. Загальна відповідальність залишається на контролерові, який має наглядати за операторами для забезпечення відповідності їхніх рішень законодавству із захисту персональних даних та його дорученням.

Більше того, якщо оператор не дотримується умов обробки даних, передбачених контролером, оператор стає контролером щонайменше в тій мірі, в якій він порушив інструкції контролера. Найпевніше, це призведе до визнання оператора контролером, який діє незаконно. У свою чергу початковий контролер має пояснити, яким чином було можливо, щоб оператор порушив його доручення[246]. Насправді Робоча група «Стаття 29» вбачає в таких справах спільне контролювання, оскільки саме так забезпечується найкращий захист інтересів суб'єкта персональних даних[247].

У разі, якщо контролер – це мале підприємство, а оператор – велика корпоративна компанія, яка має право диктувати умови щодо надання своїх послуг, може бути порушено питання про розподіл відповідальності. Хоча за таких обставин Робоча група «Стаття 29» вважає, що рівень відповідальності не

244 Загальний регламент захисту персональних даних, стаття 29.

245 Там само, стаття 28 (3).

246 Там само, стаття 82 (2).

247 Робоча група «Стаття 29» (2010), Висновок 1/2010 про поняття «контролер» та «оператор», РГ 169, Брюссель, від 16 лютого 2010 р., 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.

повинен знижуватися через економічний дисбаланс, і що тлумачення поняття «контролер» має залишатись незмінним[248].

Задля ясності та прозорості деталі відносин між контролером і оператором слід виписувати в письмовому договорі[249]. Договір має містити предмет договору, характер, цілі та тривалість обробки, вид персональних даних та категорії суб'єктів персональних даних. Він також має передбачати обов'язки та права контролера та оператора, такі як вимога конфіденційності та безпеки. Відсутність такого договору є порушенням зобов'язання контролера щодо надання письмової документації про взаємні обов'язки і може призвести до накладення санкцій. Якщо шкоду заподіяно внаслідок дій поза межами законних інструкцій контролера або через їх недотримання, не тільки контролер може притягуватися до відповідальності, але й оператор також[250]. Оператор має вести записи (реєстр) усіх категорій діяльності з обробки даних, яку він здійснює від імені контролера[251]. Ці записи мають надаватися наглядовому органу на його вимогу, оскільки як контролер, так й оператор має співпрацювати з цим органом у виконанні його завдань[252]. Контролери та оператори також мають можливість дотримуватися затвердженого кодексу поведінки або процедур сертифікації для демонстрації виконання ними вимог ЗРЗПД[253].

Може статися, що оператори вважатимуть за необхідне делегувати певні завдання субоператорам. Це допускається якщо передбачено належні умови між контролером і оператором, включаючи питання про те, чи необхідно щоразу отримувати дозвіл контролера, чи достатньо лише повідомлення. ЗРЗПД передбачає, що початковий оператор залишається повністю відповідальним перед контролером, якщо субоператор не дотримається своїх обов'язків щодо захисту персональних даних[254].

У **праві РЄ**, як пояснювалося вище, таке тлумачення концепцій «контролер» і «оператор» є повністю застосовним[255].

248 Робоча група «Стаття 29» (2010), *Висновок 1/2010 про поняття «контролер» та «оператор»*, РГ 169, Брюссель, від 16 лютого 2010 р., с. 26.

249 Загальний регламент захисту персональних даних, стаття 28 (3) та (9).

250 Там само, стаття 82 (2).

251 Там само, стаття 30 (2).

252 Там само, стаття 30 (4) та 31.

253 Там само, стаття 28 (5) та 42 (4).

254 Там само, стаття 28 (4).

255 Див., наприклад, Оновлену Конвенцію 108, стаття 2 (b) та (f); Профайлінг Рекомендацію, ст. 1.

2.3.2 Одержувачі та треті сторони

Різниця між цими двома категоріями фізичних або юридичних осіб, як визначено в Директиві про захист персональних даних, стосується здебільшого їхнього зв'язку з контролером і, як результат, їхнього права на доступ до персональних даних, які є в контролера.

«Третя особа» – це той, хто не є контролером та оператором. Відповідно до статті 4 (10) ЗРЗПД третя особа – це «фізична чи юридична особа, орган публічної влади, агентство чи орган, який не є суб'єктом даних, контролером, оператором та особами, які під безпосереднім керівництвом контролера або оператора уповноважені опрацьовувати персональні дані». Це означає, що особи, які працюють в організації, яка не є контролером, навіть якщо вона належить до тієї самої групи чи холдингової компанії, будуть «третьою особою». З іншого боку, філії банку, який здійснює обробку рахунків своїх клієнтів з прямого дозволу своїх штаб-квартир, не будуть «третьою особою»[256].

Поняття «одержувач» має ширше значення, ніж поняття «третя особа». Відповідно до статті 4 (9) ЗРЗПД одержувач означає «фізичну чи юридичну особу, орган публічної влади, агентство чи інший орган, якому розкривають персональні дані, незалежно від того, чи є вони третьою стороною. Цей одержувач може бути особою поза межами контролера або оператора – тоді це буде третя особа – або хтось з компанії контролера або оператора, наприклад працівник або інший підрозділ тієї самої компанії або органу.

Відмінність між одержувачами і третіми особами є важливою лише у зв'язку з умовами законного оприлюднення персональних даних. Співробітники контролера або оператора 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 контролера або оператора, не має права використовувати оброблені контролером персональні дані, за винятком, коли це відбувається на особливих юридичних підставах у конкретному випадку.

Приклад: працівник контролера, 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

256 Робоча група «Стаття 29» (2010), *Висновок 1/2010 про поняття «контролер» та «оператор»*, РГ 169, Брюссель, від 16 лютого 2010 р., с. 31.

та за дорученням контролера. Наприклад, якщо роботодавець відкриває персональні дані працівників своєму відділу кадрів з огляду на майбутню атестацію, команда відділу кадрів буде одержувачем персональних даних, оскільки дані відкриваються їм в ході обробки для контролера.

Однак, якщо організація передає дані своїх працівників тренінговій компанії, яка буде їх використовувати для формування програм підготовки працівників, тренінгова компанія є третьою особою. Причина в тому, що тренінгова компанія не має спеціальних юридичних підстав або дозволу (які у випадку з відділом кадрів можна вивести з трудових відносин з контролером) для обробки цих персональних даних. Інакше кажучи, вони не отримують інформацію в процесі їх залучення контролером даних.

2.4 Згода

Ключові моменти

- Згода як юридична підстава для обробки персональних даних є добровільним, поінформованим, чітким та однозначним волевиявленням суб'єкта персональних даних, вираженим у формі чіткої стверджувальної дії, яким він дозволяє обробку своїх персональних даних.
- Обробка особливих категорій даних на підставі згоди вимагає ясно висловленої згоди.

Як буде розглянуто в главі 4, згода є однією з шести легітимних підстав обробки персональних даних. Згода означає «добровільне, чітке, поінформоване та однозначне волевиявлення суб'єкта персональних даних про свої бажання»[257].

Право ЄС встановлює декілька елементів для того, щоб згода вважалася чинною, з метою гарантування, що суб'єкти даних дійсно погоджуються на відповідне використання їхніх даних[258]:

257 Загальний регламент захисту персональних даних, стаття 4 (11). Див. також Оновлену Конвенцію 108, стаття 5 (2).

258 Загальний регламент захисту персональних даних, стаття 7.

- Згоду має бути надано у формі чіткої стверджувальної дії, яка становить добровільне, чітке, поінформоване та однозначне волевиявлення суб'єкта персональних даних щодо згоди на обробку його або її персональних даних. Такий акт може бути дією або заявою.
- Суб'єкт персональних даних має право відкликати згоду в будь-який момент.
- У контексті письмової заяви, яка також охоплює інші питання, такі як «умови надання послуг», вимогу надати згоду має бути сформульовано ясно, простою мовою у зрозумілій та доступній формі, яка чітко розмежовує згоду та інші питання. Якщо частина такої заяви порушує ЗРЗПД, вона не є обов'язковою для виконання.

Згода може бути чинною відповідно до законодавства із захисту персональних даних, лише якщо всі вимоги виконані. Тягар доведення того, що суб'єкт надав згоду на обробку своїх даних, покладається на контролера[259]. Елементи чинної згоди будуть обговорюватися далі в розділі 4.1.1 щодо правомірних підстав обробки персональних даних. Конвенція 108 не містить визначення згоди, це питання залишено для регулювання національним законодавством. Відповідно до **права РЄ** елементи чинної згоди відповідають тим, що пояснювалися вище[260].

Додаткові вимоги за цивільним законодавством щодо чинної згоди, такі як юридична правоздатність, також застосовні в контексті захисту персональних даних як мінімальні юридичні вимоги. Нечинна згода осіб, які не мають юридичної правоздатності, в результаті призведе до відсутності юридичної підстави для обробки даних таких осіб. Щодо правоздатності неповнолітніх укладати угоди, ЗРЗПД передбачає, що його правила щодо мінімального віку, з якого можливо надати згоду, не суперечать загальному законодавству держави-члена[261].

Згоду має бути надано абсолютно чітко так, щоб не залишалося жодних сумнівів щодо намірів суб'єкта персональних даних[262]. Згоду на обробку чутливих даних має бути прямо і чітко сформульовано, її може бути надано усно або

259 Там само., стаття 7 (1).

260 Оновлена Конвенція 108, стаття 5 (2); Пояснювальна записка до Оновленої Конвенції 108, пп. 42–45.

261 Загальний регламент захисту персональних даних, стаття 8 (3).

262 Там само, стаття 6 (1) (a) та 9 (2) (a).

письмово[263]. Її також може бути надано електронними засобами[264]. Відповідно до **права ЄС та РЄ** угода про обробку персональних даних має бути у вигляді заяви або чіткої стверджувальної дії[265]. Така згода не може випливати з мовчання, завчасно відмічених пунктів, завчасно заповнених форм або бездіяльності[266].

263 Там само, п. 32 преамбули.

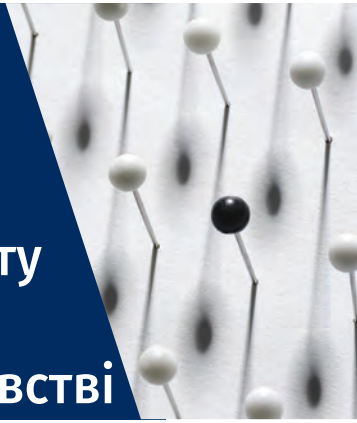
264 Там само.

265 Там само, стаття 4 (11); Пояснювальна записка до Оновленої Конвенції 108, п. 42.

266 Загальний регламент захисту персональних даних, п. 32 преамбули; Пояснювальна записка до Оновленої Конвенції 108, п. 42.

3

Ключові принципи захисту персональних даних у європейському законодавстві



ЄС	Питання, що висвітлюються	РЄ
Загальний регламент захисту персональних даних, стаття 5 (1) (a)	**Принцип законності обробки**	Оновлена Конвенція 108, стаття 5 (3)
Загальний регламент захисту персональних даних, стаття 5 (1) (a)	**Принцип чесності**	Оновлена Конвенція 108, стаття 5 (4) (a) ЄСПЛ, «К. Г. та інші проти Словаччини» (*K. H. and Others v. Slovakia*), № 32881/04, 2009 р.
Загальний регламент захисту персональних даних, стаття 5 (1) (a) СЄС, C-201/14, «Смаранда Бара та інші проти Національного фонду медичного страхування та інших» (*Smaranda Bara and Others v. Casa Naţională de Asigurări de Sănătate and Others*), 2015	**Принцип прозорості**	Оновлена Конвенція 108, стаття 5 (4) (a) та стаття 8 ЄСПЛ, «Хараламбі проти Румунії» (*Haralambie v. Romania*), № 21737/03, 2009 р
Загальний регламент захисту персональних даних, стаття 5 (1) (b)	**Принцип обмеження цілей**	Оновлена Конвенція 108, стаття 5 (4) (b)

ЄС	Питання, що висвітлюються	РЄ
Загальний регламент захисту персональних даних, стаття 5 (1) (c) СЄС, об'єднані справи C-293/12 і C-594/12, «"Digital Rights Ireland Ltd." проти Міністра зв'язку, морських та природних ресурсів та інших та Земельний уряд Каринтії та інші» *(Digital Rights Ireland and Kärntner Landesregierung and Others)* [ВП], 2014	**Принцип мінімізації даних**	Оновлена Конвенція 108, стаття 5 (4) (c)
Загальний регламент захисту персональних даних, стаття 5 (1) (d) СЄС, C-553/07, «Мер та члени міської ради Роттердама проти М.Е.Е. Рейкебура» *(College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer)*, 2009	**Принцип точності даних**	Оновлена Конвенція 108, стаття 5 (4) (d)
Загальний регламент захисту персональних даних, стаття 5 (1) (e) СЄС, об'єднані справи C-293/12 і C-594/12, «"Digital Rights Ireland Ltd." проти Міністра зв'язку, морських та природних ресурсів та інших та Земельний уряд Каринтії та інші» *(Digital Rights Ireland and Kärntner Landesregierung and Others)* [ВП], 2014	**Принцип обмеження періоду зберігання даних**	Оновлена Конвенція 108, стаття 5 (4) (e) ЄСПЛ, «S. та Марпер проти Сполученого Королівства» *(S. and Marper v. the United Kingdom)* [ВП], № 30562/04 та № 30566/04, 2008
Загальний регламент захисту персональних даних, статті 5 (1) (f) та 32	**Безпека даних (принцип цілісності та конфіденційності)**	Оновлена Конвенція 108, стаття 7

ЄС	Питання, що висвітлюються	РЄ
Загальний регламент захисту персональних даних, стаття 5 (2)	**Принцип підзвітності**	Оновлена Конвенція 108, стаття 10

Стаття 5 Загального регламенту захисту персональних даних встановлює принципи, які регулюють обробку персональних даних. Ці принципи включають:

- законність, чесність та прозорість;
- обмеження цілі;
- мінімізацію даних;
- точність даних;
- обмеження зберігання;
- цілісність та конфіденційність.

Принципи є відправними точками для більш детальних положень у наступних статтях регламенту. Вони також з'являються у статтях 5, 7, 8 та 10 Оновленої Конвенції 108. Подальше законодавство із захисту даних на рівні РЄ та ЄС має відповідати цим принципам, і їх необхідно враховувати при тлумаченні цього законодавства. Відповідно до права ЄС обмеження щодо цих принципів обробки дозволяються тільки в тій мірі, в якій вони відповідають правам та обов'язкам, передбаченим статтями 12–20, вони також повинні поважати суть основоположних прав та свобод. Будь-які винятки і обмеження щодо цих ключових принципів мають бути передбачені на рівні ЄС або національному рівні[267]; бути визначені законом, переслідувати легітимну мету і бути необхідними та пропорційними в демократичному суспільстві[268]. Всі три умови мають бути дотримані.

267 Оновлена Конвенція 108, стаття 11 (1); Загальний регламент захисту персональних даних, стаття 23 (1).

268 Загальний регламент захисту персональних даних, стаття 23 (1).

3.1 Принципи законності, чесності та прозорості

Ключові моменти

- Принципи законності, чесності та прозорості застосовуються до всієї обробки персональних даних.
- Відповідно до ЗРЗПД законність вимагає наявності одного з наступних елементів:
  - згода суб'єкта персональних даних;
  - необхідність укладання договору;
  - юридичний обов'язок;
  - необхідність захистити життєво важливі інтереси суб'єкта персональних даних або іншої особи;
  - необхідність виконання завдання в суспільних інтересах;
  - необхідність дотримання легітимних інтересів контролера або третьої особи, якщо вони переважають інтереси та права суб'єкта даних.
- Обробка персональних даних має здійснюватися чесно.
  - Суб'єкт даних повинен бути повідомлений про ризик, щоб забезпечити відсутність непередбачуваних негативних наслідків обробки даних.
- Обробка персональних даних має здійснюватись прозоро.
  - Контролери до початку обробки даних мають поінформувати суб'єкта даних, серед іншого, про цілі обробки та про ідентифікаційні дані та адресу контролера.
  - Інформацію про операції з обробки має бути надано чіткою та простою мовою, щоб забезпечити суб'єкту персональних даних можливість легко зрозуміти правила, ризики, гарантії та права.
  - Суб'єкти даних мають право доступу до своїх даних незалежно від місця, де вони обробляються.

3.1.1 Законність обробки

Право ЄС та РЄ із захисту персональних даних вимагає, щоб дані оброблялись законно[269]. Законність оброки вимагає згоди суб'єкта персональних даних або іншої легітимної підстави, яка передбачена законодавством із захисту персональних даних[270]. Стаття 6 (1) ЗРЗПД на додаток до згоди включає п'ять правомірних підстав для обробки даних, тобто якщо обробка необхідна для виконання договору, виконання завдання в ході здійснення владних повноважень, для дотримання юридичного обов'язку, для цілей легітимних інтересів контролера або третьої особи або у разі необхідності захистити життєво важливі інтереси суб'єкта персональних даних. Це буде більш детально викладено в розділі 4.1.

3.1.2 Чесність обробки

На додаток до законності обробки, право ЄС та РЄ із захисту персональних даних вимагає, щоб персональні дані оброблялись чесно[271]. Принцип чесної обробки регулює передусім відносини між контролером та суб'єктом персональних даних.

Контролери зобов'язані повідомляти суб'єкта даних та громадськість про те, що вони будуть обробляти персональні дані законно та прозоро, та мають бути здатними продемонструвати відповідність операцій обробки правилам ЗРЗПД. Операції з обробки даних не можуть здійснюватися таємно, а суб'єкт персональних даних має знати про потенційні ризики. Крім того, контролер, наскільки можливо, повинен діяти у спосіб, який дозволяє невідкладно виконувати бажання суб'єкта даних, особливо, якщо обробка здійснюється на підставі згоди суб'єкта.

Приклад: у справі «*К. Г. та інші проти Словаччини*»[272] заявницями 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.

269 Оновлена Конвенція 108, стаття 5 (3); Загальний регламент захисту персональних даних, стаття 5 (1) (a).

270 Хартія основних прав ЄС, стаття 8 (2); Загальний регламент захисту персональних даних, п. 40 та статті 6–9; Оновлена Конвенція 108, стаття 5 (2); Пояснювальна записка до Оновленої Конвенції 108, п. 41.

271 Загальний регламент захисту персональних даних, стаття 5 (1) (a); Оновлена Конвенція 108, стаття 5 (4) (a).

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

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 попередження їхньому неналежному використанню. Позитивні зобов'язання держав за статтею 8 ЄКПЛ неодмінно передбачають зобов'язання надавати суб'єкту персональних даних можливості доступу до копій своїх даних. Саме держава мала визначити механізм здійснення копіювання персональних даних або в разі необхідності надати переконливі причини для відмови. У справі заявниць національні суди здебільшого обґрунтували заборону на копіювання медичних документів необхідністю захисту відповідної інформації від зловживання. Однак ЄСПЛ не зміг зрозуміти, яким чином заявниці, які у будь-якому випадку мали б отримати доступ до всіх своїх медичних документів, зловживали б інформацією про себе. Окрім того, ризику такого зловживання можна було б запобігти за допомогою інших засобів, аніж відмова в копіюванні документів заявниць, наприклад, шляхом обмеження кола осіб, які мають право на доступ до документів. Держава не продемонструвала існування переконливих причин для відмови заявницям у доступі до інформації, яка стосувалася їхнього здоров'я. Суд дійшов висновку, що було порушено статтю 8.

Що стосується інтернет-послуг, характеристики систем обробки даних мають надавати суб'єкту персональних даних можливість дійсно розуміти, що відбувається з його персональними даними. У будь-якому разі принцип чесності обробки є ширшим, ніж обов'язок прозорості, та може бути пов'язаний з етичними аспектами обробки персональних даних.

Приклад: дослідницький департамент університету проводить експеримент з аналізу зміни настрою в 50 осіб. Відповідно до правил експерименту вимагалося записувати в електронні файли їхні думки кожну годину у призначений час. 50 осіб надали свою згоду для цього проєкту на саме таке використання даних університетом. Згодом департамент зрозумів, що завантаження думок в електронному вигляді було б дуже корисним для іншого проєкту щодо розумового здоров'я, який координується іншою командою. Навіть хоча університет, як контролер, міг би використовувати ті самі дані для роботи іншої команди без подальших кроків щодо законності обробки цих даних, оскільки цілі є сумісними, університет повідомив суб'єктів даних та попросив нової згоди у відповідності до їхнього Кодексу етики досліджень та принципу чесності обробки.

3.1.3 Прозорість обробки

Законодавство із захисту персональних даних ЄС та нормативно-правові документи РЄ вимагають, щоб обробка персональних даних здійснювалась «у прозорий спосіб щодо суб'єкта персональних даних»[273].

Цей принцип зобов'язує контролера персональних даних вживати будь-яких належних заходів для інформування суб'єктів персональних даних – які можуть бути користувачами, покупцями, клієнтами – про те, як використовуються їхні персональні дані[274]. Прозорість може стосуватись інформації, яка надається суб'єкту даних перед початком обробки[275], інформації, яка має бути готова та доступна для суб'єкта даних під час обробки[276], а також інформації, яка надається суб'єкту даних у відповідь на запит суб'єктів про доступ до їхніх даних[277].

> Приклад: у справі «*Хараламбі проти Румунії*»[278] заявник звернувся із запитом про надання йому доступу до досьє, яке було заведене на нього секретною службою, проте його прохання було задоволено лише через п'ять років. ЄСПЛ ще раз підтвердив, що особи, щодо яких органами державної влади було заведене досьє, життєво зацікавлені у можливості отримати до них доступ. Влада була зобов'язана забезпечити належну процедуру доступу до такої інформації. ЄСПЛ визнав, що ані обсяг переданого досьє, ані недоліки архівної системи не виправдовують п'ятирічну затримку із задоволенням 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,

273 Загальний регламент захисту персональних даних, стаття 5 (1) (a); Оновлена Конвенція 108, стаття 5 (4) (a) та 8.

274 Загальний регламент захисту персональних даних, стаття 12.

275 Там само,стаття 13 та 14.

276 Робоча група «Стаття 29», Висновок 2/2017 щодо обробки даних на роботі, с. 23.

277 Загальний регламент захисту персональних даних, стаття 15.

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

що відбуватиметься з їхніми персональними даними. Це означає, що суб'єкт даних має знати про конкретну мету обробки персональних даних при збиранні цих даних[279]. Принцип прозорості обробки вимагає використання зрозумілої та простої мови[280]. Зацікавленим особам має бути зрозуміло про наявні ризики, правила, гарантії та права щодо обробки їхніх персональних даних[281].

Право РЄ також передбачає, що певна важлива інформація має в обов'язковому порядку надаватись контролером суб'єкту даних у активний спосіб. Інформацію про назву та адресу контролера (або спільних контролерів), юридичну підставу та цілі обробки даних, категорії даних, що обробляються, одержувачів, а також про засоби реалізації прав може бути надано у будь-якому належному форматі (або через вебсайт, або технологічні сервіси на особистий пристрій тощо), якщо таку інформацію надають суб'єкту чесно та ефективно. Надана інформація має бути легко доступною, читабельною, зрозумілою та адаптованою для конкретного суб'єкта даних (наприклад, з використанням зручної для дитини мови у разі необхідності). Також має надаватися будь-яка інша додаткова інформація для забезпечення чесності обробки персональних даних або яка є корисною для такої мети, наприклад щодо періоду зберігання даних, обґрунтування підстав обробки даних або інформація про передачу даних одержувачам на територію іншої держави-учасниці або держави, яка не є учасницею (включно з інформацією про забезпечення цією державою належного рівня захисту або заходів, які вжив контролер для гарантування такого належного рівня захисту даних)[282].

Відповідно до права на доступ[283] суб'єкт даних має право отримати інформацію від контролера у відповідь на свій запит, чи обробляються його дані, і, якщо так, то які саме[284]. Крім того, відповідно до права на інформацію[285] особи, чиї дані обробляються, мають до початку обробки бути повідомлені контролерами або операторами про цілі, тривалість, засоби обробки та інші деталі.

279 Загальний регламент захисту персональних даних, п. 39 преамбули.

280 Там само.

281 Там само.

282 Пояснювальна записка до Оновленої Конвенції 108, п. 68.

283 Загальний регламент захисту персональних даних, стаття 15.

284 Оновлена Конвенція 108, стаття 8 та 9 (1) (b).

285 Загальний регламент захисту персональних даних, стаття 13 та 14.

Приклад: у справі «*Смаранда Бара та інші проти Національного фонду медичного страхування та інших*»[286] йшлося про передачу податкових даних, що стосувалися доходу самозайнятих осіб, з Національного агентства податкового адміністрування до Національної агенції страхування здоров'я в Румунії. На підставі цих даних були висунуті вимоги щодо оплати боргів за внески страхування здоров'я. Перед СЄС постало питання, чи мали бути повідомлені суб'єкти персональних даних про ідентифікаційні дані контролера та цілі передачі даних до того, як агентство податкового адміністрування почало їх обробку. СЄС вирішив, що у випадку, коли один орган держави-члена передає персональні дані іншому органу, який у подальшому здійснює їх обробку, суб'єкт даних повинен бути повідомлений про передачу та обробку.

У певних ситуаціях дозволяються відступи від обов'язку інформувати суб'єкта даних про обробку даних. Про це більш детально йтиметься у розділі 6.1 щодо прав суб'єкта персональних даних.

3.2 Принцип обмеження мети

Ключові моменти

- Ціль обробки персональних даних має бути визначена до початку обробки.
- Дані не можуть оброблятись, якщо обробка несумісна з початковою ціллю, хоча Загальний регламент захисту персональних даних передбачає винятки з цього правила, коли йдеться про цілі архівування в суспільних інтересах, цілі наукових або історичних досліджень та статистичні цілі.
- По суті, принцип обмеження мети означає, що будь-яка обробка персональних даних повинна здійснюватись з чітко визначеною метою, а також тільки для додаткових, визначених цілей, які сумісні з початковою метою.

Принцип обмеження мети є одним з основоположних принципів європейського законодавства із захисту персональних даних. Він тісно пов'язаний з

286 Рішення Суду ЄС, C-201/14, «Смаранда Бара та інші проти Національного фонду медичного страхування та інших» (*Smaranda Bara and Others v. Casa Naţională de Asigurări de Sănătate and Others*), від 1 жовтня 2015р, пп. 28–46.

прозорістю, передбачуваністю та контролем з боку користувача: якщо ціль обробки достатньо чітка та ясна, фізичні особи знають чого очікувати, а прозорість та юридична визначеність посилюються. Водночас чітке окреслення мети є важливим для забезпечення ефективної реалізації суб'єктами персональних даних своїх прав, як-то права на заперечення проти обробки[287].

Цей принцип вимагає, щоб будь-яка обробка персональних даних здійснювалась з конкретною, належно визначеною метою, а також тільки для додаткових цілей, які сумісні з початковою метою[288]. Обробка персональних даних для невизначених та/або необмежених цілей є неправомірною. Обробка персональних даних без певної мети, просто з міркувань, що вони можуть бути корисні колись у майбутньому, також є неправомірною. Правомірність обробки персональних даних залежатиме від мети обробки, яка має бути чітко вказана, конкретна та легітимна.

Будь-яка нова мета обробки даних, яка несумісна з початковою метою, повинна мати свою окрему юридичну підставу і не може ґрунтуватись на тому, що дані були початково отримані або оброблялись для іншої легітимної мети. В свою чергу, правомірна обробка даних обмежується початковою конкретною метою, і будь-яка нова мета обробки буде вимагати окремої нової юридичної підстави. Наприклад, відкриття персональних даних третім особам з новою ціллю має бути ретельно досліджено. Відкриття даних як таке, ймовірно, потребуватиме додаткової юридичної підстави, іншої, ніж та, на підставі якої збиралися дані.

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

287 Робоча група «Стаття 29» (2013), *Висновок 3/2013 щодо обмеження мети*, РГ 203, від 2 квітня 2013 р.

288 Загальний регламент захисту персональних даних, стаття 5 (1) (b).

При розгляді обсягу та обмежень конкретної мети Оновлена Конвенція 108 та Загальний регламент захисту персональних даних покладаються на концепцію сумісності: використання даних із сумісними цілями дозволено на тій же юридичній підставі, яка була початковою. Подальша обробка даних не може вестись у спосіб, що є неочікуваним, неналежним або у спосіб, проти якого суб'єкт може заперечити[289]. Для оцінки того, чи може подальша обробка вважатися сумісною, контролер повинен взяти до уваги (серед іншого) наступне:

- «будь-який зв'язок між тими цілями та цілями, з якими буде здійснюватись подальша обробка;
- контекст, у якому персональні дані було зібрано, зокрема стосовно обґрунтованих очікувань суб'єкта даних, заснованих на його відносинах з контролером, щодо подальшого використання даних;
- характер персональних даних;
- наслідки подальшої обробки даних для суб'єкта даних;
- існування належних гарантій щодо початкової обробки та подальших операцій з обробки, які мають здійснюватися»[290]. У свою чергу, це може бути забезпечено, наприклад, шляхом використання шифрування або псевдонімізації.

Приклад: компанія «Саншайн» отримує персональні дані через CRM-систему. Далі вона передає ці дані компанії прямого маркетингу «Мунлайт», яка хоче використати ці дані для допомоги маркетинговим компаніям третіх компаній. Передача даних компанією «Саншайн» для маркетингу іншим компаніям становить подальше використання даних з новою метою, яка несумісна з CRM-системою, першою метою збирання даних про клієнтів компанією «Саншайн». Тому передача даних компанії «Мунлайт» потребує своєї власної нової юридичної підстави.

Натомість використання даних CRM-системи компанією «Саншайн» для власних маркетингових цілей, наприклад надсилання маркетингових повідомлень покупцям своїх продуктів, є загальноприйнятою сумісною метою.

289 Пояснювальна записка до Оновленої Конвенції 108, п. 49.

290 Загальний регламент захисту персональних даних, п. 50 преамбули та стаття 6 (4); Пояснювальна записка до Оновленої Конвенції 108, п. 49.

Загальний регламент захисту персональних даних та Оновлена Конвенція 108 проголошують, що «подальша обробка для досягнення цілей архівування в суспільних інтересах, цілей наукових або історичних досліджень, або статистичних цілей» *a priori* вважаються сумісними з початковою метою[291]. Однак такі належні гарантії, як знеособлення, шифрування або псевдонімізація даних, а також обмеження доступу до даних мають бути впровадженні при подальшій обробці даних[292]. Загальний регламент захисту персональних даних крім того додає, що «у разі, якщо суб'єкт даних надав згоду або обробка ґрунтується на законодавстві Союзу чи держави-члена, що становить необхідний та пропорційний захід у демократичному суспільстві для гарантування, зокрема, важливих цілей загального суспільного інтересу, контролеру дозволяється подальша обробка персональних даних незалежно від сумісності цілей»[293]. Якщо здійснюється подальша обробка, суб'єкт даних має бути поінформованим про цілі, а також про свої права, наприклад право заперечувати проти обробки[294].

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 сумісною метою. Додаткової юридичної підстави, як-то згоди суб'єктів персональних даних, не потрібно. Однак для подальшої обробки персональних даних в статистичних цілях компанія «Саншайн» має запровадити належні захисні гарантії прав і свобод суб'єкта даних. Технічні та організаційні заходи, які компанія «Саншайн» повинна здійснити, можуть включати псевдонімізацію.

291 Загальний регламент захисту персональних даних, стаття 5 (1) (b); Оновлена Конвенція 108, стаття 5 (4) (b). Приклад таких національних положень у законі Австрії *Про захист персональних даних (Закон про конфіденційність)*, Федеральний вісник законів, № 165/1999, п. 46

292 Загальний регламент захисту персональних даних, стаття 6 (4); Оновлена Конвенція 108, стаття 5 (4) (b); Пояснювальна записка до Оновленої Конвенції 108, п. 50.

293 Загальний регламент захисту персональних даних, п. 50 преамбули.

294 Там само.

3.3 Принцип мінімізації даних

Ключові моменти

- Обробка даних має бути зведена до такого мінімуму, який вважається необхідним для досягнення легітимної мети.
- Обробка персональних даних має відбуватись виключно тоді, коли мету обробки неможливо раціонально досягти іншими засобами.
- Обробка даних не має непропорційно втручатись у відповідні інтереси, права та свободи.

Оброблятись можуть тільки такі дані, які є «адекватними, відповідними та не надмірними відносно мети, з якою вони збирались та/або в подальшому обробляються»[295]. Категорії даних, які обрані для обробки, мають бути необхідними для досягнення проголошеної загальної мети операцій з обробки, а контролер має жорстко обмежити збір даних, зводячи його до такої інформації, яка безпосередньо стосується конкретної мети обробки.

Приклад: у справі *«Digital Rights Ireland»*[296] Суд ЄС вирішив питання правомірності Директиви про зберігання даних, що мала на меті гармонізувати національні положення щодо збереження персональних даних, які згенеровані або обробляються в результаті функціонування публічно доступних електронних комунікаційних послуг або суспільних телекомунікаційних мереж для їх можливої передачі компетентним органам для боротьби з серйозними злочинами, як-от організована злочинність або тероризм. Незважаючи на те, що це було визнано метою, яка загалом відповідає цілям загального інтересу, узагальнений підхід Директиви охоплював «всіх фізичних осіб та всі засоби електронної комунікації, а також дані трафіку

295 Оновлена Конвенція 108, стаття 5 (4) (c); Загальний регламент захисту персональних даних, стаття 5 (1) (c).

296 Суд ЄС, об'єднані справи C-293/12 та C-594/12, «"Digital Rights Ireland Ltd." проти Міністра зв'язку, морських та природних ресурсів та інших та Земельний уряд Каринтії та інші» (*Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others)* [ВП]), від 08 квітня 2014 р.

без будь-якого розрізнення, обмежень або винятків у контексті боротьби з серйозними злочинами» і був визнаний проблематичним[297].

Більше того, використовуючи спеціальні технології з посилення конфіденційності, в деяких випадках можливо взагалі уникнути використання даних або використати засоби з меншою можливість співвіднести дані з суб'єктом персональних даних (наприклад, через псевдонімізацію), що в результаті призводить до вирішення питання з дотриманням конфіденційності. Це є особливо доречним для більш розгалужених систем обробки.

Приклад: рада міста пропонує чіп-картку регулярним користувачам міського громадського транспорту для певної оплати. Картка містить ім'я користувача в письмовій формі на лицевому боці картки, також в електронній формі в чипі. В автобусі або трамваї чіп-карта має прикладатися до встановленого там приладу для зчитування. Зчитані приладом дані автоматично перевіряються за допомогою бази даних осіб, які придбали картки для проїзду.

Ця система не в повній мірі відповідає принципу мінімізації даних: перевірку, чи може особа використовувати транспортні засоби, можна організувати без порівняння персональних даних на картці з базою даних. Було б достатньо, наприклад, розмістити на картці такий електронний знак, як штрих код, який би при прикладанні до приладу підтверджував чинність карти. Така система не фіксувала б, хто користувався транспортним засобом і конкретний час. Це було б оптимальним рішенням у контексті принципу мінімізації даних, оскільки він полягає в обов'язку мінімізувати збір даних.

Стаття 5 (1) Оновленої Конвенції 108 передбачає вимогу пропорційності обробки персональних даних відносно легітимної мети, яка переслідується. Справедливий баланс між всіма інтересами має бути встановлено на всіх стадіях обробки. Це означає, що «[ ] персональні дані, які є адекватними та відповідними, але які призведуть до непропорційного втручання в основоположні права та свободи, повинні визнаватися надмірними»[298].

297 Там само, пп. 44 та 57.

298 Пояснювальна записка до Оновленої Конвенції 108, п. 52; Загальний регламент захисту персональних даних, стаття 5 (1) (c).

3.4 Принцип точності даних

Ключові моменти

- Контролер повинен дотримуватися принципу точності даних під час усіх операцій з обробки даних.
- Неточні дані мають бути видалені або змінені без затримок.
- Дані мають перевірятися регулярно та підтримуватись в актуальному стані для забезпечення точності.

Контролер, що володіє персональною інформацією, не повинен використовувати цю інформацію, не вживши достатніх заходів для забезпечення, що дані були точними та актуальними[299].

Обов'язок забезпечення точності має розглядатись у контексті мети обробки даних.

Приклад: у справі «*Рейкебура*»[300] Суд ЄС розглянув запит громадянина Нідерландів на отримання інформації від місцевої адміністрації м. Амстердама щодо ідентифікаційних даних осіб, яким передавалися записи про нього протягом двох попередніх років, а також щодо змісту відкритих даних. СЄС вирішив, що «право на приватність означає, що суб'єкт персональних даних має бути певним, що його персональні дані обробляються у визначений та законний спосіб, тобто, що основні дані про нього є точними, та що вони відкриваються уповноваженим одержувачам». Далі Суд ЄС послався на преамбулу Директиви про захист персональних даних, відповідно до якої суб'єкти персональних даних повинні мати право на доступ до своїх даних для того, щоб бути здатними перевірити коректність даних[301].

299 Загальний регламент захисту персональних даних, стаття 5 (1) (d); Оновлена Конвенція 108, стаття 5 (4) (d).

300 Рішення Суду ЄС, C-553/07 «Мер та члени міської ради Роттердама проти М.Е.Е. Рейкебура», (*College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer*), від 7 травня 2009 р.

301 Пункт 41 преамбули колишньої Директиви 95/46/ЄС.

Також можуть бути випадки, коли оновлення збережених даних заборонене законом, якщо переважною метою збереження даних є документування подій як історичного «стоп-кадру».

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

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, остання 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, в особи можуть виникнути серйозні проблеми. Тому контролери таких баз даних повинні докладати особливих зусиль щодо дотримання принципу точності.

3.5 Принцип обмеження періоду зберігання даних

Ключові моменти

- Принцип обмеження періоду зберігання даних означає, що персональні дані мають бути видалені або знеособлені, як тільки вони більше не є необхідними для цілей, задля яких вони збирались.

У статті 5 (1) (e) ЗРЗПД, а також у статті 5 (4)(e) Оновленої 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 для цілей», для яких вони обробляються. Тому персональні дані повинні бути видалені або знеособлені, якщо мета була досягнута. Для цього «мають бути встановлені строки для видалення або періодичного перегляду», щоб дані не зберігалися довше, ніж це необхідно[302].

У справі «*С. та 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 стосовно діяльності поліції[303].

Приклад: у справі «*С. та Марпер*»[304] ЄСПЛ вирішив, що зберігання протягом невизначеного періоду відбитків пальців, зразків клітин та ДНК-профілів двох заявників було непропорційним та не необхідним у демократичному суспільстві, враховуючи, що кримінальне провадження проти обох заявників закінчилося їхнім виправданням та закриттям справи.

Обмеження часу зберігання персональних даних застосовується тільки до тих даних, які зберігаються у формі, що дозволяє ідентифікацію суб'єкта даних. Відповідно, законність зберігання даних, які вже не є необхідними, може бути забезпечена шляхом знеособлення даних.

Персональні дані, збережені з метою історичного, статистичного чи наукового використання, можуть зберігатися довший час за умови, що такі дані будуть використовуватись виключно для зазначених цілей[305]. Для подальшого збереження та використання персональних даних мають бути запроваджені належні технічні та організаційні заходи для гарантування прав та свобод суб'єкта персональних даних.

Оновлена Конвенція 108 також дозволяє винятки з принципу обмеженого зберігання даних за умови, що вони передбачені законом, поважають суть

302 Загальний регламент захисту персональних даних, п. 39 преамбули.

303 Рішення ЄСПЛ у справі «С. та Марпер проти Сполученого Королівства» (*S. and Marper v. the United Kingdom*) [ВП], №№ 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.

304 Рішення ЄСПЛ у справі «С. та Марпер проти Сполученого Королівства» (*S. and Marper v. the United Kingdom*) [ВП], №№ 30562/04 та 30566/04, від 4 грудня 2008 р.

305 Загальний регламент захисту персональних даних, стаття 5 (1) (e); Оновлена Конвенція 108, стаття 5 (4) (b) та 11 (2).

основоположних прав та свобод та є необхідними і пропорційними для досягнення обмеженої кількості легітимних цілей[306]. Вони, серед іншого, включають захист національної безпеки, розслідування злочинів та переслідування за їх вчинення, виконання кримінальних покарань, захист суб'єкта даних та захист прав і свобод інших.

Приклад: у справі «*Digital Rights Ireland*»[307] СЄС перевіряв чинність Директиви про зберігання даних, яка мала на меті гармонізувати національні положення щодо зберігання персональних даних, що згенеровані або обробляються в результаті функціонування публічно доступних електронних комунікаційних послуг або суспільних телекомунікаційних мереж для їх можливої передачі компетентним органам для боротьби з серйозними злочинами, як-от організована злочинність або тероризм. Директива про зберігання даних передбачала, що дані можуть зберігатися протягом «щонайменше шести місяців без будь-якого розрізнення між категоріями даних, передбачених статтею 5 Директиви, на основі їхньої можливої корисності для цілей, які переслідуються, або відповідно до осіб, яких це стосується»[308].

Суд ЄС також порушив питання щодо відсутності в Директиві об'єктивних критеріїв, на основі яких конкретний період зберігання – який міг різнитися від шести до максимальних 24 місяців – мав визначатися для забезпечення обмеження цього періоду до такого рівня, що є вкрай необхідним[309].

306 Оновлена Конвенція 108, стаття 11.1; Пояснювальна записка до Оновленої Конвенції 108, пп. 91–98.

307 Суд ЄС, об'єднані справи C-293/12 та C-594/12, «"Digital Rights Ireland Ltd." проти Міністра зв'язку, морських та природних ресурсів та інших та Земельний уряд Каринтії та інші» (*Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [ВП]), від 08 квітня 2014 р.

308 Там само, п. 63.

309 Там само, п. 64.

3.6 Принцип безпеки даних

Ключові моменти

- Безпека та конфіденційність персональних даних є ключовими для попередження негативних наслідків для суб'єкта персональних даних.
- Заходи безпеки можуть бути технічного та/або організаційного характеру.
- Псевдонімізація є процесом, який може захистити персональні дані.
- Відповідність заходів безпеки має визначатись в залежності від обставин справи та регулярно переглядатись.

Принцип безпеки даних вимагає вживати організаційних або технічних заходів при обробці персональних даних для їх захисту від випадкового, несанкціонованого або протиправного доступу, використання, зміни, відкриття, втрати, знищення або пошкодження[310]. ЗРЗПД вказує, що при застосуванні заходів безпеки контролер та оператор мають враховувати «сучасний стан справ, витрати на впровадження та характер, обсяг, контекст і мету обробки, а також ризики різного ступеня вірогідності та серйозності для прав та свобод фізичних осіб»[311]. В залежності від конкретних обставин кожної справи належні технічні та організаційні заходи можуть включати, наприклад, псевдонімізацію та шифрування даних та/або регулярну перевірку та оцінку ефективності заходів для забезпечення безпеки даних, які обробляються[312].

Як пояснюється в розділі 2.1.1, псевдонімізація даних означає заміну елементів персональних даних – які уможливлюють ідентифікацію суб'єкта даних – псевдонімом та тримання цих елементів окремо із застосуванням технічних та організаційних заходів. Процес псевдонімізації не можна плутати з процесом знеособлення, в якому всі зв'язки, що ідентифікують особу, розриваються.

310 Загальний регламент захисту персональних даних, п. 39 та стаття 5 (1) (f); Оновлена Конвенція 108, стаття 7.

311 Загальний регламент захисту персональних даних, стаття 32 (1).

312 Там само.

Приклад: речення «Шарль Спенсер, народжений 3 квітня 1967, є батьком у сім'ї з чотирма дітьми, двома хлопчиками та двома дівчатками» може бути псевдонімізоване, наприклад, наступним чином:

«Ш.С., 1967 р.н., є батьком у сім'ї з чотирма дітьми, двома хлопчиками та двома дівчатками»; або

«324 є батьком у сім'ї з чотирма дітьми, двома хлопчиками та двома дівчатками»; або

«YESz320l є батьком у сім'ї з чотирма дітьми, двома хлопчиками та двома дівчатками».

Користувачі, які не мають доступу до псевдонімізованих даних, як правило, не зможуть ідентифікувати «Шарля Спенсера, народженого 3 квітня 1967» за псевдонімом «324» або «YESz3201». Таким чином, ці дані з більшою ймовірністю захищені від неналежного використання.

Водночас перший приклад є менш безпечним. Якщо речення «Ш.С., 1967 р.н., є батьком у сім'ї з чотирма дітьми, двома хлопчиками та двома дівчатками» використовується в маленькому містечку, у якому Шарль Спенсер проживає, пан Спенсер є впізнаваним без ускладнень. Метод псевдонімізації може вплинути на ефективність захисту даних.

Персональні дані, які закодовані або елементи яких зберігаються окремо, використовуються в багатьох контекстах як засіб тримання ідентичності осіб в таємниці. Це особливо корисно у випадках, коли контролери повинні переконатися, що мають справу з тими самими суб'єктами, однак при цьому не вимагається або ж вони взагалі не повинні знати дійсну особистість суб'єкта даних. Наприклад, таким випадком є дослідження перебігу хвороби пацієнтів, чия ідентифікація відома тільки лікарні, де вони лікувалися, та з якої дослідник отримує псевдонімізовані історії хвороби. Таким чином, псевдонімізація є потужним елементом в арсеналі технологій із забезпечення конфіденційності. Вона може бути важливою ланкою системи конфіденційності. Це означає, що система обробки персональних даних має розроблятися з вбудованим у ній захистом персональних даних.

Стаття 25 ЗРЗПД, яка регулює захист даних за призначенням і за замовчуванням, містить чітке посилання на псевдонімізацію, як на приклад належного технічного та організаційного заходу, який контролери мають впроваджувати

для включення принципу захисту даних та захисних гарантій. Діючи таким чином, контролери будуть дотримуватися вимог регламенту та будуть захищати права суб'єктів даних при обробці їхніх персональних даних.

Дотримання затвердженого кодексу етичної поведінки або затвердженого сертифікаційного механізму може допомогти продемонструвати дотримання вимоги безпеки обробки даних[313]. У своєму висновку щодо засад захисту персональних даних при обробці реєстраційних даних пасажирів Рада Європи наводить інші приклади належних заходів безпеки для захисту персональних даних у системі реєстрації пасажирів. Вони включають зберігання даних у фізично безпечному середовищі, обмеження доступу шляхом використання складних логінів та захист руху даних через шифрування[314].

Приклад: сайти соціальних мереж і провайдери електронних пошт забезпечують користувачам можливість підвищити рівень безпеки послуг, які вони надають, шляхом запровадження дворівневої автентифікації. На додаток до введення пароля для того, щоб ввійти в свій акаунт, користувачі мають здійснити другий вхід. Останнім може бути, наприклад, введення коду безпеки, надісланого на мобільний телефон, зв'язаний з особистим акаунтом. Таким чином, дворівнева перевірка надає більший захист персональної інформації від несанкціонованого доступу до особистого акаунту шляхом його зламу.

Пояснювальна записка до Оновленої Конвенції 108 наводить додаткові приклади належних захисних гарантій, таких як запровадження обов'язку зберігати професійну таємницю або вжиття таких кваліфікованих технічних заходів безпеки, як шифрування даних[315]. При впровадженні спеціальних заходів безпеки контролер – або у разі застосовності оператор – мають враховувати декілька аспектів, як-от характер та обсяг персональних даних, які обробляються, потенційні негативні наслідки для суб'єкта даних та необхідність обмеження доступу до даних[316]. Сучасний стан заходів з безпеки даних та технологій обробки даних мають бути враховані при впровадженні належних заходів захисту. Вартість таких заходів має бути пропорційною серйозності та

313 Там само., стаття 32 (3).

314 Рада Європи, Комітет Конвенції 108, *Висновок щодо наслідків для захисту персональних даних від обробки записів імен пасажирів*, T-PD(2016)18rev, від 19 серпня 2016 р., с. 9.

315 Пояснювальна записка до Оновленої Конвенції 108, п. 56.

316 Там само, п. 62.

ймовірності потенційних ризиків. Вимагається також регулярний перегляд заходів безпеки з тим, щоб їх можна було оновити у разі необхідності[317].

У випадках витоку персональних даних як Оновлена Конвенція 108, так й ЗРЗПД вимагає від контролера без затримки повідомити компетентний наглядовий орган про витік даних та ризики для прав і свобод фізичних осіб[318]. Такий же обов'язок повідомлення суб'єкта даних існує у випадках, коли витік персональних даних може призвести до значних загроз для його прав і свобод[319]. Повідомлення суб'єктів даних про такі витоки мають бути здійснені простою та ясною мовою[320]. Якщо оператору стало відомо про порушення захисту персональних даних, контролер має бути повідомлений про це негайно[321]. За певних обставин можуть застосовуватися винятки з зобов'язання здійснювати повідомлення. Наприклад, контролер не має повідомляти компетентний наглядовий орган у випадку, коли «малоймовірним є ризик для прав і свобод фізичних осіб внаслідок витоку даних»[322]. Також не потрібно повідомляти суб'єкта даних у разі, якщо застосовані заходи безпеки роблять дані незрозумілими для осіб, які не уповноважені мати до них доступ, або якщо в результаті подальших заходів здійснення загрози стає малоймовірною[323]. Якщо повідомлення суб'єктів даних про порушення захисту даних покладає на контролера непропорційний тягар, публічне повідомлення або схожий захід може забезпечити «повідомлення суб'єктів даних таким саме ефективним шляхом»[324].

317 Там само, п. 63.

318 Оновлена Конвенція 108, стаття 7 (2); Загальний регламент захисту персональних даних, стаття 33 (1).

319 Оновлена Конвенція 108, стаття 7 (2); Загальний регламент захисту персональних даних, стаття 34 (1).

320 Загальний регламент захисту персональних даних, стаття 34 (2).

321 Там само, стаття 33 (1).

322 Там само, стаття 32 (1).

323 Там само, стаття 34 (3) (a) та (b).

324 Там само, стаття 34 (3) (c).

3.7 Принцип підзвітності

Ключові моменти

- Підзвітність вимагає від контролерів та операторів активного здійснення заходів щодо підтримки та захисту персональних даних під час їх обробки.
- Контролери та оператори відповідають за дотримання законодавства про захист персональних даних та своїх відповідних обов'язків під час операцій з обробки даних.
- Контролери мають бути готові в будь-який час продемонструвати відповідність нормам закону про захист персональних даних суб'єктам персональних даних, громадськості та наглядовим органам. Оператори також повинні виконувати певні обов'язки, які тісно пов'язані з підзвітністю (такі як ведення записів (реєстру) операцій з обробки даних та призначення спеціаліста із захисту персональних даних).

ЗРЗПД та Оновлена Конвенція 108 передбачають, що контролер несе відповідальність за дотримання принципів обробки даних, описаних у цій главі, та має бути здатним продемонструвати це[325]. Для цього контролер має впровадити належні технічні та організаційні заходи[326]. Хоча стаття 5 (2) ЗРЗПД, яка унормовує принцип підзвітності, спрямована тільки на контролерів, від операторів також очікується підзвітність, оскільки вони тісно пов'язані з підзвітністю і мають дотримуватися низки обов'язків.

Законодавство із захисту персональних даних ЄС та РЄ також визначає, що контролер є відповідальним за дотримання принципів, які описані в розділах 3.1–3.6, та має бути в змозі забезпечити таке дотримання[327]. Робоча група «Стаття 29» вказує, що «види процедур та механізмів можуть різнитися в залежності від ризиків, які пов'язані з обробкою та характером даних»[328].

Контролери можуть сприяти виконанню цієї вимоги різними шляхами, які включають:

325 Там само, стаття 5 (2); Оновлена Конвенція 108, стаття 10 (1).

326 Загальний регламент захисту персональних даних, стаття 24.

327 Там само, стаття 5 (2); Оновлена Конвенція 108, стаття 10 (1).

328 Робоча група «Стаття 29», *Висновок 3/2010 про принцип підзвітності*, РГ 173, Брюссель, від 13 липня 2010 р., п. 12.

- документування діяльності з обробки та надання їх наглядовому органу за вимогою[329];
- призначення в певних випадках спеціаліста із захисту персональних даних, який залучений до вирішення всіх питань щодо захисту персональних даних[330];
- здійснення аналізу наслідків обробки даних для таких видів даних, обробка яких, ймовірно, призведе до високого ризику для прав і свобод фізичних осіб[331];
- забезпечення захисту даних за призначенням та за замовчуванням[332];
- впровадження методів і процедур реалізації прав суб'єктів даних[333];
- дотримання затвердженого кодексу поведінки або сертифікаційних механізмів[334].

Хоча стаття 5 (2) ЗРЗПД, яка унормовує принцип підзвітності, не спрямована безпосередньо на операторів, вона містить пов'язані з підзвітністю положення, які також вказують на їхні обов'язки, такі як ведення записів про обробку даних і призначення спеціаліста із захисту персональних даних для будь-якої діяльності з обробки даних, яку вони здійснюють[335]. Оператори також мають забезпечити вжиття всіх належних заходів з безпеки даних[336]. Юридично обов'язковий договір між контролером та оператором повинен передбачати, що оператор має допомагати контролеру у дотриманні таких вимог, як здійснення оцінки наслідків обробки даних або повідомлення контролера про будь-який витік даних, щойно йому буде про це відомо[337].

Організація економічного співробітництва та розвитку (ОЕСР) у 2013 році затвердила посібник з конфіденційності, де підкреслюється, що контролери відіграють важливу роль у втіленні на практиці захисту даних. У

329 Загальний регламент захисту персональних даних, стаття 30.

330 Там само, стаття 37–39.

331 Там само, стаття 35; Оновлена Конвенція 108, стаття 10 (2).

332 Загальний регламент захисту персональних даних, стаття 25; Оновлена Конвенція 108, стаття 10 (2) та (3).

333 Там само, стаття 12 та стаття 24.

334 Там само, стаття 40 та стаття 42.

335 Там само, стаття 5 (2), 30 та 37.

336 Там само, стаття 28 (3) c.

337 Там само, стаття 28 (3) d.

посібнику вказується, що принцип підзвітності полягає в тому, що «контролер має бути відповідальним за заходи, які реалізують [матеріальні] принципи, вказані вище»[338].

Приклад: прикладом нормативного акта, у якому наголошено на принципі підзвітності, є доповнена у 2009 році[339] Директива про конфіденційність та електронні комунікації (2002/58/ЄС). Положення доповненої статті 4 Директиви зобов'язують «забезпечити реалізацію політики безпеки щодо обробки персональних даних». Таким чином, стосовно норм безпеки в цій Директиві законодавець вирішив, що необхідно внести обов'язкову вимогу мати і гарантувати політику безпеки.

Відповідно до висновку Робочої групи «Стаття 29»[340] суть підзвітності полягає в обов'язках контролера:

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

Таким чином, принцип підзвітності вимагає від контролера активно демонструвати відповідність нормам, а не просто чекати, доки суб'єкти персональних даних або наглядові органи вкажуть на недоліки.

338 ОЕСР (2013), Керівні принципи, що регулюють захист приватності та транскордонні потоки персональних даних, ст. 14.

339 *Директива 2009/136/ЕС* Європейського Парламенту та Ради від 25 листопада 2009 р., яка доповнює Директиву 2002/22/ЕС «Про універсальні послуги та права користувачів стосовно електронних мереж зв'язку та послуг, Директива 2002/58/ЕС «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.

340 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 даних		
Загальний регламент захисту персональних даних, стаття 6 (1) (a)	**згода**	*Рекомендація щодо профайлінгу*, статті 3.4 (b) та 3.6
СЄС, C-543/09, «“Deutsche Telekom” проти Федеративної Республіки Німеччини» *(Deutsche Telekom AG v. Bundesrepublik Deutschland)*, 2011		Оновлена Конвенція 108, стаття 5 (2)
СЄС, C-536/15, «“Tele2 (Netherlands) BV” та інші проти Управління споживачів та ринку (УСР)» *(Tele2 (Netherlands) BV and Others v. Autoriteit Consument en Markt (AMC)*, 2017		
Загальний регламент захисту персональних даних, стаття 6 (1) (b)	**відносини до укладення договору**	Рекомендація щодо профайлінгу, стаття 3.4 (b)
Загальний регламент захисту персональних даних, стаття 6 (1) (c)	**юридичні обов’язки контролера**	Рекомендація щодо профайлінгу, стаття 3.4 (a)
Загальний регламент захисту персональних даних, стаття 6 (1) (d)	**життєво важливі інтереси суб’єкта персональних даних**	Рекомендація щодо профайлінгу, стаття 3.4 (b)

ЄС	питання, що висвітлюються	РЄ
Загальний регламент захисту персональних даних, стаття 6 (1) (e) СЄС, C-524/06, «Гайнц Губер проти Федеративної Республіки Німеччини» (*Huber v. Bundesrepublik Deutschland*) [ВП], 2008	**суспільний інтерес та виконання офіційних повноважень**	Рекомендація щодо профайлінгу, стаття 3.4 (b)
Загальний регламент захисту персональних даних, стаття 6 (1) (f) СЄС, C-13/16, «Служба з дорожньо-транспортних пригод поліції безпеки м. Риги проти тролейбусної компанії м. Риги» (*Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA 'Rīgas satiksme'*) 2017 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*), 2011	**легітимні інтереси інших осіб**	Рекомендація щодо профайлінгу, стаття 3.4 (b) ЄСПЛ, «Y проти Туреччини» (*Y v. Turkey*), № 648/10, 2015
Загальний регламент захисту персональних даних, стаття 6 (4)	**винятки з принципу обмеження цілі: подальша обробка для інших цілей**	Оновлена Конвенція 108, стаття 5 (4) (b)
Правила законної обробки чутливих даних		
Загальний регламент захисту персональних даних, стаття 9 (1)	**загальна заборона на обробку**	Оновлена Конвенція 108, стаття 6

ЄС	питання, що висвітлюються	РЄ
Загальний регламент захисту персональних даних, стаття 9 (2)	**винятки із загальної заборони на обробку**	Оновлена Конвенція 108, стаття 6
Безпекові правила процесу обробки		
Загальний регламент захисту персональних даних, стаття 32	**зобов'язання щодо забезпечення безпеки обробки**	Оновлена Конвенція 108, стаття 7 (1)
		ЄСПЛ, «I. проти Фінляндії» *(I v. Finland)*, № 20511/03, 2008
Загальний регламент захисту персональних даних, статті 28 та 32 (1) (b)	**зобов'язання щодо конфіденційності**	Оновлена Конвенція 108, стаття 7 (1)
Загальний регламент захисту персональних даних, стаття 34 Директива про конфіденційність і електронні комунікації, стаття 4 (2)	**повідомлення про порушення безпеки даних**	Оновлена Конвенція 108, стаття 7 (2)
Правила щодо підзвітності та сприяння відповідності		
Загальний регламент захисту персональних даних, статті 12, 13 та 14	**загальна прозорість**	Оновлена Конвенція 108, стаття 8
Загальний регламент захисту персональних даних, статті 37, 38 та 39	**спеціаліст із захисту персональних даних**	Оновлена Конвенція 108, стаття 10 (1)
Загальний регламент захисту персональних даних, стаття 30	**документування обробки даних**	
Загальний регламент захисту персональних даних, статті 35 та 36	**оцінка впливу та попередня консультація**	Оновлена Конвенція 108, стаття 10 (2)
Загальний регламент захисту персональних даних, статті 33 та 34	**повідомлення про витік даних**	Оновлена Конвенція 108, стаття 7 (2)
Загальний регламент захисту персональних даних, статті 40 та 41	**кодекси поведінки**	
Загальний регламент захисту персональних даних, статті 42 та 43	**сертифікація**	

ЄС	питання, що висвітлюються	РЄ
Захист даних за призначенням та за замовчуванням		
Загальний регламент захисту персональних даних, стаття 25 (1) (a)	**захист даних за призначенням**	Оновлена Конвенція 108, стаття 10 (2)
Загальний регламент захисту персональних даних, стаття 25 (1) (b)	**захист даних за замовчуванням**	Оновлена Конвенція 108, стаття 10 (3)

Принципи мають загальний характер. Їх застосування в конкретних ситуаціях залишає певне поле розсуду для тлумачення та вибору засобів. Право РЄ уповноважує сторони Оновленої Конвенції 108 роз'яснювати межі тлумачення в національному законодавстві. У праві ЄС ситуація інша: було визнано, що для того, щоб запровадити захист персональних даних на внутрішньому рівні, необхідно визначити більш конкретні норми на рівні ЄС, відповідно до яких треба гармонізувати національні закони держав-членів про захист персональних даних. Загальний регламент захисту персональних даних передбачає низку детальних правил згідно з принципами, викладеними в статті 5, які прямо застосовні в національному правопорядку. Тому викладені далі зауваження щодо конкретних правил захисту персональних даних на європейському рівні стосуються переважно правової системи ЄС.

4.1 Правила законної обробки даних

Ключові моменти

- Персональні дані обробляються законно, якщо вони відповідають одному із наступних критеріїв:
  - обробка здійснюється на підставі згоди суб'єкта персональних даних;
  - обробка даних вимагається договірними відносинами;
  - обробка даних необхідна для дотримання контролером юридичного обов'язку;
  - обробка даних вимагається для дотримання життєво важливих інтересів суб'єктів персональних даних або інших осіб;
  - обробка даних необхідна для виконання завдання в суспільних інтересах;

- легітимні інтереси контролерів або інших осіб є підставою для обробки, але тільки якщо їх не переважають інтереси або основоположні права суб'єктів даних.

- Законна обробка чутливих даних є предметом спеціальних, суворіших вимог.

4.1.1 Законні підстави обробки даних

Розділ II Загального регламенту захисту персональних даних під назвою «Принципи» передбачає, що вся обробка персональних даних, по-перше, повинна здійснюватись з дотриманням принципів щодо якості даних, передбачених статтею 5 ЗРЗПД. Один із принципів передбачає, що персональні дані повинні «оброблятись законно, чесно та прозоро». По-друге, для того, щоб дані оброблялися законно, обробка має відповідати одній із законних підстав, які роблять обробку даних правомірною і які перераховані в статті 6[341] для нечутливих даних та в статті 9 – для особливих категорій даних (або чутливих даних). Аналогічно розділ II Оновленої Конвенції 108, у якому йдеться про «основні принципи захисту персональних даних», визначає, що для того, щоб вважатися правомірною, обробка даних повинна бути «пропорційною до легітимної мети, яка переслідується».

Незалежно від законних підстав обробки, на які посилається контролер для здійснення операцій з обробки даних, контролер також має застосувати захисні заходи, передбачені загальним законодавством із захисту персональних даних.

Згода

Що стосується **права РЄ**, про згоду зазначено в статті 5 (2) Оновленої Конвенції 108. Про неї також йдеться у практиці ЄСПЛ та декількох рекомендаціях РЄ[342]. Що стосується **права ЄС**, згоду як основу законної обробки пер-

341 Рішення Суду ЄС C-465/00, C-138/01 та C-139/09, «Рахункова палата проти австрійської телерадіокомпанії "Österreichischer Rundfunk" та інших» та «Кріста Нойкомм і Джозеф Лауерманн проти австрійської телерадіокомпанії "Österreichischer Rundfunk"» (*Rechnungshof v. Österreichischer Rundfunk and Others and Christa Neukomm and Jospeh Lauermann v. Österreichischer Rundfunk*), від 20 травня 2003 р., п. 65; рішення Суду ЄС, C-524/06, «Гайнц Губер проти Федеративної Республіки Німеччини» (*Huber v. Germany*), [ВП], від 16 грудня 2008 р., п. 48; рішення Суду ЄС, 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.

342 Див., наприклад, Рада Європи, Комітет міністрів (2010), Рекомендація Комітету міністрів CM/Rec(2010)13 державам-членам про захист осіб стосовно автоматичної обробки персональних даних у контексті профайлінгу, від 23 листопада 2010 р., стаття 3.4 (b).

сональних даних чітко зафіксовано в статті 6 ЗРЗПД, а також відображено в статті 8 Хартії. Характерні ознаки чинної згоди роз'яснюються в самому визначені згоди в статті 4, водночас умови отримання чинної згоди перераховані в статті 7, а спеціальні правила щодо згоди дитини стосовно інформаційного суспільства встановлено в статті 8 ЗРЗПД.

Як пояснюється в розділі 2.4, згоду має бути надано добровільно, поінформовано, чітко визначено та однозначно. Згода має бути у формі заяви або чіткої стверджувальної дії, якою дозволяється обробка даних. Особа має право відкликати згоду в будь-який час. Контролери мають обов'язок зберігати записи про згоду, які можна перевірити.

Добровільна згода

Відповідно до положень Оновленої Конвенції 108 **РЄ** згода суб'єкта даних повинна «відображати вільне вираження наміреного вибору»[343]. Добровільна згода є чинною, «якщо суб'єкт даних здатен зробити справжній вибір за відсутності ризику введення в оману, залякування, примусу або значних негативних наслідків для себе у разі відмови від надання згоди»[344]. У цьому зв'язку **законодавство ЄС** передбачає, що згода не є вільно наданою, «якщо суб'єкт даних не має справжнього та вільного вибору або нездатен відмовитися, або відкликати згоду без негативних наслідків»[345]. У ЗРЗПД наголошується, що «при оцінці питання, чи була надана згода добровільно, найвищий рівень уваги має бути приділено питанню, *inter alia*, чи є надання згоди на обробку даних, які не є необхідними для виконання договору, умовою виконання договору або надання послуг»[346]. Пояснювальна записка до Оновленої Конвенції 108 передбачає, що «суб'єкт персональних даних не може бути підданий прямому чи непрямому неналежному впливу або тиску (які можуть бути економічного або іншого характеру), а згода не може вважатися вільно наданою, якщо суб'єкт даних не має справжнього вибору або нездатний відмовитися чи відкликати згоду без негативних наслідків»[347].

343 Пояснювальна записка до Оновленої Конвенції 108, п. 42.

344 Див. також Робоча група «Стаття 29» (2011), Висновок 15/2011 про поняття згоди, РГ 187, Брюссель, від 13 липня 2011 р., с. 12.

345 Загальний регламент захисту персональних даних, п. 42 преамбули.

346 Там само, стаття 7 (4).

347 Пояснювальна записка до Оновленої Конвенції 108, п. 42.

Приклад: деякі органи місцевого самоврядування в державі А вирішили виготовити картки, де вказано місце проживання, із вшитими чипами. Для мешканців отримання цієї електронної картки є необов'язковим. Однак мешканці, які не мають цієї картки, не мають доступу до низки важливих адміністративних послуг, таких як сплата місцевих податків онлайн, подання електронних скарг з триденним строком надання відповіді, навіть до купівлі квитків без черги для відвідання місцевої концертної зали та використання сканерів при вході.

Обробку даних органами місцевої влади в цьому випадку не може бути здійснено на підставі згоди. Оскільки існує щонайменше опосередкований тиск на мешканців в отриманні електронної картки, згода не є вільно наданою. Відповідно, розвиток системи електронних карток має ґрунтуватись на іншій легітимній підставі, яка виправдовує обробку. Наприклад, місцеві органи влади можуть посилатись на те, що це необхідно для виконання завдання в суспільних інтересах, що є законною підставою для обробки даних відповідно до статті 6 (1)(e) ЗРЗПД[348].

Добровільна згода також може бути сумнівною у випадках субординації, коли існує значний економічний або інший дисбаланс між контролером, який забезпечує згоду, та суб'єктом даних, який надає згоду[349]. Типовим прикладом такого дисбалансу та субординації є обробка персональних даних роботодавцем у контексті трудових відносин. Робоча група «Стаття 29» зазначає, що «працівники практично ніколи не мають можливості надання вільної згоди, відмови або відкликання згоди, виходячи з залежності, яка випливає з відносин роботодавця і працівника. Враховуючи нерівні умови, працівники можуть надати добровільну згоду за виняткових обставин, коли ніякі наслідки взагалі не пов'язані з прийняттям або відмовою у прийнятті пропозиції»[350].

348 Робоча група «Стаття 29» (2011), Висновок 15/2011 про поняття згоди, РГ 187, Брюссель, від 13 липня 2011 р., с. 16. Додаткові приклади справ, у яких обробка даних не може ґрунтуватися на згоді, а вимагає іншої юридичної підстави для легітимізації обробки, можна знайти в пп. 14 та 17 висновку.

349 Див. також Робоча група «Стаття 29» (2001), Висновок 8/2001 про обробку даних у трудовій сфері, РГ 48, Брюссель, від 13 вересня 2001 р.; РГ «Стаття 29» (2005), Робочий документ про спільне тлумачення, стаття 26 (1) Директиви 95/46/ЕС від 24 жовтня 1995 р., РГ 114, Брюссель, від 25 листопада 2005 р.; РГ «Стаття 29» (2017), Висновок 2/2017 про обробку даних на роботі, РГ 249, Брюссель, від 8 червня 2017 р.

350 Робоча група «Стаття 29», *Висновок 2/2017 про обробку даних на роботі*, РГ 249, Брюссель, від 8 червня 2017 р.

Приклад: велика компанія спланувала створити довідкову книгу, яка містить імена працівників, їхні обов'язки в компанії та їхні робочі адреси, виключно з метою покращити внутрішню комунікацію в компанії. Керівник відділу кадрів запропонував додати до книги фото кожного працівника, щоб було легше впізнати колег на засіданнях. Представник працівників наполягав, що це можливо, лише якщо працівники нададуть згоду.

У такій ситуації згоду працівників може бути визнано юридичною підставою для обробки фото для книги, оскільки дійсно працівники не матимуть ніяких наслідків, якщо він або вона вирішать погодитись або ні на вміщення своїх фото в книзі.

Приклад: компанія А планує зустріч між трьома своїми працівниками та директорами компанії В для обговорення потенційної майбутньої взаємодії в певному проєкті. Зустріч буде відбуватись у приміщенні компанії В, яка вимагає в компанії А направити електронною поштою імена, резюме та фото учасників зустрічі. Компанія В пояснює, що їй необхідні імена та фото учасників для того, щоб служба охорони при вході до будівлі могла перевірити, що це саме ті особи, а резюме допоможе директорам краще підготуватися для зустрічі. У цьому випадку передача персональних даних працівників компанії А не може ґрунтуватися на згоді. Така згода не може вважатися «вільно наданою», оскільки існує можливість того, що працівники можуть зазнати негативних наслідків, якщо вони відмовляться від пропозиції (наприклад, їх можуть замінити на інших працівників не тільки для участі в зустрічі, але й також для укладення угоди з компанією В та участі в проєкті загалом). Відповідно, обробка має ґрунтуватися на іншій законній підставі.

Однак, це не означає, що згода ніколи не може бути чинною за обставин, коли її ненадання матиме певні негативні наслідки. Наприклад, якщо ненадання згоди на отримання картки покупця супермаркету може призвести лише до відсутності маленької знижки на певні продукти, згода може бути чинною законною підставою для обробки персональних даних тих покупців, які погодилися мати таку картку. У такому випадку відсутня субординація між компанією та покупцем, та наслідки ненадання згоди недостатньо серйозні для перешкоджання суб'єкту даних зробити вільний вибір (за умови, що зменшення ціни є достатньо незначним, щоб не вплинути на його вільний вибір).

Водночас, якщо товари та послуги можуть бути отримані лише за умови відкриття персональних даних контролеру або в подальшому третій стороні, згода суб'єкта на відкриття своїх даних, які не є необхідними для договору, не може вважатись вільним рішенням та, відповідно, чинною за законодавством про персональні дані[351]. ЗРЗПД є достатньо жорстким у забороні прив'язування згоди до надання товарів або послуг[352].

Приклад: угода пасажирів з авіакомпаніями, які передають так звані реєстраційні дані пасажирів (тобто їхні ідентифікаційні дані, інформацію про харчові звички або проблеми зі здоров'ям) міграційним службам відповідних іноземних держав, не може вважатися чинною згодою відповідно до законодавства із захисту персональних даних, оскільки подорожуючи пасажири не мають вибору, якщо вони хочуть відвідати цю державу. Для того, щоб така передача була законною, вимагається інша, ніж згода, законна підстава, швидше за все спеціальний закон.

Поінформована згода

Суб'єкт даних повинен мати достатню інформацію перед тим, як робити свій вибір. Поінформована згода, як правило, передбачає точний та легкозрозумілий опис предмета, який вимагає згоди. Як пояснює Робоча група «Стаття 29», згода має ґрунтуватися на оцінці та розумінні фактів і наслідків надання згоди на обробку даних суб'єктом персональних даних. Відповідно, «згода фізичної особи повинна бути надана в ясний та зрозумілий спосіб, маючи точну та повну інформацію про відповідні питання [...] такі, як характер даних, що підлягатимуть обробці, цілі обробки, можливих одержувачів та права суб'єкта даних»[353]. Для того, щоб згода була поінформованою, фізичні особи також мають бути обізнані з наслідками ненадання згоди на обробку.

З огляду на важливість поінформованої згоди ЗРЗПД та Пояснювальна записка до Оновленої Конвенції 108 намагалися прояснити це поняття. Положення загальної частини ЗРЗПД вказують, що поінформована згода означає, що

351 Загальний регламент захисту персональних даних, стаття 7 (4).

352 Там само.

353 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.

«суб'єкт даних має бути обізнаним щонайменше з ідентифікаційними даними контролера та цілями обробки», для яких надаються персональні дані[354].

У винятковому випадку, якщо згода використовується як відступ з метою забезпечення законної підстави для міжнародної передачі даних, контролер повинен поінформувати суб'єкта даних про можливі ризики такої передачі в зв'язку з відсутністю рішення про відповідність та належних гарантій для того, щоб така згода вважалась чинною[355].

Пояснювальна записка до Оновленої Конвенції 108 вказує, що має бути надана інформація про наслідки рішення суб'єкта даних, а саме «до яких фактів призведе згода та обсяг, на який погоджується суб'єкт даних»[356].

Якість інформації є важливою. Якість інформації означає, що мова інформації має бути адаптована для її передбачуваних отримувачів. Інформація має бути надана без використання жаргону, зрозумілою та простою мовою, яку здатний зрозуміти звичайний користувач[357]. Інформація також має бути легкодоступною для суб'єкта персональних даних, може бути надана усно або письмово. Доступність та наочність інформації є важливими елементами: інформація має бути чітко наочною та помітною. В онлайн-середовищі хорошим рішенням можуть бути багаторівневі інформаційні повідомлення, оскільки це дозволяє суб'єкту даних вибрати, чи мати доступ до стислої або більш розширеної версії інформації.

Точно визначена згода

Для того, щоб згода була чинною, вона має бути точно визначеною відносно цілі обробки, яка має бути чітко описана в однозначних формулюваннях. Це тісно пов'язано з якістю інформації, яка надається щодо цілі згоди. У цьому контексті варто зважати на слушні очікування середньостатистичного суб'єкта даних. Суб'єкта даних знову мають запитати про згоду, якщо операції з обробки даних додаються або змінюються у спосіб, який неможливо було розумно передбачити при наданні початкової згоди, отже, змінюється ціль обробки. Коли обробка має декілька цілей, згода має надаватися щодо кожної з них[358].

354 Загальний регламент захисту персональних даних, п. 42 преамбули.

355 Там само, стаття 49 (1) (a).

356 Пояснювальна записка до Оновленої Конвенції 108, п. 42.

357 Робоча група «Стаття 29» (2011), *Висновок 15/2011 про поняття згоди*, РГ187, Брюссель, від 13 липня 2011 р., с. 19.

358 Загальний регламент захисту персональних даних, п. 32 преамбули.

Приклад: у справі «*Deutsche Telekom AG*»[359] Суд ЄС розглянув питання, чи потрібно було телекомунікаційному оператору, який мав передати персональні дані підписників для публікації в каталозі, поновлювати згоду суб'єктів даних[360], оскільки отримувачів даних не було названо, коли надавалася перша згода.

СЄС вирішив, що відповідно до статті 12 Директиви про конфіденційність та електронні комунікації поновлення згоди не вимагалося до передання персональних даних. Оскільки суб'єкти даних мали лише один варіант згоди на ціль обробки, якою була публікація їхніх даних, вони не могли обирати між різними каталогами, де ці дані можуть друкуватись.

Як підкреслив СЄС, «як випливає з контекстуального та системного тлумачення статті 12 Директиви про конфіденційність та електронні комунікації, згода за статтею 12 (2) стосується мети публікації персональних даних у публічному каталозі, а не ідентифікаційних даних конкретного каталогу»[361]. На додаток «сама публікація персональних даних як така в публічному каталозі з чіткою метою могла мати негативні наслідки для підписників»[362], а не питання ідентифікації видавця.

Приклад: справа *«"Tele2 (Netherlands) BV" та інші проти Управління споживачів та ринку (УСР)»*[363] стосувалася запиту бельгійської компанії про надання довідковим службам та каталогам доступу до даних підписників компаній, які надавали телефонні номери в Нідерландах. Бельгійська компанія посилалася на обов'язок, передбачений Директивою про універсальні послуги[364]. Вона вимагала від компаній,

359 Рішення Суду ЄС, C-543/09, «"Deutsche Telekom" проти Федеративної Республіки Німеччини» (*Deutsche Telekom AG v. Bundesrepublik Deutschland*), від 5 травня 2011 р. Див. пп. 53 та 54.

360 Директива Європейського парламенту та Ради 2002/58/ЕС про обробку персональних даних та захист таємниці в секторі електронних комунікацій, OJ 2002 L 201 (Директива про конфіденційність і електронні комунікації).

361 Рішення Суду ЄС, C-543/09, «"Deutsche Telekom" проти Федеративної Республіки Німеччини» (*Deutsche Telekom AG v. Bundesrepublik Deutschland*), від 5 травня 2011 р.; п. 61.

362 Там само, п. 62.

363 Рішення Суду ЄС, C-536/15, «"Tele2 (Netherlands) BV" та інші проти Управління споживачів та ринку (УСР)» (*Tele2 (Netherlands) BV and Others v. Autoriteit Consument en Markt (AMC)*), від 15 березня 2017 р.

364 Директива 2009/136/ЕС Європейського Парламенту та Ради від 25 листопада 2009 р., яка доповнює Директиву 2002/22/ЕС «Про універсальні послуги та права користувачів стосовно електронних мереж зв'язку та послуг, Директива 2002/58/ЕС «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.

що надають телефонні номери, зробити номери доступними для каталогів, які їх вимагають, якщо підписники надали згоду на публікацію імен. Компанії Нідерландів відмовилися передати дані, стверджуючи, що від них не вимагалося передавати дані за зобов'язанням, встановленим в іншій державі-учасниці. Вони стверджували, що користувачі надали свою згоду на публікацію своїх даних, розуміючи, що їх розмістять в каталозі Нідерландів. СЄС вирішив, що Директива про універсальні послуги охоплює всі запити підприємств-довідкових служб, незалежно від держави-члена, у якій вони були створені. СЄС також вирішив, що передача тих самих персональних даних іншому підприємству, яке має намір опублікувати публічний каталог без отримання додаткової згоди від підписників, не може нанести суттєву шкоду праву на захист персональних даних[365]. Таким чином, підприємствам, які надають телефонні номери своїм підписникам, немає необхідності розрізняти в запиті на отримання згоди, адресованому підписнику, держави-члени, до яких їхні персональні дані можуть бути надіслані[366].

Однозначна згода

Згоду має бути надано однозначно[367]. Це означає, що не може бути жодного розумного сумніву, що суб'єкт даних хотів висловити своє волевиявлення у вигляді дозволу на обробку своїх даних. Тож пасивність суб'єкта даних не свідчить про однозначну згоду.

Наприклад, так буде у випадку, коли контролер отримує згоду суб'єкта даних, застосовуючи таку форму у своїх правилах конфіденційності: «використовуючи наш сервіс, ви надаєте згоду на обробку персональних даних». У такому випадку контролери мають пересвідчитися, що користувачі вручну та індивідуально погоджуються з такими правилами.

Якщо згоду надано в письмовій формі, яка є частиною договору, згода на обробку персональних даних має бути індивідуалізована та у будь-якому випадку «мають існувати гарантії, що суб'єкт даних знає про факт надання згоди та її обсяг»[368].

365 Рішення Суду ЄС, C-536/15, «"Tele2 (Netherlands) BV" та інші проти Управління споживачів та ринку (УСР)» (*Tele2 (Netherlands) BV and Others v. Autoriteit Consument en Markt (AMC)*), від 15 березня 2017 р., п. 36.

366 Там само, пп. 40–41.

367 Загальний регламент захисту персональних даних, стаття 4 (11).

368 Там само, п. 42 преамбули.

Вимоги щодо згоди дітей

ЗРЗПД передбачає спеціальний захист для дітей у контексті надання послуг інформаційного суспільства, оскільки «вони можуть бути менш обізнаними з ризиками, наслідками та гарантіями щодо своїх прав стосовно обробки персональних даних»[369]. Таким чином, відповідно до **законодавства ЄС**, коли надавачі послуг інформаційного суспільства обробляють персональні дані дітей віком до 16 років на підставі згоди, така обробка буде законною «лише у випадку, якщо згоду надано або погоджено законним представником дитини, та лише в тій мірі, в якій останній її надав або погодив»[370]. Держави-члени можуть передбачити менший вік у національному законі, хоча не менше ніж 13 років[371]. Згода законного представника не вимагається, «якщо обробка здійснюється в контексті надання превентивних або консультативних послуг, пропонованих напряму дитині»[372]. Інформація та повідомлення у випадках обробки даних дитини мають подаватися чіткою та простою мовою, легкозрозумілою дитині[373].

Право відкликати згоду в будь-який час

ЗРЗПД включає загальне право відкликати згоду в будь-який час[374]. Суб'єкт даних повинен бути поінформований про таке право до моменту надання згоди і може реалізувати це право на власний розсуд. Не може бути вимоги пояснювати причини відклику, а також не може бути жодного ризику негативних наслідків, крім тих, що пов'язані з припиненням надання переваг, які можуть випливати із попередньо домовленого використання даних. Відклик згоди має бути так само легким, як і її надання[375]. Не може бути вільної згоди, якщо суб'єкт даних не може відкликати свою згоду без негативних наслідків, або якщо відкликання не є таким же легким, яким було надання згоди[376].

369 Там само, п. 38 преамбули.

370 Там само, стаття 8 (1). Поняття послуг інформаційного суспільства визначено в статті 4 (25) Загального регламенту про захист персональних даних.

371 Загальний регламент захисту персональних даних, стаття 8 (1), друге речення.

372 Там само, п. 38 преамбули.

373 Там само, п. 58 преамбули. Див. також Оновлену Конвенцію 108, стаття 15 (2) (e). Пояснювальна записка до Оновленої Конвенції 108, пп. 68 та 125.

374 Загальний регламент захисту персональних даних, стаття 7 (3). Пояснювальна записка до Оновленої Конвенції 108, п. 45.

375 Загальний регламент захисту персональних даних, стаття 7 (3).

376 Загальний регламент захисту персональних даних, п. 42 преамбули; Пояснювальна записка до Оновленої Конвенції про захист персональних даних 108, п. 42.

Приклад: покупець погоджується на отримання рекламної інформації на електронну адресу, яку він або вона надає контролеру. Як тільки покупець відкликає свою згоду, контролер має негайно припинити надсилати рекламні листи. Жодних каральних заходів, як-от витрати, не може бути накладено. Відкликання, однак, має наслідки лише для майбутнього та не має зворотного ефекту. Період, протягом якого персональні дані покупця оброблялися законно – завдяки його згоді – був легітимним. Відкликання згоди запобігає будь-якій подальшій обробці цих даних, якщо така обробка не відповідає праву на видалення даних[377].

Необхідність виконання договору

Відповідно до **законодавства ЄС,** стаття 6 (1)(b) ЗРЗПД передбачає іншу підставу для правомірної обробки, а саме якщо вона «необхідна для виконання договору, стороною якого є суб'єкт персональних даних». Це положення також охоплює відносини до укладення договору. Наприклад, у справах, у яких сторона має намір укласти договір, але ще цього не зробила, можливо в зв'язку з незакінченими певними перевірками. Якщо одна сторона потребує обробки даних для цієї цілі, така обробка є законною настільки довго, наскільки це «необхідно для здійснення кроків за вимогою суб'єкта даних до укладення договору»[378].

Таке поняття обробки даних як «правомірна підстава, передбачена законом» у статті 5 (2) Оновленої Конвенції 108 також охоплює «обробку даних для виконання договору (або заходів до укладення договору на вимогу суб'єкта персональних даних), стороною якого є суб'єкт даних»[379].

Юридичні обов'язки контролера

Право ЄС передбачає ще одну підставу правомірної обробки, а саме якщо «обробка є необхідним для дотримання встановленого законом зобов'язання, яке поширюється на контролера» (Стаття 6 (1)(c) ЗРЗПД). Це положення охоплює як контролерів, що діють у приватному секторі, так тих, що діють у державній сфері; юридичний обов'язок контролерів державного сектору також може охоплюватися статтею 6 (1)(e) ЗРЗПД. Існує багато прикладів ситуацій, у яких закон

377 Загальний регламент захисту персональних даних, стаття 17 (1) (b).

378 Там само, стаття 6 (1) (b).

379 Пояснювальна записка до Оновленої Конвенції 108, п.. 46; Рада Європи, Комітет міністрів (2010), Рекомендація Комітету міністрів CM/Rec(2010)13 державам-членам про захист осіб стосовно автоматичної обробки персональних даних у контексті профайлінгу, від 23 листопада 2010 р., стаття 3.4 (b).

зобов'язує контролерів приватного сектору обробляти персональні дані конкретного суб'єкта даних. Наприклад, роботодавці повинні обробляти дані своїх працівників для соціального страхування та оподаткування, а комерційні компанії мають обробляти дані своїх покупців в цілях сплати податків.

Юридичний обов'язок може випливати із законодавства ЄС або держави-учасниці, яке може бути підставою для однієї чи декількох операцій з обробки. Саме закон має визначати цілі обробки, запроваджувати специфікації для визначення контролера, види персональних даних суб'єкта, які підлягають обробці, суб'єктів даних, яких це стосується, підприємства, яким дані можуть бути відкриті, обмеження цілей, період зберігання та інші заходи для забезпечення законної та чесної обробки[380]. Будь-який такий закон, що є основою обробки персональних даних, має відповідати статтям 7 та 8 Хартії та статті 8 ЄКПЛ.

Юридичний обов'язок контролера також є підставою для правомірної обробки відповідно до **права РЄ**[381]. Як зазначалося раніше, юридичний обов'язок контролера приватного сектору є лише одним із спеціальних випадків легітимного інтересу інших осіб, про який йдеться в статті 8 (2) ЄСПЛ. Приклад обробки роботодавцем даних про його працівників також застосовний до права РЄ.

Життєво важливі інтереси суб'єкта даних або іншої фізичної особи

Згідно **з законодавством ЄС,** стаття 6 (1)(d) ЗРЗПД вказує, що обробка персональних даних також є законною, якщо «вона необхідна для захисту життєво важливих інтересів суб'єкта даних або іншої фізичної особи». Це може бути правомірною підставою для обробки персональних даних з огляду на життєво важливі інтереси іншої фізичної особи, лише якщо така обробка «очевидно не може здійснюватись на іншій законній підставі»[382]. Інколи певний вид обробки може здійснюватись як на підставі суспільного інтересу, так і на підставі життєво важливих інтересів суб'єкта даних або іншої фізичної особи. Наприклад, у ситуації моніторингу епідемії та її розвитку або у випадку надзвичайної ситуації гуманітарного характеру.

Відповідно до **права РЄ** життєво важливі інтереси суб'єкта даних не зазначені в статті 8 ЄКПЛ. Однак життєво важливі інтереси суб'єкта даних вважаються

380 Загальний регламент захисту персональних даних, п. 45 преамбули.

381 Рекомендація Комітету міністрів CM/Rec(2010)13 державам-членам про захист осіб стосовно автоматичної обробки персональних даних у контексті профайлінгу, від 23 листопада 2010 р., стаття 3.4 (a).

382 Загальний регламент захисту персональних даних, п. 46 преамбули.

включеними в поняття «правомірна підстава» в статті 5 (2) Оновленої Конвенції 108, яка врегульовує питання правомірності обробки персональних даних[383].

Суспільний інтерес та виконання офіційних повноважень

Враховуючи багатоманітність способів організації публічних справ, стаття 6 (1) (e) ЗРЗПД передбачає, що обробка персональних даних може бути законною у разі, якщо «вона необхідна для виконання завдань у суспільних інтересах або для виконання офіційних повноважень, покладених на контролера [...]»[384].

Приклад: у справі *«Губер проти Німеччини»*[385] пан Губер, громадянин Австрії, що проживає в Німеччині, звернувся до Федерального відомства з питань міграції та біженців з проханням вилучити 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 осіб у злочинній діяльності або такій, що 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 95/46[386], персональні дані можуть законно оброблятися за умови, якщо це необхідно для виконання завдання, здійснюваного в суспільних інтересах, чи при виконанні офіційних повноважень.

На думку СЄС, «враховуючи ціль забезпечення однакового захисту в усіх державах-членах, передбачене у статті 7 (e) Директиви 95/46[387] поняття необхідності [...] не може бути різним у державах-членах. З цього

383 Пояснювальна записка до Оновленої Конвенції 108, п. 46.

384 Загальний регламент захисту персональних даних, п. 45 преамбули.

385 Рішення Суду ЄС, C-524/06, «Гайнц Губер проти Федеративної Республіки Німеччини» *(Heinz Huber v. Bundesrepublik Deutschland)*, [ВП], від 16 грудня 2008 р.

386 Колишня Директива про захист персональних даних, стаття 7 (e), тепер Загальний регламент захисту персональних даних, стаття 6 (1) (e).

387 Там само.

випливає, що дане питання є концепцією, яка має своє незалежне значення у праві Співтовариства і повинна тлумачитись у спосіб, який повністю відображає закладену в статті 1 (1) ціль вказаної Директиви[388].

Суд зазначає, що здійснення права громадянина держави-члена ЄС щодо вільного пересування територією держави-члена, громадянином якої він чи вона не є, не є абсолютним і може бути предметом обмежень і умов, встановлених Договором про створення Європейського Співтовариства 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 лише ті дані, які необхідні для застосування такого закону, а централізований характер системи сприяє ефективнішому його застосуванню. Національний суд має встановити, чи дотримано цих умов в даному конкретному випадку. Якщо ні, то збереження і обробка персональних даних у такому реєстрі, як AZR, для статистичних цілей не може, за будь-яких підстав, вважатися необхідною у розумінні статті 7 (e)[389] Директиви 95/46 /ЕС[390].

Нарешті, стосовно питання використання даних реєстру для цілей боротьби зі злочинністю СЄС вирішив, що до таких цілей «обов'язково включено мету судового 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 ця різниця в поводженні є дискримінацією, заборону якої передбачено у статті 18 ДфЄС. Отже, у тлумаченні СЄС 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»[391].

388 Рішення Суду ЄС, C-524/06, «Гайнц Губер проти Федеративної Республіки Німеччини» (*Heinz Huber v. Bundesrepublik Deutschland*), [ВП], від 16 грудня 2008 р., п. 52.

389 Колишня Директива про захист персональних даних, стаття 7 (e), тепер Загальний регламент захисту персональних даних, стаття 6 (1) (e).

390 Рішення Суду ЄС, C-524/06, «Гайнц Губер проти Федеративної Республіки Німеччини» (*Heinz Huber v. Bundesrepublik Deutschland*), [ВП], від 16 грудня 2008 р., п. 54, 58–59 та 66–68.

391 Там само, пп. 78 та 81.

Використання персональних даних органами влади, які діють у публічній сфері, також охоплюється статтею 8 ЄКПЛ та, якщо це застосовно, статтею 5 (2) Оновленої Конвенції 108[392].

Легітимні інтереси контролера або третьої особи

Відповідно до **права ЄС** суб'єкт даних не є єдиним, хто має легітимні інтереси. Стаття 6 (1)(f) ЗРЗПД передбачає, що персональні дані можуть законно оброблятись, якщо «це необхідно для цілей легітимного інтересу, що переслідується контролером, або третьої стороною, або сторонами [крім органів влади при виконанні своїх завдань], яким відкриваються персональні дані, крім випадків, коли над такими інтересами переважають інтереси або основоположні права та свободи суб'єкта даних, що потребують захисту [...]»[393].

Наявність легітимного інтересу має бути ретельно оцінена в кожному конкретному випадку[394]. Якщо легітимні інтереси контролера визначені, тоді проводиться пошук балансу між цими інтересами та інтересами або основоположними правами та свободами суб'єкта даних[395]. Обґрунтовані очікування суб'єкта даних мають бути враховані під час здійснення такої оцінки, щоб переконатись у тому, що інтереси контролера переважають над інтересами або основоположними правами суб'єкта даних[396]. Якщо права суб'єкта даних переважають над легітимними інтересами контролера, тоді контролер може вжити заходів та застосувати захисні гарантії, щоб забезпечити мінімізацію впливу на права суб'єкта даних (такі, як псевдонімізація даних) та змінити «баланс» до отримання можливості правомірно посилатися на цю легітимну підставу для обробки. У своєму висновку щодо поняття легітимних інтересів контролера даних Робоча група «Стаття 29» підкреслила ключову роль підзвітності та прозорості, а також прав суб'єкта даних заперечувати проти обробки його даних або аналізу даних, права на зміну, вилучення або передання даних при здійсненні балансування легітимних інтересів контролера та інтересів основоположних прав суб'єкта даних[397].

392 Пояснювальна записка до Оновленої Конвенції 108, пп. 46 та 47.

393 У порівнянні з Директивою 95/46, Загальний регламент захисту персональних даних передбачає більшу кількість випадків, які вважаються легітимним інтересом.

394 Загальний регламент захисту персональних даних, п. 47 преамбули.

395 Робоча група «Стаття 29» (2014), *Висновок 06/2014 про поняття легітимних інтересів контролера відповідно до статті 7 Директиви 95/46/ЄС*, від 4 квітня 2014 р.

396 Там само.

397 Там само.

У пунктах загальної частини ЗРЗПД надано певні приклади того, що становить легітимний інтерес контролера даних. Наприклад, дозволяється обробка даних без згоди суб'єкта даних, якщо вона здійснюється для цілей прямого маркетингу, або якщо така обробка є «суворо необхідною для цілей попередження шахрайства»[398].

У практиці СЄС є детальніша інформація щодо визначення, що становить легітимний інтерес.

Приклад: справа «*Служба з дорожньо-транспортних пригод поліції безпеки м. Риги*»[399] стосувалася шкоди, завданої ризькій транспортній тролейбусній компанії пасажиром, який раптово відчинив двері таксі. Ризька тролейбусна компанія хотіла позиватися до пасажира для стягнення шкоди. Однак поліція могла надати лише прізвище пасажира та відмовилася надавати номер документа, що посвідчує особу пасажира, його адресу проживання, стверджуючи, що таке відкриття персональних даних становитиме порушення закону про захист персональних даних.

Латвійський суд звернувся до Суду ЄС із запитом про винесення попереднього рішення з питання, чи зобов'язує законодавство із захисту персональних даних ЄС відкрити всі персональні дані, які необхідні для ініціювання цивільного провадження проти особи, яка, як стверджується, відповідальна за адміністративне правопорушення[400].

СЄС роз'яснив, що законодавство із захисту персональних даних ЄС передбачає можливість – але не обов'язок – повідомлення персональних даних третій стороні для цілей легітимних інтересів, які переслідуються цією стороною[401]. СЄС встановив три критерії, які сукупно мають бути дотримані для того, щоб обробка персональних даних була законною на підставі «легітимних інтересів»[402]. По-перше, третя особа, якій відкриваються персональні дані, повинна переслідувати легітимний інтерес. У цій конкретній справі це означає, що вимога надати особисту інформацію для подання позову проти особи про відшкодування шкоди становить

398 Загальний регламент захисту персональних даних, п. 47 преамбули.

399 Рішення Суду ЄС, C-13/16, «Служба з дорожньо-транспортних пригод поліції безпеки м. Риги проти тролейбусної компанії м. Риги» (*Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA 'Rīgas satiksme'*), від 4 травня 2017 р.

400 Там само,п. 23.

401 Там само, п. 26.

402 Там само, пп. 28–34.

легітимний інтерес третьої особи. По-друге, обробка персональних даних має бути необхідною для цілей легітимного інтересу, який переслідується. У цій справі отримання таких даних як адреса та номер документа, що посвідчує особу, є абсолютно необхідними для ідентифікації тієї особи. По-третє, основоположні права суб'єкта даних не мають бути більш важливими, ніж легітимні інтереси контролера або третіх осіб. Баланс інтересів повинен досліджуватися в кожній конкретній справі з урахуванням таких елементів, як серйозність порушення прав суб'єкта даних або навіть вік суб'єкта за певних обставин. Однак у цій конкретній справі Суд ЄС не пристав до позиції, що відмова у відкритті даних була б виправданою просто тому, що суб'єкт даних є неповнолітнім.

У рішенні *ASNEF* та *FECEMD* СЄС вирішував питання щодо обробки персональних даних на юридичній підставі «легітимних інтересів», що в той час була передбачена статтею 7 (f) Директиви про захист персональних даних[403].

Приклад: у справі «*Національна асоціація кредитних фінансових установ (ASNEF) і Федерація електронної комерції і прямого маркетингу (FECEMD)*»[404] Суд ЄС надав роз'яснення, що національне законодавство не може доповнювати положення статті 7 (f) Директиви додатковими умовами щодо законності обробки даних[405]. Це стосується ситуації із законом Іспанії «Про захист персональних даних», який містив положення, згідно з яким будь-які фізичні особи могли заявляти про свої легітимні інтереси на обробку персональних даних лише за умови оприлюднення інформації в публічних джерелах.

Суд передусім зазначив, що метою Директиви 95/46/ЄС[406] є забезпечення належного рівня захисту прав і свобод осіб при здійсненні обробки

403 Колишня Директива про захист персональних даних, стаття 7 (f), тепер Загальний регламент захисту персональних даних, стаття 6 (1) (f).

404 Рішення Суду ЄС, 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*), від 24 листопада 2011 р.

405 Колишня Директива про захист персональних даних, стаття 7 (f), тепер Загальний регламент захисту персональних даних, стаття 6 (1) (f).

406 Колишня Директива про захист персональних даних, тепер Загальний регламент захисту персональних даних.

персональних даних у всіх державах-членах. Результатом гармонізації національних законів, що діють у цій сфері, не повинне бути зниження наявного в них рівня захисту. Натомість її метою має бути забезпечення високого рівня захисту персональних даних у ЄС[407]. Отже, СЄС постановив, що «саме метою забезпечення належного рівня захисту в усіх державах-членах обумовлено викладення у статті 7 Директиви 95/46[408] вичерпного та обмежувального переліку умов, за яких обробка персональних даних може вважатися законною». Окрім того, «держави-члени не можуть доповнювати статтю 7 Директиви 95/46[409] новими принципами законності обробки персональних даних або додавати вимоги, якими може бути змінено сферу дії одного з шести принципів, передбачених у статті 7»[410]. 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 в результаті обробки може варіюватися залежно від наявності чи відсутності цих даних у публічних джерелах».

Більше того, «положення статті 7 (f) Директиви чітко і повно застерігають державу-члена від можливості здійснювати обробку певних категорій персональних даних без забезпечення балансу між конфліктними правами та інтересами в кожному конкретному випадку».

З огляду на ці міркування Суд дійшов висновку, що «положення статті 7 (f) Директиви 95/46[411] слід тлумачити як такі, що виключають національні норми, які, за відсутності згоди суб'єкта персональних даних і з метою надання дозволу на здійснення обробки цих персональних даних суб'єкта даних, необхідних для досягнення легітимних інтересів контролера персональних даних або третьої сторони або сторін, яким ці дані

407 Рішення Суду ЄС, 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*), від 24 листопада 2011 р., п. 28; Директива про захист персональних даних, пп. 8 та 10 преамбули.

408 Колишня Директива про захист персональних даних, стаття 7, тепер Загальний регламент захисту персональних даних, стаття 6 (1) (f).

409 Колишня Директива про захист персональних даних, стаття 7, тепер Загальний регламент захисту персональних даних, стаття 6.

410 Там само.

411 Колишня Директива про захист персональних даних, стаття 7 (f), тепер Загальний регламент захисту персональних даних, стаття 6 (1) (f).

розкриваються, вимагають дотримання не лише основоположних прав і свобод суб'єкта персональних даних, а й також оприлюднення даних у публічних джерелах, тим самим категорично і сповна виключає можливість обробки даних, які відсутні у таких джерелах»[412].

У будь-який момент обробки персональних даних на підставі «легітимних інтересів» особа має право заперечувати проти обробки з огляду на свою конкретну ситуацію відповідно до статті 21 (1) ЗРЗПД. Контролер повинен зупинити обробку, якщо він не продемонструє переконливі правомірні підстави продовжувати її.

Щодо **права РЄ**, подібні формулювання можна знайти в Оновленій Конвенції 108[413] та рекомендаціях РЄ. Рекомендація щодо профайлінгу визнає здійснення обробки персональних даних для легітимних цілей профайлінгу, якщо необхідно – для легітимних інтересів інших осіб, «за винятком, коли над такими інтересами переважають основоположні права і свободи суб'єктів персональних даних»[414]. На додаток, «захист прав та свобод інших» зазначено в статті 8(2) ЄКПЛ як одну із правомірних підстав для обмеження права на захист даних.

Приклад: у справі «*Y проти Туреччини*»[415] заявник був ВІЛ-інфікований. Оскільки в момент прибуття до лікарні він був без свідомості, команда швидкої допомоги повідомила працівників лікарні про його статус. У скарзі до ЄСПЛ заявник стверджував, що відкриття цієї інформації становило порушення його права на повагу до приватного життя. Однак, враховуючи потребу в безпеці працівників лікарні, поширення цієї інформації не було визнано порушенням його прав.

412 Рішення Суду ЄС, 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*), від 24 листопада 2011 р., пп. 40, 44 та 48–49.

413 Пояснювальна записка до Оновленої Конвенції 108, п. 46.

414 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) (*Recommendation CM/Rec(2010)13 and explanatory memorandum on the protection of individuals with regard to automatic processing of personal data in the context of profiling*), від 23 листопада 2010 р., стаття 3.4 (b) (Рекомендація щодо профайлінгу).

415 Рішення ЄСПЛ у справі «Y. проти Туреччини» (*Y v. Turkey*), № 648/10, від 17 лютого 2015 р.

4.1.2 Обробка особливих категорій даних (чутливі дані)

Право РЄ залишає за національним законодавством можливість встановлення належного захисту для використання чутливих даних за умови дотримання статті 6 Оновленої Конвенції 108, а саме, що належні гарантії, вказані в інших положеннях Конвенції, встановлені законом. У **праві ЄС** стаття 9 ЗРЗПД містить детальні правила регулювання обробки особливих категорій даних (також названих «чутливими даними»). Ці дані містять інформацію про расове або етнічне походження, політичні переконання, членство в профспілках, релігійні чи інші переконання, а також йдеться про обробку генетичних та біометричних даних для унікальної ідентифікації фізичної особи та дані про здоров'я, статеве життя або сексуальну орієнтацію. Обробка чутливих даних в принципі заборонена[416].

Проте у статті 9 (2) Регламенту можна знайти вичерпний перелік винятків із цієї заборони. Ці винятки становлять законні підстави для обробки чутливих даних:

- суб'єкт даних чітко і явно надав згоду на обробку даних;
- обробка здійснюється неприбутковою організацією з політичною, філософською, релігійною ціллю або для цілей професійної спілки в ході правомірної діяльності та за умови, що обробка стосується виняткового членів чи колишніх членів організації або осіб, що в таких цілях регулярно підтримують контакт з нею;
- обробка стосується даних, які суб'єкт даних відкрито оприлюднив;
- обробка є необхідною:
    - для здійснення обов'язків або реалізації спеціальних прав контролера або суб'єкта даних у трудовій сфері, у сфері соціальної безпеки та соціального захисту;
    - для захисту життєво важливих інтересів суб'єкта даних або іншої фізичної особи (коли суб'єкт даних не в змозі надати згоду);
    - для формування, здійснення або захисту правових претензій або коли суди діють як судові органи;

416 Колишня Директива про захист персональних даних, стаття 7 (f), тепер Загальний регламент захисту персональних даних, стаття 9 (1).

- для цілей превентивної медицини чи гігієни праці: «для оцінювання працездатності працівника, медичного діагнозу, надання послуг у сфері охорони здоров'я чи соціального забезпечення чи лікування або управління системами та послугами в сфері охорони здоров'я чи соціального забезпечення чи лікування на підставі законодавства Союзу або держави-члена чи відповідно до договору з медичним працівником»;
- для цілей архівування в суспільних інтересах, для цілей наукових та історичних досліджень або статистичних цілей;
- з причин суспільного інтересу у сфері громадського здоров'я;
- з причин значного суспільного інтересу.

У контексті обробки особливих категорій даних договірні відносини з суб'єктом даних не вважаються юридичною підставою для законної обробки чутливих даних, крім укладання договору з медичним спеціалістом, де діє обов'язок збереження професійної таємниці[417].

Явна згода суб'єкта даних

За **законодавством ЄС** першою умовою здійснення законної обробки будь-яких персональних даних, незалежно від того, чи є вони нечутливими, чи чутливими, має бути згода суб'єкта персональних даних. Коли йдеться про чутливі дані, така згода має бути явною. Попри це, у національному законодавстві держави-члена або законодавстві Союзу може бути передбачено, що згода на використання чутливих даних не є достатньою правовою підставою для надання дозволу на їхню обробку[418], коли, наприклад, у надзвичайних ситуаціях, обробка здійснюється з незвичайними для суб'єкта персональних даних ризиками.

Законодавство про працю або соціальну безпеку та соціальний захист

За **законодавством ЄС** заборона в пункті 1 статті 9 може бути знята, якщо обробка необхідна для здійснення зобов'язань або прав контролера чи суб'єкта персональних даних у сфері зайнятості або соціального захисту. Проте обробка має бути дозволена законодавством ЄС, національним законом або колективним договором відповідно до національного законодавства, який передбачає належні захисні гарантії для основоположних прав та інтересів

417 Загальний регламент захисту персональних даних, стаття 9 (2) (h) та (i).

418 Там само, стаття 9 (2) (a).

суб'єкта даних[419]. Документи щодо працевлаштування, які ведуться організацією, можуть включати чутливі персональні дані за певних умов, визначених у ЗРЗПД та відповідному національному законі. Приклади чутливих даних можуть включати інформацію про членство в профспілках або інформацію про здоров'я.

Життєво важливі інтереси суб'єкта даних або іншої особи

Відповідно до **законодавства ЄС** як і у випадку з нечутливими даними, життєво важливі інтереси суб'єкта даних або іншої особи можуть бути підставою для здійснення обробки чутливих даних[420]. Така підстава для обробки чутливих даних, як життєво важливі інтереси суб'єкта даних або іншої особи, може бути законною підставою, якщо така обробка «не може очевидно ґрунтуватися на іншій правовій підставі»[421]. У деяких справах обробка персональних даних може захистити як індивідуальний, так і суспільний інтерес, наприклад, коли обробка необхідна в гуманітарних цілях[422].

Для того, щоб обробка чутливих даних була легітимною на цій підставі, має бути відсутня можливість просити суб'єкта даних про згоду через те, що, наприклад, суб'єкт даних був без свідомості, або був відсутнім і з ним неможливо було зв'язатись. Інакше кажучи, особа була фізично або юридично нездатна надати згоду.

Благодійність або неприбуткові організації

Обробка персональних даних також дозволена в ході легітимної діяльності організацій, об'єднань або неприбуткових установ з політичною, світоглядною, релігійною ціллю або для цілей професійної спілки. Втім, обробка повинна стосуватися винятково членів, чи колишніх членів організації, чи осіб, що регулярно підтримують контакт з нею[423]. Чутливі дані не можуть бути відкриті поза межами цих організацій за відсутності згоди суб'єкта даних.

419 Загальний регламент захисту персональних даних, стаття 9 (2) (b).

420 Там само, стаття 9 (2) (c).

421 Там само, п. 46 преамбули.

422 Там само.

423 Там само,стаття 9 (2) (d).

Дані, відкрито оприлюднені суб'єктом даних

Стаття 9 (2)(e) ЗРЗПД передбачає, що обробка даних не забороняється, якщо вона стосується даних, які відкрито були оприлюднені суб'єктом даних. Хоча поняття «відкрито оприлюднені суб'єктом персональних даних» регламентом не визначено, однак, оскільки це є винятком із заборони обробки чутливих даних, воно має бути сформульовано чітко та в такий спосіб, що вимагає свідомого оприлюднення суб'єктом персональних даних своїх даних. Таким чином, коли телебачення транслює відео, зняте камерою спостереження, де, серед іншого, видно, що пожежник травмувався при евакуації з будинку, це не може вважатись очевидним свідомим оприлюдненням пожежником своїх даних. З іншого боку, якщо пожежник вирішує описати випадок та опублікувати відео і фото на публічній інтернет-сторінці, він або вона здійснить свідому стверджувальну дію для оприлюднення своїх персональних даних. Важливо зауважити, що оприлюднення особою своїх даних не є згодою, це інший дозвіл для обробки особливих категорій даних.

Той факт, що суб'єкт даних оприлюднив персональні дані, які обробляються, не виключає обов'язків контролера відповідно до законодавства про захист персональних даних. Наприклад, принцип обмеження цілі продовжує застосовуватися до персональних даних, якщо такі дані стали публічно доступними[424].

Юридичні вимоги

ЗРЗПД також дозволяє обробку особливих категорій даних, якщо вона «необхідна для формування, здійснення або захисту юридичних вимог»[425] незалежно від того, чи здійснюється це в судовому або адміністративному провадженні чи в позасудовій процедурі[426]. У такому випадку, обробка повинна бути відповідною до юридичної вимоги або її реалізації чи захисту, і може вимагатися будь-якою зі сторін спору.

Діючи як судові органи, суди можуть обробляти особливі категорії даних у контексті вирішення правових спорів[427]. Прикладами таких особливих категорій даних у цьому контексті можуть бути генетичні дані при встановленні батьківства або стан здоров'я, коли частина доказів стосується деталей отриманого жертвою злочину ушкодження.

424 Робоча група «Стаття 29» (2013), *Висновок 3/13 щодо обмеження мети*, РГ 203, Брюссель, від 2 квітня 2013 р., с. 14.

425 Там само, стаття 9 (2) (f).

426 Загальний регламент захисту персональних даних, п. 52 преамбули.

427 Там само.

Причини суттєвого суспільного інтересу

Відповідно до статті 9 (2)(g) ЗРЗПД держави-члени можуть встановити додаткові обставини, за яких чутливі дані можуть оброблятись, якщо:

- обробка даних здійснюється з причин суттєвого суспільного інтересу;
- це передбачено законодавством ЄС або національним законом;
- європейський або національний закон є пропорційним, поважає право на захист персональних даних та передбачає належні і спеціальні засоби для захисту прав та інтересів суб'єкта даних[428].

Яскравим прикладом є система електронних файлів у сфері охорони здоров'я. Така система дозволяє, щоб дані щодо здоров'я, зібрані надавачами послуг у цій сфері в ході лікування пацієнта, були доступні іншим надавачам послуг цьому пацієнту в сфері здоров'я, зазвичай у загальнонаціональному масштабі.

Робоча група «Стаття 29» дійшла висновку, що таку систему неможливо було б встановити за наявних юридичних правил обробки даних пацієнтів[429]. Однак система електронних файлів у сфері здоров'я може існувати, якщо вона діє на «підставі суттєвого суспільного інтересу»[430]. Це б вимагало чіткої законодавчої підстави для її запровадження, яка б також містила необхідні захисні гарантії для безпечного управління такою системою[431].

Інші підстави для обробки чутливих даних

ЗРЗПД передбачає, що чутливі дані можуть оброблятись, якщо обробка необхідна[432]:

- для цілей превентивної медицини чи гігієни праці, для оцінювання працездатності працівника, медичного діагнозу, надання послуг у сфері охорони здоров'я чи соціального забезпечення чи лікування, чи управління системами та послугами у сфері охорони здоров'я, чи соціального захисту

428 Там само, стаття 9 (2) (g).

429 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. Див. також Загальний регламент захисту персональних даних., стаття 9 (3).

430 Загальний регламент захисту персональних даних, стаття 9 (2) (g).

431 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.

432 Загальний регламент захисту персональних даних, стаття 9 (2) (h), (i) та (j).

на підставі законодавства Союзу або держави-члена чи відповідно до договору з медичним працівником;

- з причин суспільного інтересу у сфері охорони громадського здоров'я, зокрема захисту від серйозних транскордонних загроз здоров'ю чи забезпечення високих стандартів якості та безпеки у сфері охорони здоров'я і лікарських препаратів або медичного обладнання, на підставі законодавства Союзу або держави-члена. Закон має передбачати належні та спеціальні заходи для захисту прав і свобод суб'єкта даних;
- для досягнення цілей архівування, цілей наукового чи історичного дослідження або статистичних цілей на підставі законодавства Союзу або держави-члена, що має бути пропорційним цілі, яка переслідується, має поважати сутність права на захист даних і передбачати належні та спеціальні заходи для захисту основоположних прав та інтересів суб'єкта даних.

Додаткові умови за національним законом

ЗРЗПД також дозволяє державам-членам встановлювати або мати додаткові умови, включаючи обмеження для обробки генетичних, біометричних даних та даних про стан здоров'я[433].

433 Там само, стаття 9 (2) (h) та 9 (4).

4.2 Правила щодо безпеки обробки даних

Ключові моменти

- Правила щодо безпеки обробки даних зобов'язують контролера та оператора вжити належних технічних та організаційних заходів для попередження будь-якого несанкціонованого втручання в операції з обробки даних.
- Необхідний рівень захисту визначається залежно від:
  - засобів забезпечення безпеки, які наявні на ринку для будь-якого конкретного виду обробки;
  - вартості;
  - ризиків обробки даних для основоположних прав і свобод суб'єкта даних.
- Забезпечення конфіденційності персональних даних є частиною загального принципу Загального регламенту захисту персональних даних.

Як за **правом ЄС**, так і за **правом РЄ**, контролери мають загальний обов'язок працювати прозоро та підзвітно при обробці персональних даних, і особливо у разі витоку даних. У випадку порушення захисту персональних даних, контролери повинні повідомити орган контролю, крім випадків, якщо мало ймовірно, що це порушення може призвести до ризиків для прав та свобод фізичних осіб. Суб'єкти даних також мають бути повідомлені про витік персональних даних, якщо ймовірно, що порушення призведе до значного ризику для прав і свобод фізичних осіб.

4.2.1 Елементи безпеки даних

Згідно з відповідними положеннями законодавства ЄС:

> *Зважаючи на сучасний рівень розвитку, витрати на реалізацію, характер, обсяги, контекст і цілі обробки, а також ризики різної ймовірності та тяжкості для прав і свобод фізичних осіб, які викликає обробка, контролер і оператор повинні вжити необхідних технічних і організаційних заходів для забезпечення рівня безпеки відповідно до ризику [...]»*[434].

434 Там само, стаття 32 (1).

Ці заходи, серед іншого, включають:

- використання псевдонімів та шифрування персональних даних[435];
- забезпечення конфіденційності, цілісності, наявність і стійкість систем та послуг з обробки[436];
- вчасне відновлення персональних даних і доступ до них у випадку технічної аварії[437];
- процес для регулярного тестування, оцінювання та аналізу результативності технічних і організаційних заходів для гарантування безпеки обробки[438].

Схоже положення існує і в **праві ЄС**:

> *«Кожна Сторона забезпечує, щоб контролер та – де це застосовно – оператор вживав належних заходів безпеки щодо таких ризиків, як випадковий або несанкціонований доступ, знищення, втрата, використання, зміна або розкриття персональних даних»*[439].

Відповідно до **законодавства ЄС та РЄ** контролер зобов'язаний повідомити контролюючий орган про витік персональних даних, який може мати вплив на права і свободи осіб (див. *розділ 4.2.3*).

Часто також існують промислові, національні та міжнародні стандарти, розроблені для безпечної обробки даних. Наприклад, європейський знак конфіденційності (EuroPriSe) є проєктом 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 створене з метою посилення здатності ЄС, держав – членів ЄС та бізнес-спільноти запобігати, усувати та реагувати на проблеми мережевої та інформаційної безпеки[440]. Європейське агентство з мережевої та інформаційної безпеки регулярно

435 Там само, стаття 32 (1) (a).

436 Там само, стаття 32 (1) (b).

437 Там само, стаття 32 (1) (c).

438 Там само, стаття 32 (1) (d).

439 Оновлена Конвенція 108, стаття 7 (1).

440 Регламент (ЄС) № 526/2013 Європейського Парламенту та Ради від 21 травня 2013 р. щодо Європейського агентства з мережевої та інформаційної безпеки (ENISA) та про скасування Регламенту (ЄС) № 460/2004, OJ 2013 L 165.

оприлюднює аналіз поточного стану безпекових загроз та рекомендації щодо їх усунення[441].

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

- регулярне забезпечення всіх 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 або суб'єктам даних;
- використання персональних даних лише за вказівкою уповноваженої особи чи згідно з викладеними загальними правилами;
- захист доступу до місцезнаходження апаратного і програмного забезпечення контролера або оператора, включно з перевіркою авторизації доступу;
- забезпечення задокументованого належним чином дозволу на доступ до персональних даних, наданого уповноваженою на це особою;
- електронна база автоматизованої системи протоколів доступу до персональних даних і регулярна перевірка таких протоколів внутрішнім органом нагляду (відповідно, вимагається, щоб усі операції з обробки даних були фіксованими);
- 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 процедури перевірки для забезпечення виконання відповідних заходів на практиці, а не лише на папері (наприклад, внутрішній або зовнішній аудит).

441 Наприклад, ENISA, (2016), Кібербезпека та стійкість розумних авто. Кращі практики та рекомендації (*Cyber Security and Resilience of smart cars. Good practices and recommendations*). ENISA (2016), Безпека мобільних виплат і цифрових гаманців (*Security of Mobile Payments and Digital Wallets*).

Заходи щодо підвищення рівня безпеки контролера або оператора включають такі інструменти, як наявність посадовців з питань захисту персональних даних, навчання співробітників з питань безпеки, проведення регулярних аудитів, перевірки можливостей проникнення і якості захисту.

Приклад: у справі «*I. проти Фінляндії*»[442] заявниця не змогла довести факт незаконного доступу до її медичної картки з боку інших співробітників лікарні, де 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 з'ясувати, хто мав доступ до медичної картки пацієнтки, бо 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, а національні суди не надали цьому факту належної уваги.

ЄС прийняв Директиву про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу (Директива MIC, NIS)[443], яка є першим загальним для ЄС правовим інструментом щодо кібербезпеки. Директива має на меті покращити кібербезпеку на національному рівні з одного боку, та підвищити рівень взаємодії з ЄС – з іншого. Вона також покладає обов'язки на надавачів основних послуг (зокрема в секторах постачання енергії, здоров'я, банківських послуг, транспортних, послуг у сфері цифрової інфраструктури тощо) та надавачів цифрових послуг управляти ризиками, забезпечувати безпеку їхніх мережевих та інформаційних систем, а також повідомляти про випадки порушення безпеки.

Огляд

У вересні 2017 року Європейська Комісія запропонувала проєкт регламенту, спрямованого на реформування мандату Європейського агентства з мережевої та інформаційної безпеки (ENISA) для врахування нових повноважень агентства та відповідальності за Директивою MIC. Метою запропонованого

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

443 Директива (ЄС) 2016/1148 Європейського Парламенту та Ради про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу від 6 липня 2016 р., OJ 2016 L 194.

регламенту є розвиток функцій агентства та посилення його ролі як «головного центру екосистеми кібербезпеки ЄС»[444]. Запропонований регламент не має зашкоджувати принципам ЗРЗПД та шляхом роз'яснення необхідних складових елементів європейського механізму сертифікації кібербезпеки повинен посилювати безпеку персональних даних. Поряд з цим, у вересні 2017 року Європейська Комісія запропонувала проєкт виконавчого документа, у якому визначаються елементи, що мають враховуватись надавачами цифрових послуг для гарантування безпеки своїх мережевих та інформаційних систем, як цього вимагає стаття 16 (8) Директиви MIC. На час написання цього посібника дискусії щодо цих двох проєктів ще тривали.

4.2.2 Конфіденційність

У **праві ЄС** ЗРЗПД встановлює, що конфіденційність персональних даних є частиною загального принципу[445]. Надавачі публічно доступних послуг з електронної комунікації мають забезпечити конфіденційність. Вони також мають зобов'язання гарантувати безпеку своїх послуг[446].

Приклад: до співробітниці страхової компанії телефонують, представляються клієнтом компанії і вимагають інформацію про свій договір страхування. Обов'язок зберігати конфіденційними дані клієнтів вимагає від працівниці 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.

Відповідно до статті 5 (1)(f) обробка персональних даних повинна забезпечувати належну безпеку персональних даних, включаючи захист від несанкціонованої або незаконної обробки або від випадкової втрати, знищення або пошкодження. При цьому мають використовуватися належні технічні або організаційні заходи («цілісність і конфіденційність»).

444 *Проєкт* Регламенту Європейського Парламенту та Ради про ENISA, «ЄС Агенція з питань кібербезпеки» та скасування Регламенту (ЄС) 526/2013, та про сертифікацію інформаційної та комунікаційної технології кібербезпеки (Акт щодо кібербезпеки), COM(2017)477, від 13 вересня 2017 р., с. 6.

445 Загальний регламент захисту персональних даних, стаття 5 (1) (f).

446 Директива про конфіденційність та електронні комунікації, стаття 5 (1).

За статтею 32 контролер та оператор повинні вживати технічних та організаційних заходів для забезпечення високого рівня безпеки. Такі заходи включають, серед іншого, псевдонімізацію та шифрування персональних даних, здатність забезпечувати безперервну конфіденційність, цілісність, наявність та стійкість персональних даних, регулярне тестування, оцінювання та аналіз результативності технічних і організаційних заходів, здатність вчасно відновити наявність і доступ до персональних даних у разі технічної аварії. Крім того, дотримання затверджених кодексів поведінки або затвердженого механізму сертифікації можуть бути чинником демонстрації дотримання принципу цілісності та конфіденційності. На додаток, відповідно до статті 28 ЗРЗПД договір, який пов'язує оператора зобов'язальними відносинами з контролером, повинен містити положення про обов'язок оператора забезпечити те, щоб особи, які отримали дозвіл на обробку персональних даних, взяли на себе зобов'язання зберігати конфіденційність чи мали передбачені відповідним статутом обов'язок збереження конфіденційності.

Обов'язок конфіденційності не поширюється на ситуації, коли особа дізналася про дані як фізична особа, а не як працівник контролера чи оператора. У такому разі стаття 32 та 28 ЗРЗПД не застосовується, оскільки використання персональних даних приватною особою повністю виключається з регламенту, якщо таке використання підпадає під так званий виняток побутового характеру[447]. Виняток побутового характеру означає використання персональних даних «фізичною особою в ході суто особистої або побутової діяльності»[448]. Враховуючи рішення СЄС у справі «*Боділ Ліндквіст*»[449], цей виняток повинен тлумачитися вузько, особливо стосовно випадків відкриття даних. Зокрема, виняток побутового характеру не повинен поширюватися на виклад персональних даних в інтернеті для необмеженої кількості користувачів або на обробку даних, яка має професійний або комерційний аспекти (більш детально див. розділи *2.1.2*, *2.2.2* та *2.3.1*).

«Конфіденційність комунікації» є іншим аспектом конфіденційності, який підлягає спеціальному регулюванню (*lex specialis*). Ці спеціальні норми для забезпечення конфіденційності електронної комунікації відповідно до Директиви про конфіденційність та електронні комунікації (e-Privacy Directive) вимагають від держав-членів заборонити будь-яким особам, які не є

447 Загальний регламент захисту персональних даних, стаття 2 (2) (c).

448 Там само.

449 Суд ЄС, C-101/01, Кримінальне провадження проти Bodil Lindqvist (*Criminal proceedings against Bodil Lindqvist*), від 6 листопада 2003 р.

користувачами, або без згоди користувачів прослуховування, запис, зберігання або інші види перехоплення чи стеження за комунікаціями або пов'язаними мета даними[450]. Національний закон може встановлювати винятки з цього принципу лише з підстав національної безпеки, оборони, попередження або виявлення злочинів, а також якщо такі заходи є необхідними та пропорційними для цілей, що мають досягатися[451]. Ті самі правила також будуть застосовуватися за новою Директивою про конфіденційність та електронні комунікації, водночас сфера дії цієї Директиви буде розширена, щоб включати не лише публічно доступні послуги електронної комунікації, але й комунікацію, яка здійснюється через OTT-послуги (такі як мобільні застосунки).

За **правом РЄ** зобов'язання зберігати конфіденційність випливає з поняття «безпека даних» статті 7 (1) Оновленої Конвенції 108, у якій ідеться про безпеку персональних даних.

Для операторів конфіденційність означає, що вони не можуть відкривати дані третім особам або іншим одержувачам без надання дозволу. Для співробітників контролера або оператора збереження конфіденційності означає, що вони використовують персональні дані лише відповідно до інструкцій, наданих їхніми уповноваженими керівниками.

У будь-якому договорі між контролерами та їхніми операторами має бути передбачене зобов'язання щодо збереження конфіденційності. Окрім того, контролери або оператори повинні вживати конкретних заходів щодо встановлення для своїх співробітників правового обов'язку зберігати конфіденційність, що зазвичай досягається шляхом включення пунктів про конфіденційність до договору про працевлаштування.

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

4.2.3 Повідомлення про порушення захисту персональних даних

Порушення захисту персональних даних означає порушення безпеки, що призводить до випадкового чи незаконного знищення, втрати, зміни,

450 Директива про конфіденційність та електронні комунікації, стаття 5 (1).

451 Там само, стаття 15 (1).

несанкціонованого розкриття або доступу до персональних даних[452]. Хоча нові технології, як-от шифрування, тепер надають більших можливостей гарантувати безпеку обробки, порушення захисту персональних даних досі залишається поширеним явищем. Причини порушення захисту даних можуть бути різними: від ненавмисної помилки людей, які працюють в організації, до зовнішніх загроз, як-от хакери та кіберзлочинні організації.

Порушення захисту даних можуть бути дуже згубними для приватного життя та прав захисту даних особи, яка внаслідок порушення втрачає контроль над своїми персональними даними. Порушення захисту даних може призвести до крадіжки або шахрайства, фінансових втрат або матеріальної шкоди, втрати конфіденційності персональних даних, захищених професійною таємницею, а також може завдати шкоди репутації суб'єкта даних. У посібнику з питань повідомлення про порушення захисту персональних даних відповідно до Регламенту № 2016/679 Робоча група «Стаття 29» пояснює, що порушення може бути трьох видів за своїм впливом на персональні дані: відкриття, втрата та/або зміна даних[453]. Крім обов'язку вживати заходів для забезпечення безпеки обробки, як це пояснюється в розділі 4.2, так само важливо забезпечити належне та вчасне реагування контролера на порушення захисту в разі його виникнення.

Контролюючі органи або особи часто залишаються необізнаними про випадки порушення захисту, що перешкоджає особам вживати заходів для свого захисту від негативних наслідків. Для утвердження прав фізичних осіб і для обмеження впливу порушень захисту **ЄС та РЄ** покладає на контролерів вимогу повідомлення в певних випадках.

Відповідно до Оновленої Конвенції 108 Договірні Сторони повинні щонайменше зобов'язувати контролерів повідомляти компетентний контролюючий орган про випадки порушення захисту, які можуть становити серйозне втручання в права суб'єкта даних. Таке повідомлення має здійснюватися «без затримок»[454].

Законодавство ЄС встановлює детальне регулювання строків і змісту повідомлення[455]. Відповідно до цього регулювання контролери повинні повідомляти контролюючий орган про певні випадки порушення захисту без затримки

452 Загальний регламент захисту персональних даних, стаття 4 (12); див. також Робоча група «Стаття 29» (2017), Посібник щодо повідомлення про порушення захисту персональних даних відповідно до Регламенту 2016/679, РГ250, від 3 жовтня 2017 р., с. 8.

453 Робоча група «Стаття 29» (2017*), Посібник щодо повідомлення про порушення захисту персональних даних відповідно до Регламенту 2016/679*, РГ250, від 3 жовтня 2017 р., с. 6.

454 Оновлена Конвенція 108, стаття 7 (2); Пояснювальна записка до Оновленої Конвенції 108, пп. 64–66.

455 Загальний регламент захисту персональних даних, стаття 33 та 34.

та, по можливості, протягом 72 годин з моменту, коли їм стало відомо про порушення. Якщо вони повідомляють про це пізніше, ніж за 72 години, у повідомленні має бути пояснено причини затримки. Контролери можуть не повідомляти про випадки порушення захисту лише у разі, якщо вони здатні продемонструвати, що настання ризиків для прав і свобод зацікавлених осіб є малоймовірним.

Регламент вказує, яка мінімальна інформація має міститись у повідомленні для того, щоб контролюючий орган міг вжити необхідних заходів[456]. Повідомлення має включати щонайменше опис характеру порушення та категорії і приблизну кількість суб'єктів даних, на яких таке порушення може вплинути, опис можливих наслідків порушення та заходи, вжиті контролером для реагування на порушення та зменшення його наслідків. На додаток, має бути повідомлено ім'я та контактні дані спеціаліста із захисту персональних даних або інші контактні дані, щоб контролюючий орган міг отримати додаткову інформацію у разі необхідності.

Якщо є ймовірність високого рівня ризиків для прав і свобод осіб, контролер зобов'язаний повідомити цих осіб (суб'єктів даних) про порушення без зайвої затримки[457]. Інформація суб'єкту даних, включаючи опис характеру порушення, повинна бути викладена чіткою та простою мовою та містити інформацію, аналогічну тій, що надається контролюючому органу. За певних обставин можуть існувати винятки з обов'язку контролера повідомляти суб'єкта даних про порушення. Винятки застосовуються у разі, якщо контролер вжив належних технічних та організаційних заходів захисту, і ці заходи були застосовані до персональних даних, щодо яких мало місце порушення, зокрема, заходи, які роблять персональні дані незрозумілими для будь-якої особи, яка не має дозволу на доступ до них, наприклад, такі, як шифрування. Заходи, вжиті контролером після порушення для забезпечення ненастання шкоди для прав суб'єкта даних, також можуть зняти з контролера обов'язок щодо повідомлення суб'єкта даних. Зрештою, якщо повідомлення призводить до непропорційних зусиль контролера, суб'єкти даних можуть бути поінформовані про порушення іншими шляхами, як-от публічне повідомлення або схожі заходи[458].

Обов'язок повідомляти контролюючий орган та суб'єкта даних про порушення покладається на контролера. Порушення захисту даних може мати місце незалежно від того, хто здійснював обробку – контролер або оператор. З

456 Там само, стаття 33 (3).

457 Там само, стаття 34.

458 Там само, стаття 34 (3) (c).

цих міркувань дуже важливо забезпечити, щоб оператори також повідомляли про порушення. У такому разі оператори повинні повідомити контролера про порушення без неналежної затримки[459]. Далі контролер відповідальний за повідомлення контролюючого органу та суб'єктам даних, яких стосується порушення, у порядку, передбаченому вказаними правилами, та у відповідні строки.

4.3 Правила щодо підзвітності та сприяння відповідності

Ключові моменти

- Для забезпечення підзвітності обробки персональних даних контролери та оператори мають вести записи діяльності з обробки, за здійснення якої вони відповідальні, та надавати записи контролюючому органу у відповідь на запит.
- Загальний регламент захисту персональних даних встановлює декілька інструментів для забезпечення відповідності:
  - призначення за певних умов спеціаліста з питань захисту персональних даних;
  - здійснення оцінки впливу до початку операції з обробки, яка вірогідно спричинить високий рівень ризику для прав та свобод фізичних осіб;
  - попередні консультації з відповідним контролюючим органом, якщо оцінка вказує на ризики обробки, які не можуть бути зменшені;
  - кодекс поведінки контролерів та операторів, який визначає застосування регламенту в різних секторах обробки;
  - механізми сертифікації, відзнаки та оцінки.
- Право РЄ пропонує схожі інструменти для забезпечення відповідності Оновленій Конвенції 108.

Принцип підзвітності особливо важливий для гарантування виконання правил із захисту персональних даних у Європі. Контролер відповідальний за дотримання правил із захисту персональних даних та зобов'язаний бути здатним це продемонструвати. Підзвітність не має реалізовуватися виключно у разі порушення. Натомість контролери мають обов'язок активно вести належну політику управління даними на всіх стадіях обробки. Європейське

459 Там само, стаття 33 (2).

законодавство із захисту персональних даних вимагає від контролерів вжити технічних та організаційних заходів для забезпечення дотримання закону при здійсненні обробки. Вони також мають бути здатні це продемонструвати. Ці заходи, зокрема, включають призначення спеціаліста з питань захисту персональних даних, ведення записів та документації, пов'язаних з обробкою даних, а також здійснення оцінки впливу на приватне життя.

4.3.1 Спеціаліст із захисту персональних даних

Спеціалісти із захисту персональних даних (СЗПД) – це особи, які консультують з питань дотримання правил захисту персональних даних в організаціях, що здійснюють обробку даних. Вони є «наріжним каменем підзвітності», оскільки вони сприяють дотриманню правил та водночас діють як посередники між контролюючим органом, суб'єктами даних та організацією, яка їх призначила.

За **законодавством РЄ,** стаття 10 (1) Оновленої Конвенції 108 покладає загальну відповідальність за підзвітність на контролерів та операторів. Це вимагає від контролерів та операторів вживати належних заходів для виконання правил із захисту персональних даних, передбачених у Конвенції, та для здатності продемонструвати, що здійснювана під їхнім контролем обробка даних відповідає положенням Конвенції. Хоча Конвенція не передбачає конкретних заходів, яких мають вживати контролери та оператори, пояснювальна записка до Конвенції 108 вказує, що призначення СЗПД може бути одним із можливих заходів, який допоможе продемонструвати відповідність Конвенції. СЗПД має бути забезпечений усіма необхідними засобами для виконання його завдань[460].

На противагу законодавству РЄ, **у ЄС** призначення СЗПД не завжди віддається на розсуд контролерів та операторів, таке призначення є обов'язковим за певних умов. ЗРЗПД визнає, що СЗПД відіграє ключову роль у новій системі управління, та включає детальні положення щодо призначення такого спеціаліста, його посади, обов'язків та завдань[461].

ЗРЗПД вимагає обов'язкового призначення СЗПД у трьох конкретних випадках: коли обробку здійснює орган або установа державної влади; якщо основні види діяльності контролера або оператора становлять операції з обробки, які, в силу їхньої специфіки, обсягів та/чи цілей, вимагають регулярного,

460 Пояснювальна записка до Оновленої Конвенції 108, п. 87.

461 Загальний регламент захисту персональних даних, стаття 37–39.

систематичного і широкомасштабного моніторингу суб'єктів даних; або основні види діяльності контролера чи оператора становлять широкомасштабну обробку особливих категорій даних і персональних даних про судимості та злочини[462]. Хоча такі поняття, як «систематичний і широкомасштабний моніторинг» та «основні види діяльності» не визначені в регламенті, Робоча група «Стаття 29» сформувала рекомендації щодо їх тлумачення[463].

Приклад: компанії соціальних медіа та інформаційно-пошукових систем вірогідно мають вважатися контролерами, чиї операції з обробки вимагають проведення регулярного, систематичного та широкомасштабного моніторингу суб'єктів даних. Бізнесова модель таких компаній засновується на обробці великих обсягів персональних даних, і вони генерують значний дохід через послуги адресної реклами та дозвіл компаніям рекламувати себе на сайтах. Адресна реклама є способом розміщення реклами на основі демографічних характеристик і попередньої історії купівельних звичок споживачів. Таким чином, вона вимагає систематичного моніторингу звичок і поведінки суб'єктів персональних даних в інтернеті.

Приклад: лікарня та медична страхова компанія є типовими прикладами контролерів, чия діяльність полягає в широкомасштабній обробці особливих категорій персональних даних. Дані, які містять інформацію щодо здоров'я особи, є особливими категоріями персональних даних як відповідно до права РЄ, так і права ЄС, тож вони вимагають посиленого захисту. Законодавство ЄС також відносить генетичні та біометричні дані до особливих категорій. Оскільки медичні установи та страхові компанії обробляють такі дані широкомасштабно, від них вимагається призначення спеціаліста із захисту персональних даних відповідно до ЗРЗПД.

Крім того, стаття 37 (4) ЗРЗПД передбачає, що в інших ситуаціях, ніж ті, що вказані в статті 37 (1), контролер чи оператор, чи асоціації та інші органи, що представляють категорії контролерів або операторів, можуть або, відповідно до вимог законодавства Союзу чи держави-члена, зобов'язані призначити спеціаліста з питань захисту даних.

462 Там само, стаття 37 (1).

463 Робоча група «Стаття 29» (2017), *Посібник щодо спеціаліста з питань захисту персональних даних ('DPOs')*, РГ 243 rev.01, востаннє переглянутий та прийнятий 5 квітня 2017 р.

Усі інші організації не зобов'язані призначати СЗПД. Однак ЗРЗПД передбачає, що контролери та оператори можуть добровільно призначити СЗПД, та водночас надає державам-членам можливість зробити таке призначення обов'язковим для більшої кількості видів організацій, ніж ті, що передбачені регламентом[464].

Після призначення СЗПД контролери мають забезпечити, щоб він або вона «були залученими, належним чином і вчасно, до всіх питань, що стосуються захисту персональних даних» в організації[465]. Наприклад, СЗПД має бути залучений до надання порад щодо здійснення оцінки впливу або до створення та ведення записів діяльності з обробки даних в організації. Для забезпечення можливості СЗПД ефективно здійснювати свої завдання контролери та оператори повинні забезпечити їх належними ресурсами, зокрема фінансовими, інфраструктурою та устаткуванням. Додаткові вимоги включають надання СЗПД достатнього часу для виконання своїх завдань і забезпечення постійного навчання для того, щоб вони розвивали та вдосконалювали свої знання відносно розвитку сфери права захисту персональних даних[466].

ЗРЗПД встановлює певні основні гарантії для забезпечення незалежного способу діяльності СЗПД. Контролери та оператори повинні забезпечити, щоб при виконанні своїх завдань, пов'язаних із захистом персональних даних, СЗПД не отримував будь-яких інструкцій від компанії, включаючи посадовців найвищого рівня управління. Крім того, вони не можуть бути звільненні або піддані покаранню в будь-який спосіб за виконання своїх завдань[467]. Візьмемо, наприклад, ситуацію, у якій СЗПД радить контролеру або оператору провести оцінку впливу на захист даних, оскільки він або вона вважає, що обробка, вірогідно, містить високий ризик для суб'єкта даних. Компанія не погоджується з порадою СЗПД, вважаючи, що вона необґрунтована, і в результаті вирішує відмовитись від проведення такої оцінки. Компанія може знехтувати порадою, однак не може звільнити або покарати СЗПД за її надання.

Нарешті, завдання та обов'язки СЗПД детально викладені в статті 39 ЗРЗПД. Вони включають вимоги інформувати та надавати рекомендації компаніям та працівникам, які здійснюють обробку, щодо їхніх обов'язків відповідно до законодавства та здійснювати моніторинг відповідності правилам захисту

464 Загальний регламент захисту персональних даних, стаття 37 (3) та (4).

465 Там само, стаття 38 (1).

466 Робоча група «Стаття 29» (2017), *Посібник щодо спеціаліста з питань захисту персональних даних ('DPOs')*, РГ 243 rev.01, востаннє переглянутий та прийнятий 5 квітня 2017 р., п. 3.1.

467 Загальний регламент захисту персональних даних, стаття 38 (2) та (3).

персональних даних ЄС та національним правилам шляхом проведення аудитів та тренінгів для працівників, які залучені до обробки. СЗПД також мають взаємодіяти з контролюючим органом та діяти як контактний центр для останнього щодо питань, пов'язаних з обробкою даних, таких як порушення безпеки даних.

Щодо персональних даних, які знаходяться в інституціях та органах ЄС, Регламент 45/2001 передбачає, що кожна інституція та орган ЄС повинен призначити СЗПД. СЗПД уповноважений стежити, щоб положення регламенту правильно застосовувались у межах інституцій та органів ЄС, а також щоб суб'єкти даних і контролери були поінформовані щодо їхніх прав та обов'язків[468]. Він або вона також відповідає за відповіді на запити ЄІЗПД та взаємодію з ним чи нею в разі потреби. Аналогічно до ЗРЗПД Регламент 45/2001 містить положення про незалежність СЗПД у виконанні їхніх завдань та потребу забезпечити їх необхідним персоналом і ресурсами[469]. СЗПД має бути повідомлений до того, як інституція або орган ЄС (або департаменти цих організацій) будуть здійснювати операції з обробки даних, а також мають вести реєстр усіх доведених до їхнього відома операцій з обробки[470].

4.3.2 Документування обробки даних

Для того, щоб бути здатними продемонструвати відповідність правилам та підзвітність, від компаній часто вимагається документувати та вести записи своїх дій. Важливим прикладом у цьому контексті є податкове право та аудит, які вимагають від усіх компаній вести великий обсяг документації та звітності. Встановлення схожих вимог в інших сферах права, а саме у сфері захисту персональних даних, також є важливим, оскільки ведення записів є важливим способом сприяння дотриманню правил захисту персональних даних. **Законодавство ЄС** передбачає, що контролери або їхні представники зобов'язані вести записи дій з обробки даних, яка здійснюється в межах їхньої відповідальності[471]. Цей обов'язок має забезпечити, щоб у разі потреби контролюючий орган мав усю необхідну документацію для підтвердження законності обробки.

Інформація, яка підлягає документуванню, включає наступне:

468 Див. статтю 24 (1) Регламенту(ЄС) № 45/2001 щодо повного списку завдань СЗПД.

469 Регламент (ЄС) № 45/2001, стаття 24 (6) та (7).

470 Там само, стаття 25 та 26.

471 Загальний регламент захисту персональних даних, стаття 30.

- ім'я та контактні дані контролера, співконтролера, представника контролера та СЗПД у разі його призначення;
- цілі обробки;
- опис категорій суб'єктів даних і категорій персональних даних, які стосуються обробки;
- інформацію про категорії отримувачів, яким було чи буде відкрито персональні дані;
- інформацію про те, чи були або чи будуть персональні дані передані третім державам або міжнародним організаціям;
- якщо можливо, передбачені строки для видалення різних категорій персональних даних, а також огляд технічних заходів, вжитих для забезпечення безпеки обробки[472].

Обов'язок вести записи дій з обробки відповідно до ЗРЗПД стосується не лише контролерів, але також і операторів. Це важливий крок вперед, оскільки до прийняття Регламенту обов'язки оператора визначалися переважно в договорі між контролером та оператором. Їхній обов'язок вести записи тепер передбачено безпосередньо законом.

ЗРЗПД передбачає винятки з цього обов'язку. Вимога вести записи не застосовується до підприємств або організацій (контролера або оператора), де кількість працівників є меншою за 250 осіб. Однак виняток застосовний за умови, що організація не здійснює обробку, яка може призвести до ризику для прав і свобод суб'єкта даних, що обробка не є систематичною та що вона не включає особливих категорій даних, передбачених статтею 9 (1) або персональних даних щодо засудження за злочини або правопорушення, передбачені статтею 10.

Ведення записів дій з обробки даних має надати можливість контролерам та операторам продемонструвати дотримання правил. Це також має забезпечити можливість контролюючому органу здійснювати моніторинг законності обробки. Якщо контролюючий орган вимагає надати доступ до цих записів, контролер та оператор зобов'язані взаємодіяти та надати доступ до записів.

472 Там само, стаття 30 (1).

4.3.3 Оцінка впливу та попередня консультація

Операції з обробки даних містять певні внутрішні ризики для прав осіб. Персональні дані можуть бути втрачені, відкриті неуповноваженим сторонам або оброблятись у незаконний спосіб. Звісно, ризики можуть різнитися залежно від характеру та обсягу обробки. Широкомасштабна обробка, яка включає обробку особливих категорій даних, несе набагато більші ризики для суб'єкта даних у порівнянні з потенційними ризиками обробки маленькою компанією даних про адресу та особисті номери телефонів своїх працівників.

З'явилися нові технології, обробка даних стає все більш складною, і контролери зобов'язані реагувати на такі ризики, оцінюючи можливий вплив на заплановану обробку до її початку. Це дає можливість організаціям належним чином ідентифікувати, реагувати та мінімізувати ризики завчасно, значним чином обмеживши можливий негативний вплив на осіб в результаті обробки.

Оцінка впливу обробки даних передбачена **як в праві ЄС, так і в праві РЄ**. У правових документах РЄ стаття 10 (2) Оновленої Конвенції 108 вимагає від Договірних Сторін забезпечити, щоб контролери та оператори «оцінювали можливий вплив запланованої обробки даних на права та основоположні права суб'єкта даних до початку такої обробки», а після здійснення такої оцінки організовувати обробку у такий спосіб, щоб попередити або мінімізувати можливі ризики обробки.

Право ЄС покладає на контролерів, діяльність яких регулюється ЗРЗПД, схожий, хоча й більш деталізований, обов'язок. Стаття 35 передбачає, що оцінка впливу має здійснюватися, якщо обробка, ймовірно, призведе до значного ризику для прав та свобод осіб. Регламент не визначає, яким чином має бути оцінено ймовірність ризику, але вказує, якими можуть бути такі ризики[473]. Він містить перелік операцій з обробки, що пов'язані зі значним ризиком, для якої особливо необхідна попередня оцінка, а саме, якщо:

- персональні дані обробляються для прийняття рішення щодо фізичних осіб внаслідок будь-якої системної та широкої оцінки пов'язаних з цими особами особистих аспектів (профайлінг);
- здійснюється широкомасштабна обробка чутливих даних або даних, пов'язаних із кримінальними засудженнями та правопорушеннями;

473 Загальний регламент захисту персональних даних, п. 75 преамбули.

- обробка включає широкомасштабний, систематичний моніторинг публічно доступних сфер.

Контролюючі органи повинні прийняти та опублікувати перелік видів операцій з обробки, вплив яких має оцінюватися. Вони також можуть сформувати перелік операцій з обробки, де цей обов'язок не передбачений[474].

Коли вимагається оцінка впливу, контролери повинні оцінити необхідність і пропорційність обробки та можливі ризики для прав осіб. Оцінка впливу також має містити заплановані заходи безпеки для усунення виявлених ризиків. У процесі формування переліку контролюючи органи держав-сторін повинні взаємодіяти між собою та з Європейською радою із захисту персональних даних. Це забезпечить узгоджений підхід усього ЄС щодо операцій, які вимагають оцінки впливу, і контролери матимуть справу з подібними вимогами незалежно від свого місця знаходження.

Якщо в результаті оцінки впливу виявиться, що обробка призведе до значного ризику для прав осіб, і жодних заходів для зниження ризику вжито не було, контролер повинен проконсультуватися з відповідним контролюючим органом до початку операції з обробки[475].

Робоча група «Стаття 29» видала Посібник для оцінки впливу захисту персональних даних та способу встановлення ймовірності значного ризику[476]. Вона сформувала дев'ять критеріїв для визначення, чи вимагається здійснення оцінки впливу захисту даних у конкретній справі[477]: (1) аналіз або присвоєння балів; (2) автоматичне прийняття рішення з юридичним або схожими значними наслідками; (3) систематичний моніторинг; (4) чутливі дані; (5) широкомасштабна обробка даних; (6) набори даних, які були зіставлені або об'єднані; (7) дані щодо вразливих суб'єктів даних; (8) інноваційне використання або застосування технологічних чи організаційних рішень; (9) якщо обробка «перешкоджає суб'єктам даних реалізовувати певне право або користуватися послугою чи договором». Робоча група «Стаття 29» запровадила практичне правило, за яким операції з обробки, які відповідають менш ніж двом критеріям,

474 Там само, стаття (4) та (5).

475 Там само, стаття 36 (1); Робоча група «Стаття 29» (2017), *Посібник для оцінки впливу на захист персональних даних (DPIA) та визначення, чи є обробка такою, що уможливлює високий рівень ризику для цілей Регламенту 2016/679*, РГ 248 rev.01, Брюссель, від 4 жовтня 2017 р.

476 Робоча група «Стаття 29» (2017), *Посібник для оцінки впливу на захист персональних даних (DPIA) та визначення, чи є обробка такою, що уможливлює високий рівень ризику для цілей Регламенту 2016/679*, РГ 248 rev.01, Брюссель, від 4 жовтня 2017 р.

477 Там само, сс. 9–11.

містять ризики низького рівня та не вимагають оцінки захисту персональних даних. Водночас ті операції, які відповідають двом або більше критеріям, будуть вимагати такої оцінки. У випадках, коли не ясно, чи вимагається оцінка впливу захисту даних, Робоча група «Стаття 29» рекомендує здійснити таку оцінку, оскільки це «корисний засіб, який допомагає контролерам дотримуватись законодавства із захисту персональних даних»[478]. Також важливо, щоб оцінка впливу захисту даних була здійснена, якщо запроваджено нові технології обробки персональних даних[479].

4.3.4 Кодекс поведінки

Кодекси поведінки мають застосовуватись у декількох галузях виробництва для окреслення та уточнення порядку застосування ЗРЗПД у їхніх конкретних секторах. Для контролерів та операторів персональних даних створення таких кодексів може значно полегшити дотримання виконання правил із захисту персональних даних ЄС. Досвід представників таких секторів сприятиме віднайденню рішень, які є практичними і отже будуть, імовірно, виконуватися. Визнаючи важливість таких кодексів для ефективного застосування законодавства із захисту персональних даних, ЗРЗПД закликає держави-сторони, контрольні органи, Комісію та Європейську раду з захисту персональних даних заохочувати створення таких кодексів поведінки з метою сприяння належному застосуванню регламенту в усій Європі[480]. Кодекси можуть визначати застосування регламенту в конкретних секторах, включаючи такі питання, як збір персональних даних, інформація, яка має бути надана суб'єкту даних і громадськості, та питання реалізації прав суб'єкта даних.

Для того, щоб кодекси поведінки відповідали правилам ЗРЗПД, кодекси мають бути надані компетентним контролюючим органам перед затвердженням. Контролюючий орган надає висновок щодо відповідності проєкту кодексу положенням регламенту, та якщо він вважає, що кодекс передбачає належні гарантії захисту, погоджує його[481]. Контролюючий орган повинен опублікувати погоджений кодекс поведінки, так само, як і критерії, на яких ґрунтувалося це погодження. Якщо кодекс поведінки стосується обробки в декількох державах-сторонах, компетентний контролюючий орган до погодження проєкту кодексу, внесення до нього змін або розширення має подати цей кодекс

478 Там само, с. 9.

479 Там само.

480 Загальний регламент захисту персональних даних, стаття 40 (1).

481 Там само, стаття 40 (5).

до Європейської ради із захисту персональних даних, яка надає свій висновок щодо його відповідності ЗРЗПД. У процесі виконання нормативних актів Комісія може вирішити, що погоджений кодекс поведінки матиме загальну чинність у межах Союзу.

Дотримання кодексу поведінки надає важливі переваги як суб'єктам даних, так і контролерам та операторам. Такі кодекси передбачають детальні інструкції, які визначають застосовність правових вимог до конкретних галузей і сприяють прозорості дій з обробки. Контролери та оператори також можуть використовувати дотримання кодексів як доказ, що свідчить про дотримання законодавства ЄС, а також для покращення свого іміджу як організацій, для яких захист персональних даних в операціях є пріоритетом та обов'язком. Ухвалені кодекси поведінки разом з обов'язковими та захищеними санкцією зобов'язаннями можуть використовуватись як належні гарантії для передачі даних третім державам.

Для переконання в тому, що організації дійсно дотримуються кодексів поведінки, може призначатись спеціальна організація (акредитована відповідним контролюючим органом) для моніторингу та забезпечення дотримання. Для ефективного виконання своїх завдань ця організація має бути незалежною, володіти підтвердженими експертними знаннями з питань, які регулюються кодексом поведінки, та мати прозорі процедури і структуру, яка забезпечує можливість розглядати скарги щодо порушення кодексу[482].

У **праві РЄ** Оновлена Конвенція 108 передбачає, що рівень захисту персональних даних, гарантований національним законом, може бути посилений добровільними засобами, такими як кодексом належної практики або кодексом професійної поведінки. Втім, вони є лише добровільними засобами за Оновленою Конвенцією 108: з них неможливо вивести юридичне зобов'язання застосовувати такі засоби, хоча це і рекомендується, до того ж такі засоби самі собою не є достатніми для забезпечення повного дотримання положень Конвенції[483].

4.3.5 Сертифікація

Іншими засобами на додаток до кодексів поведінки, за допомогою яких контролери та оператори можуть продемонструвати дотримання ЗРЗПД, є механізм сертифікації, відзнаки та оцінки. З цією метою регламент передбачає добровільну сертифікаційну систему, де певні установи або контролюючі

482 Там само, стаття 41 (1) та (2).

483 Пояснювальна записка до Оновленої Конвенції 108, п. 33.

органи можуть видавати сертифікати. Контролери та оператори, які скористалися таким сертифікаційним механізмом, можуть набути більшої наочності та довіри, оскільки сертифікація, відзнаки та оцінки дозволяють суб'єктам даних швидко оцінити рівень захисту персональних даних, який надає організація. Важливо, що наявність у контролера або оператора відповідного сертифікату не звужує його обов'язки та відповідальність за дотримання всіх вимог регламенту.

4.4 Захист даних за призначенням та за замовчуванням

Захист даних за призначенням

Законодавство ЄС вимагає, щоб контролери вжили заходів для ефективного виконання принципів захисту персональних даних та для запровадження необхідних захисних гарантій для дотримання вимог регламенту та захисту прав суб'єктів даних[484]. Ці заходи мають бути вжиті як під час обробки даних, так і при визначенні засобів обробки. При виконанні цих заходів контролер повинен взяти до уваги сучасний стан справ, витрати на виконання, характер, обсяг та цілі обробки персональних даних, а також ризики та небезпеку для прав і свобод суб'єкта даних[485].

Правові документи РЄ вимагають, щоб контролери та оператори оцінювали ймовірний вплив обробки персональних даних на права та свободи суб'єктів даних до початку обробки. Крім того, контролери та оператори зобов'язані організовувати обробку даних таким чином, щоб попередити або мінімізувати ризик втручання в ці права і свободи, а також вжити технічних та організаційних заходів, які мають враховувати наслідки, пов'язані із правом на захист персональних даних на всіх стадіях обробки даних[486].

484 Загальний регламент захисту персональних даних, стаття 25 (1).

485 Див. Робоча група «Стаття 29» (2017), *Посібник про оцінку впливу на захист персональних даних (DPIA) та визначення, чи є обробка такою, що уможливлює високий рівень ризику для цілей Регламенту 2016/679*, РГ 248 rev.01, Брюссель, від 4 жовтня 2017 р. Див, також ЄАМІБ (ENISA) (2015), *Приватність та захист даних за призначенням – від політики до конструювання,* від 12 січня 2015 р.

486 Оновлена Конвенція 108, стаття 10 (2) та (3), Пояснювальна записка до Оновленої Конвенції 108, п. 89.

Захист даних за замовчуванням

Право ЄС вимагає, щоб контролер вжив належних заходів для забезпечення принципової обробки лише тих персональних даних, які є необхідними для цілей обробки. Такий обов'язок застосовують до кількості зібраних персональних даних, ступеня їх обробки, періоду їх зберігання та доступності[487]. Наприклад, такі заходи повинні забезпечити доступ не всіх працівників контролера до персональних даних суб'єкта даних. Детальний огляд представлено ЄІЗПД у *навчальному посібнику з питань необхідності*[488].

Право РЄ вимагає, щоб контролери та оператори вживали технічних та організаційних заходів для врахування наслідків, пов'язаних з правом на захист персональних даних, а також технічних та організаційних заходів, які враховують наслідки, пов'язані з правом на захист персональних даних на всіх стадіях обробки даних[489].

У 2016 році ENISA опублікував огляд наявних інструментів та послуг з питань приватності[490]. Крім інших аспектів, цей аналіз надає індекс критеріїв і параметрів, які є показниками хороших або поганих підходів до захисту приватного життя. Деякі критерії взято безпосередньо з положень ЗРЗПД – такі як використання псевдонімів і погоджені сертифікаційні механізми, інші передбачають інноваційні ініціативи для забезпечення приватності за призначенням та за замовчуванням. Наприклад, критерій зручності використання, хоча й не прямо стосується приватності, може її посилити, оскільки він може розширити застосування інструментів і послуг у сфері приватності. Дійсно, інструменти забезпечення приватного життя, які складно виконати на практиці, можуть мати дуже низькі рівні застосування широкими колами суспільства, навіть якщо вони пропонують дуже потужні гарантії приватності. Крім того, критерій зрілості та стабільності інструмента приватності – у значенні способу, в який цей інструмент формується протягом часу та відповідає на наявні або нові виклики стосовно приватності – має принципову важливість. Інші технології з посилення приватності, наприклад, у контексті безпеки комунікацій, включають суцільне шифрування (спілкування, у якому лише особи, які спілкуються між собою, можуть читати повідомлення); шифрування

487 Загальний регламент захисту персональних даних, стаття 25 (2).

488 Європейський інспектор із захисту персональних даних (EDPS, ЄІЗПД), (2017), *Посібник з необхідності*, Брюссель, від 11 квітня 2017 р.

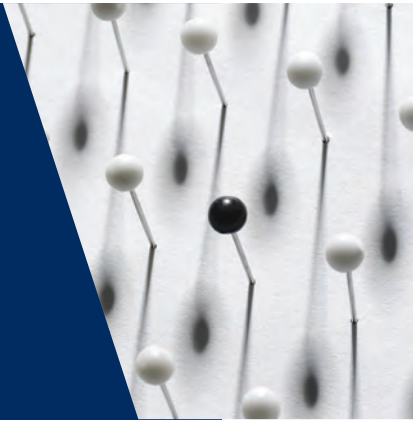
489 Оновлена Конвенція 108, стаття 10 (3), Пояснювальна записка до Оновленої Конвенції 108, п. 89.

490 ENISA (ЄАМІБ), *Контрольні матриці PETs: системний підхід для оцінки засобів онлайн та мобільної приватності*, від 20 грудня 2016 р.

клієнт-сервер (шифрування комунікаційних каналів між клієнтом і сервером); автентифікацію (перевірку ідентичності сторін комунікації); та анонімну комунікацію (відсутність можливості ідентифікувати учасників спілкування третіми сторонами).

5

Незалежний нагляд



ЄС	Питання, що висвітлюються	РЄ
Хартія, стаття 8 (3) *Договір про функціонування Європейського Союзу*, стаття 16 (2) *Загальний регламент захисту персональних даних*, статті 51–59 СЄС, C-518/07, «Європейська Комісія проти Федеративної Республіки Німеччини» (*European Commission v. Federal Republic of Germany*) [ВП], 2010 СЄС, C-614/10, «Європейська Комісія проти Республіки Австрії» (*European Commission v. Republic of Austria*) [ВП], 2012 СЄС, C-288/12, «Європейська Комісія проти Угорщини» (*European Commission v. Hungary*) [ВП], 2014 СЄС, C-362/14,	**Контролюючий орган** **Взаємодія контролюючих органів** **Європейська рада із захисту персональних даних**	Оновлена Конвенція 108, стаття 15 Оновлена Конвенція 108, статті 16–21

ЄС	Питання, що висвітлюються	РЄ
«Максиміліан Шремс проти Уповноваженого із захисту персональних даних» (*Maximillian Schrems v. Data Protection Commissioner*) [ВП], 2015 Загальний регламент захисту персональних даних, статті 60–67 Загальний регламент захисту персональних даних, статті 68–76		

Ключові моменти

- Незалежний нагляд є суттєвим елементом європейського права із захисту персональних даних, він передбачений у статті 8 (3) Хартії
- Для забезпечення ефективного захисту персональних даних у національному законодавстві мають бути запроваджені незалежні контролюючі органи.
- Контролюючі органи мають діяти з абсолютною незалежністю, що має гарантуватися законом та відображатись у спеціальній організаційній структурі контролюючого органу.
- Контролюючі органи мають конкретні повноваження та завдання. Вони, серед іншого, повинні:
  - моніторити та сприяти захисту персональних даних на національному рівні;
  - консультувати суб'єкта даних і контролерів, а також державні органи та громадськість;
  - розглядати скарги та допомагати суб'єктам даних у питаннях щодо стверджуваних порушень прав на захист даних;
  - наглядати за контролерами та операторами.
- Контролюючі органи також мають повноваження здійснювати втручання, якщо необхідно, шляхом:
  - попередження, винесення догани або навіть накладення штрафів на контролерів та операторів;
  - внесення припису про зміну, блокування або вилучення даних;
  - накладення заборони на обробку або адміністративний штраф;

- передання питань до суду.

- Контролюючі органи повинні взаємодіяти один з одним щодо транскордонних питань для забезпечення ефективності захисту осіб у Європі, оскільки обробка персональних даних часто стосується контролерів, операторів і суб'єктів даних, які розташовані в різних державах.
- У ЄС Загальний регламент захисту персональних даних встановлює для справ із транскордонною обробкою механізм єдиного вікна. Деякі компанії здійснюють транскордонну обробку у зв'язку з обробкою даних у контексті діяльності установ, розташованих у більш ніж одній державі-учасниці, або в контексті діяльності однієї установи в межах Союзу, однак з наслідками для суб'єктів даних у більш ніж одній державі-учасниці. Згідно з цим механізмом такі компанії будуть мати справу лише з одним національним контролюючим органом з питань захисту персональних даних.
- Взаємодія та механізм узгодження дозволять забезпечити скоординований підхід між усіма контролюючими органами, залученими до справи. Головний контролюючий орган – головної або єдиної установи – буде консультуватися з іншими зацікавленими контролюючими органами і надасть їм проєкт рішення.
- Так само як теперішня Робоча група «Стаття 29», контролюючий орган кожної держави-члена та ЄІЗПД будуть частиною Європейської ради із захисту персональних даних.
- Завдання Європейської ради із захисту персональних даних включають, наприклад, моніторинг правильного застосування регламенту, надання порад Комісії щодо відповідних питань, надання висновків, рекомендацій, окреслення найкращих підходів щодо різноманітних питань.
- Головна різниця полягає в тому, що Європейська рада із захисту персональних даних буде не лише надавати висновки, як це відбувалося відповідно до Директиви 95/46ЄС. Вона також буде виносити обов'язкові рішення у випадках, коли контролюючий орган висловив доцільне та обґрунтоване заперечення у справах щодо єдиного вікна; якщо існують конфліктні погляди на те, який контролюючий орган є головним; а також у випадках, коли компетентний контролюючий орган не звертається за висновком ЄРЗПД або не виконує його. Метою є забезпечити узгоджене застосування регламенту серед держав-членів.

Незалежний нагляд є суттєвим елементом європейського законодавства із захисту персональних даних. Як право ЄС, так і право РЄ розглядають існування незалежного контролюючого органу як невід'ємний елемент ефективного захисту прав і свобод осіб щодо обробки їхніх персональних даних. Оскільки обробка даних зараз є повсякчасною і все складнішою для розуміння, ці контролюючі органи є вартовими цифрової ери. У ЄС існування незалежних контролюючих органів вважається одним із найбільш суттєвих елементів права на захист персональних даних, який передбачено в первинному законодавстві ЄС. Стаття 8 (3) Хартії основних прав ЄС та стаття 16 (2) ДФЄС визнають

захист персональних даних як основоположне право та підкреслюють, що дотримання правил захисту персональних даних має відбуватися під контролем незалежного органу.

Важливість незалежного нагляду за дотриманням законодавства про захист персональних даних також визнавалась у судовій практиці.

Приклад: у справі «*Шремс*»[491] Суд ЄС розглядав питання, чи відповідала законодавству із захисту персональних даних ЄС передача персональних даних на територію Сполучених Штатів Америки на підставі першого Договору ЄС – США «Про безпечну гавань» у світлі викриття Едварда Сноудена щодо здійснення масового спостереження Національною службою безпеки США. Передача персональних даних до США ґрунтувалася на рішенні від 2000 року, яке дозволяло передачу персональних даних з ЄС до організацій США, які були самосертифіковані відповідно до схеми «Безпечної гавані» – системи, яка забезпечує адекватний рівень захисту персональних даних. У відповідь на запит щодо розслідування скарги заявника на правомірність передачі даних після викриття пана Сноудена контролюючий орган Ірландії відхилив скаргу на підставі того, що рішення Комісії щодо відповідності режиму захисту персональних даних США, яке відображається в принципах «Безпечної гавані» (Рішення «Про безпечну гавань»), не дозволяє йому розслідувати скаргу.

Однак Суд ЄС вирішив, що існування рішення Комісії про дозвіл на передачу даних третім країнам, які забезпечують адекватний рівень захисту даних, не усуває або не зменшує повноваження національного контролюючого органу. СЄС зазначив, що повноваження цих органів моніторити та забезпечувати відповідність правилам захисту персональних даних ЄС випливає із первинного права ЄС, а саме статті 8 (3) Хартії та статті 16 (2) ДФЄС. «Таким чином, заснування незалежних контролюючих органів є важливим елементом захисту осіб стосовно обробки персональних даних»[492].

Таким чином, СЄС вирішив, що навіть у випадку, якщо передачу персональних даних було обумовлено рішенням Комісії про відповідність гарантій, у разі надходження скарги до національного

491 Рішення Суду ЄС, C-362/14, «Максиміліан Шремс проти Уповноваженого із захисту персональних даних» (*Maximilliam Schrems v. Data Protection Commissioner*) [ВП], від 6 жовтня 2015 р.

492 Рішення Суду ЄС, C-362/14, «Максиміліан Шремс проти Уповноваженого із захисту персональних даних» (*Maximillian Schrems v. Data Protection Commissioner*) [ВП], від 6 жовтня 2015, п. 41.

контролюючого органу, останній має її розглядати з належною сумлінністю. Контролюючий орган може відхилити скаргу, якщо він вирішить, що вона безпідставна. У такому випадку СЄС підкреслив, що право на ефективний засіб судового захисту вимагає, щоб особа мала право на оскарження такого рішення в національних судах, які можуть передати питання до СЄС для попереднього рішення щодо чинності рішення Комісії. Якщо контролюючий орган вважає, що скарга є обґрунтованою, він повинен мати можливість ініціювати юридичне провадження та передати питання до національних судів. Національні суди можуть передати справу до СЄС, оскільки це єдиний орган з повноваженням вирішувати питання щодо чинності рішень Комісії стосовно відповідності гарантій[493].

СЄС далі розглянув чинність рішення «Про безпечну гавань» для встановлення того, чи відповідала система передачі даних правилам захисту персональних даних ЄС. Він вказав, що стаття 3 рішення «Про безпечну гавань» обмежує право національних контролюючих органів (яке забезпечується Директивою про захист персональних даних) вживати заходів для попередження передачі даних у випадку невідповідності рівня захисту персональних даних у США. З огляду на важливу роль незалежного контролюючого органу в забезпеченні дотримання правил із захисту персональних даних, СЄС вирішив, що відповідно до Директиви про захист персональних даних, розтлумаченої в світлі Хартії, Комісія не мала права обмежувати повноваження незалежних наглядових органів у такий спосіб. Обмеження повноважень контролюючих органів була однією з підстав для визнання Судом ЄС рішення «Про безпечну гавань» нечинним.

Таким чином, європейське право вимагає існування незалежного контролю як важливого механізму для забезпечення ефективного захисту даних. Незалежні контролюючі органи є першим контактним пунктом для суб'єктів даних у випадках порушення конфіденційності[494]. Відповідно до права ЄС та права РЄ запровадження незалежних контролюючих органів є обов'язковим. Обидві юридичні системи визначають завдання та повноваження цих органів аналогічно до того, як вони передбачені ЗРЗПД. Загалом контролюючі органи повинні функціонувати однаковим чином як відповідно до права ЄС, так і до права РЄ[495].

493 Там само, пп. 53–66.

494 Загальний регламент захисту персональних даних, стаття 13 (2) (d).

495 Там само, стаття 51; Оновлена Конвенція 108, стаття 15.

5.1 Незалежність

Право ЄС та **право РЄ** вимагає, щоб кожний контролюючий орган діяв з повною незалежністю у виконанні своїх завдань і повноважень[496]. Незалежність контролюючого органу та його членів і працівників від прямих або непрямих зовнішніх впливів є основною гарантією повної об'єктивності при вирішенні питань щодо захисту даних. Не лише закон, який передбачає створення органу, має містити конкретні гарантії незалежності, але й організаційна структура цього органу повинна демонструвати незалежність. У 2010 році СЄС вперше розглянув питання щодо рівня незалежності контролюючого органу[497]. Наведені приклади демонструють визначення «повної незалежності».

Приклад: у справі «*Європейська Комісія проти Німеччини*»[498] Європейська Комісія звернулася до СЄС з вимогою визнати, що Німеччина неправильно виконала вимогу «повної незалежності» стосовно контролюючого органу, який відповідальний за забезпечення захисту даних, та, відповідно, не виконала своїх обов'язків за статтею 28 (1) Директиви із захисту персональних даних. На думку Комісії, той факт, що Німеччина встановила державний нагляд за органами моніторингу обробки персональних даних контролюючого органу в різних федеральних землях (*Länder*) для забезпечення дотримання законодавства про захист персональних даних, порушив вимогу незалежності.

Суд ЄС підкреслив, що слова «з повною незалежністю» повинні тлумачитися на основі наявного формулювання цього положення та цілей, а також системи права ЄС із захисту персональних даних[499]. СЄС наголосив, що наглядові органи є «вартовими» прав, пов'язаних з обробкою персональних даних. Таким чином, їхнє існування в державах-членах розглядається як «суттєвий елемент захисту осіб стосовно обробки персональних даних»[500]. СЄС дійшов висновку, що «при здійсненні своїх завдань контро-

496 Загальний регламент захисту персональних даних, стаття 52 (1); Оновлена Конвенція 108, стаття 15 (5).

497 FRA (2010), Основоположні права: виклики та досягнення у 2010 році, щорічна доповідь 2010, п. 59; FRA (2010), Захист персональних даних у Європейському Союзі: роль національних органів із захисту персональних даних, травень 2010 р.

498 Рішення Суду ЄС, C-518/07, «Європейська Комісія проти Федеративної Республіки Німеччини» (*European Commission v. Federal Republic of Germany*) [ВП], від 9 березня 2010 р., п. 27.

499 Там само, пп. 17 та 29.

500 Там само, п. 23.

люючі органи повинні діяти об'єктивно та безсторонньо. Для досягнення цієї мети вони мають залишатися вільними від будь-якого зовнішнього впливу, включаючи прямий або непрямий вплив органів влади»[501].

СЄС також вирішив, що значення формулювання «повна незалежність» має тлумачитись у світлі незалежності ЄІЗПД, як це передбачено в Регламенті інституцій ЄС про захист персональних даних. У цьому регламенті концепція незалежності вимагає, щоб ЄІЗПД не просив і не приймав інструкцій від будь-кого.

Відповідно, СЄС вирішив, що контролюючий орган у Німеччині не був повністю незалежним у значенні законодавства із захисту персональних даних ЄС у зв'язку з наглядом над ним органів влади.

Приклад: у справі «*Європейська Комісія проти Австрії*»[502] Суд ЄС наголосив на схожих проблемах з незалежністю певних членів і працівників контролюючого органу Австрії (Комісія із захисту персональних даних, КЗПД). СЄС дійшов висновку, що той факт, що Федеральна канцелярія забезпечує контролюючий орган працівниками, підриває вимогу незалежності, яка передбачена законодавством із захисту персональних даних ЄС. СЄС також вирішив, що вимога постійно повідомляти Канцелярію про роботу органу заперечує повну незалежність контролюючого органу.

Приклад: у справі «*Європейська Комісія проти Угорщини*»[503] було заборонено схожу національну практику, яка впливала на незалежність співробітників. СЄС вказав, що «вимога [...] забезпечити, щоб кожний контролюючий орган міг виконувати свої завдання цілком незалежно, передбачає, що держава-член має обов'язок дати можливість цьому органу здійснювати свої повноваження повний строк». СЄС також вирішив, що «достроково припинивши строк виконання повноважень офісу контролюючого органу із захисту персональних даних, Угорщина порушила свої зобов'язання за Директивою 95/46/ЄС[...]».

501 Там само, п. 25.

502 Рішення Суду ЄС, C-614/10, «Європейська Комісія проти Республіки Австрії» (*European Commission v. Republic of Austria*) [ВП], від 16 жовтня 2012 р., пп. 59 та 63.

503 Суд ЄС, C-288/12, «Європейська Комісія проти Угорщини» (*European Commission v. Hungary*) [ВП], від 8 квітня 2014 р., пп. 50 та 67.

Поняття та критерій «повна незалежність» зараз чітко передбачені ЗРЗПД, який включає принципи, встановлені в описаних рішеннях СЄС. Відповідно до регламенту повна незалежність у виконанні своїх завдань та повноважень означає, що[504]:

- члени кожного контролюючого органу повинні залишатися вільними від зовнішнього впливу – прямого або непрямого – та не повинні приймати від будь-кого інструкції;
- члени кожного контролюючого органу мають утримуватися від дій, несумісних з їхніми обов'язками, попереджати конфлікти інтересів;
- держави-члени повинні надавати контролюючому органу необхідні людські, технічні та фінансові ресурси або інфраструктуру для ефективного виконання їхніх завдань;
- держави-члени зобов'язані забезпечити, щоб кожний контролюючий орган сам обирав своїх працівників;
- фінансовий контроль, якому підлягає кожен контролюючий орган відповідно до національного законодавства, не повинен впливати на незалежність. Контролюючі органи повинні мати окремий фінансований державою бюджет, який дозволяє їм належним чином функціонувати.

Незалежність контролюючого органу також вважається суттєвою вимогою відповідно до права РЄ. Оновлена Конвенції 108 вимагає від контролюючого органу «діяти з повною незалежністю та безсторонністю у виконанні своїх завдань і повноважень», не просячи і не отримуючи інструкцій[505]. У такий спосіб Конвенція визнає, що ці контролюючі органи не можуть ефективно захищати права і свободи осіб, пов'язані з обробкою персональних даних, якщо вони не виконують своїх функцій з повною незалежністю. Пояснювальна записка до Оновленої Конвенції 108 встановлює низку чинників, які сприяють гарантіям такої незалежності. Такі елементи включають можливість для контролюючого органу наймати свій апарат працівників та приймати рішення без зовнішнього втручання, а також включають питання тривалості виконання своїх функцій та умови, за яких вони можуть припинити виконувати свої функції[506].

504 Загальний регламент захисту персональних даних, стаття 52.

505 Оновлена Конвенція 108, стаття 15 (5).

506 Пояснювальна записка до Оновленої Конвенції 108.

5.2 Компетенція та повноваження

Відповідно до права ЄС ЗРЗПД окреслює компетенцію та організаційну структуру контролюючих органів та повноваження, з якими вони мають бути спроможними виконувати завдання, які вимагаються регламентом.

Контролюючий орган є головною установою згідно з національним законодавством, що забезпечує дотримання нормативних актів ЄС із захисту персональних даних. Окрім моніторингу, контролюючі органи мають широкий набір завдань і повноважень, що включає активну та превентивну наглядову діяльність. Для здійснення цих завдань контролюючі органи повинні мати належні слідчі, корегувальні та рекомендаційні повноваження такі, як передбачені в статтях 57 та 58 ЗРЗПД[507]:

- консультування контролерів і суб'єктів даних щодо всіх питань із захисту даних;
- ухвалення стандартних договірних положень, обов'язкових корпоративних правил та адміністративних заходів;
- розслідування операцій з обробки даних та здійснення належного реагування;
- вимоги надати будь-яку інформацію, яка є важливою для нагляду за діяльністю контролера;
- внесення попереджень або доган контролерам і приписів щодо повідомлення суб'єктів даних про випадки порушення захисту даних;
- внесення наказів щодо зміни, блокування, видалення або знищення даних;
- накладення тимчасової або постійної заборони на обробку або накладення адміністративних штрафів;
- спрямування справ до суду.

Для виконання своїх функцій контролюючий орган повинен мати доступ до всіх персональних даних та інформації, необхідної для перевірки, а також доступ до будь-яких приміщень, у яких контролер зберігає відповідну інформацію. Відповідно до СЄС повноваження контролюючого органу мають тлумачитися широко для забезпечення повної ефективності захисту персональних даних суб'єктів даних у ЄС.

507 Загальний регламент захисту персональних даних, стаття 57 та 58. Див. також Конвенцію 108, Додатковий протокол, стаття 1.

Приклад: у справі «*Шремс*» Суд ЄС розглядав питання, чи відповідала законодавству із захисту персональних даних ЄС передача персональних даних на територію Сполучених Штатів Америки на підставі першого Договору ЄС – США «Про безпечну гавань» у світлі викриття Едварда Сноудена щодо здійснення масового спостереження Національною службою безпеки США. СЄС у своєму мотивуванні вказав, що національні контролюючі органи в якості незалежних моніторів обробки даних контролерами можуть запобігти передачі персональних даних третім країнам, незважаючи на наявність рішення про належний захист, якщо існують обґрунтовані докази того, що належний захист більше не гарантований у третій країні[508].

Кожний контролюючий орган правомочний виконувати слідчі дії і має повноваження втручатися в межах своєї території. Втім, оскільки діяльність контролерів та операторів часто є транскордонною, а обробка даних впливає на суб'єктів даних у різних державах-членах, виникає питання розділення компетенції між різними контролюючими органами. СЄС мав можливість розглянути це питання у справі «*Велтіммо*».

Приклад: у справі «*Велтіммо*»[509] СЄС розглядав питання щодо повноважень національних контролюючих органів розглядати питання стосовно організацій з місцем реєстрації поза територією їхньої юрисдикції. «Велтіммо» була компанією, зареєстрованою в Словаччині, що вела сайт з продажу майна для Угорщини. Рекламодавці подали скаргу до контролюючого органу із захисту персональних даних Угорщини на порушення законодавства із захисту персональних даних Угорщини. Контролюючий орган наклав штраф на «Велтіммо». Компанія оскаржила штраф у національних судах і справу було направлено до Суду ЄС для з'ясування, чи дозволяла Директива із захисту персональних даних ЄС контролюючому органу держави-члена застосовувати своє національне законодавство із захисту персональних даних до компанії, зареєстрованої в іншій державі, яка є членом Союзу.

СЄС розтлумачив статтю 4 (1) (a) Директиви із захисту персональних даних як таку, що дозволяє застосування законодавства із захисту персональних

508 Суд ЄС, C-362/14, «Максиміліан Шремс проти Уповноваженого із захисту персональних даних» (*Maximilliam Schrems v. Data Protection Commissioner*) [ВП], від 6 жовтня 2015 р., пп. 26–36 та 40–41.

509 Суд ЄС, C-230/14, «"Weltimmo s. r. o." проти Контролюючого органу захисту даних та доступу до інформації Угорщини» (*Weltimmo s.r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*), від 1 жовтня 2015 р.

даних іншої держави-члена, ніж та, у якій зареєстровано компанію, «якщо такий контролер завдяки постійним домовленостям на території тієї держави-члена виконує дійсну та ефективну діяльність – навіть наймінімальнішу – в контексті якої здійснюється така обробка». СЄС вказав, що згідно з наданою йому інформацією «Велтіммо» вела реальну та ефективну діяльність в Угорщині, оскільки компанія мала представника в Угорщині, який був включений до реєстру компаній Словаччини з адресою в Угорщині, а також мав банківський рахунок в угорському банку, поштову скриньку та здійснював діяльність в Угорщині, використовуючи угорську мову. Ця інформація вказує на існування установи та призводить до застосовності угорського законодавства із захисту персональних даних та до поширення юрисдикції контролюючого органу Угорщини. Втім СЄС залишив за національними судами питання перевірки інформації та прийняття рішення щодо того, чи дійсно «Велтіммо» мав установу в Угорщині.

Якщо суд, який направив запит, вирішить, що «Велтіммо» мала установу в Угорщині, тоді угорський наглядовий орган мав повноваження накладати штраф. Однак, якщо національний суд вирішить навпаки, тобто що «Велтіммо» не мала установи в Угорщині, тоді слід застосовувати законодавство тієї держави або держав-членів, де компанія була зареєстрована. У такому разі контролюючий орган Угорщини не мав би повноважень накладати покарання, оскільки повноваження контролюючого органу повинні реалізовуватися відповідно до територіального суверенітету іншої держави-члена. Водночас, оскільки Директива із захисту персональних даних передбачає обов'язок взаємодії контролюючих органів, угорський контролюючий орган міг звернутися до словацького органу-колеги з вимогою розглянути питання, встановити порушення словацького закону та накласти покарання, яке передбачене законодавством Словаччини.

З прийняттям ЗРЗПД правила щодо компетенції контролюючих органів у транскордонних справах тепер детально врегульовано. Регламент встановлює «механізм єдиного вікна» та включає положення про обов'язкову взаємодію між різними контролюючими органами. Для ефективної взаємодії у транскордонних справах ЗРЗПД вимагає, щоб контролюючий орган з головним осідком або єдиним осідком контролера чи оператора мав компетенцію діяти як керівний контролюючий орган для транскордонної обробки[510]. Керівний

510 Загальний регламент захисту персональних даних, стаття 56 (1).

контролюючий орган є відповідальним у транскордонних справах, є єдиною контактною особою контролера або оператора та координує взаємодію з іншими контролюючими органами для досягнення консенсусу. Взаємодія включає обмін інформацією, взаємну допомогу в моніторингу, розслідуванні та прийнятті обов'язкових рішень[511].

У праві РЄ компетенції та повноваження контролюючих органів вказані в статті 15 Оновленої Конвенції 108. Ці повноваження відповідають тим, які передбачені для контролюючих органів відповідно до права ЄС, включаючи повноваження здійснювати розслідування та втручання, повноваження приймати рішення та накладати адміністративні санкції за порушення положень Конвенції, повноваження брати участь у юридичних провадженнях. Незалежні контролюючі органи також мають повноваження розглядати запити та скарги, подані суб'єктами даних, сприяють обізнаності з питань законодавства із захисту персональних даних і консультують суб'єктів прийняття рішень щодо будь-яких законодавчих або адміністративних заходів, які передбачають обробку персональних даних.

5.3 Співпраця

ЗРЗПД встановив загальну систему регулювання співпраці між контролюючими органами та більш конкретні правила взаємодії контролюючих органів стосовно транскордонної діяльності з обробки даних. Відповідно до ЗРЗПД контролюючі органи повинні надавати взаємну допомогу та ділитися відповідною інформацію для узгодженого виконання та застосування Регламенту[512]. Це включає здійснення за вимогою контролюючим органом консультацій, перевірок та розслідувань. Контролюючі органи можуть проводити спільні операції, включаючи спільні розслідування та спільні виконавчі заходи із залученням працівників усіх контролюючих органів[513].

У ЄС контролери та оператори все більше діють на транскордонному рівні. Це вимагає тісної взаємодії між компетентними контролюючими органами держав-членів для забезпечення відповідності обробки персональних даних вимогам ЗРЗПД. Згідно з «механізмом єдиного вікна» Регламенту, якщо контролер або оператор має осідки в декількох державах-членах, або якщо він має один осідок, але операції з обробки суттєво впливають на суб'єктів даних у

511 Там само, стаття 60.

512 Там само, стаття 61 (1)–(3) та 62 (1).

513 Там само, стаття 62 (1).

більш ніж одній державі-члені, контролюючий орган головного (або єдиного) осідка є керівним органом для транскордонної діяльності контролера або оператора. Керівні органи мають повноваження вживати примусових заходів щодо контролера або оператора. Механізм єдиного вікна має на меті покращити гармонізацію та уніфікацію застосування права ЄС із захисту персональних даних серед різних держав-членів. Це також є корисним для комерційних компаній, оскільки вони мають контактувати з керівним органом, а не з декількома контролюючими органами. Це посилює юридичну визначеність для компаній та на практиці також має означати, що рішення приймаються швидше, і що компанії не стикаються з різними контролюючими органами, які висувають суперечливі вимоги.

Ідентифікація керівного органу вимагає визначення місця знаходження головного осідку бізнесової компанії в ЄС. Поняття «головний осідок» визначено в ЗРЗПД. Додатково Робоча група «Стаття 29» видала навчальні матеріали з питань ідентифікації керівного наглядового органу, контролера або оператора, який включає критерії для ідентифікації головного осідку[514].

Для забезпечення високого рівня захисту даних у ЄС керівний орган не діє один. Він має взаємодіяти з іншими зацікавленими контролюючими органами для прийняття рішення щодо обробки персональних даних контролерами та операторами в прагненні досягти консенсусу та забезпечити узгодженість. Співпраця між відповідними контролюючими органами включає обмін інформацією, взаємну допомогу, проведення спільних розслідувань і моніторингів[515]. Під час надання взаємної допомоги контролюючі органи повинні сумлінно ставитися до інформаційних запитів, надісланих іншими контролюючими органами, та вживати контролюючих заходів, як-от, наприклад, попередній дозвіл та консультування контролера даних щодо його обробки, перевірки або розслідувань. Допомога контролюючим органам в інших державах-членах повинна надаватися на запит без неналежних затримок та не пізніше ніж через один місяць після отримання запиту[516].

Якщо контролер має осідки в декількох державах-членах, контролюючі органи можуть проводити спільні операції, включаючи розслідування та примусові заходи, до яких залучаються члени контролюючих органів інших держав-членів[517].

514 Робоча група «Стаття 29» (2016), *Посібник щодо ідентифікації головного контрольного органу контролера або оператора*, РГ 244, Брюссель, від 13 грудня 2016 р., переглянутий 5 квітня 2017 р.

515 Загальний регламент захисту персональних даних, стаття 60 (1)–(3).

516 Там само, стаття 61 (1) та (2).

517 Там само, стаття 62 (1).

Співпраця між різними контролюючими органами є також важливою вимогою відповідно до нормативно-правових документів РЄ. Оновлена Конвенція 108 передбачає, що контролюючі органи повинні взаємодіяти один з одним задля ефективного виконання своїх завдань[518]. Це має відбуватися, наприклад, шляхом надання один одному важливої та корисної інформації, координації розслідувань, проведення спільних дій[519].

5.4 Європейська рада із захисту персональних даних

Важливість незалежних контролюючих органів та їхніх основних повноважень відповідно до права ЄС із захисту персональних даних було описано в попередній главі. Європейська рада із захисту персональних даних (ЄРЗПД) є іншим важливим суб'єктом у ЄС щодо забезпечення ефективного та узгодженого виконання правил захисту персональних даних.

У ЗРЗПД вказано, що ЄРЗПД є органом ЄС з юридичною правосуб'єктністю[520]. Це правонаступник Робочої групи «Стаття 29»[521], яка була утворена Директивою із захисту персональних даних для надання порад Комісії щодо будь-яких заходів ЄС, які впливають на права осіб у плані обробки персональних даних та приватності, сприяння уніфікованому застосуванню Директиви та надання експертних висновків Комісії щодо питань захисту персональних даних. Робоча група «Стаття 29» складалася з представників контролюючих органів держав-членів ЄС разом із представниками з Комісії та ЄРЗПД.

Аналогічно до Робочої групи, ЄРЗПД складається з голів контролюючих органів кожної держави-члена та ЄІЗПД або їхніх представників[522]. ЄІЗПД має таке саме право голосу, крім випадків вирішення спорів, у яких він може голосувати лише за рішення щодо принципів і правил, застосовних до інституцій ЄС, що по суті відповідають правилам ЗРЗПД. Комісія має право брати участь

518 Оновлена Конвенція 108, стаття 16 та 17.

519 Там само, стаття 12 bis (7).

520 Загальний регламент захисту персональних даних, стаття 68.

521 Відповідно до Директиви 95/46/ЄС, Робоча група «Стаття 29» мала надавати рекомендації Комісії щодо будь-яких заходів ЄС, які мали вплив на права осіб щодо обробки персональних даних та приватності, сприяти уніфікованому застосуванню Директиви та надавати експертні висновки Комісії щодо питань захисту даних. Робоча група «Стаття 29» складалася з представників контролюючих органів держав-членів ЄС, Комісії та Європейського інспектора із захисту персональних даних (ЄІЗПД).

522 Загальний регламент захисту персональних даних, стаття 68 (3).

у діяльності ЄРЗПД та її засіданнях, але не має права голосу[523]. Рада обирає Голову (який має повноваження її представляти) та двох заступників з її членів простою більшістю на п'ять років. Крім того, ЄРЗПД у своєму розпорядженні також має секретаріат, який забезпечує ЄІЗПД, щоб Рада мала аналітичну, адміністративну та логістичну підтримку[524].

Завдання ЄРЗПД детально передбачені у статтях 64, 65 та 70 ЗРЗПД та включають широкий обсяг обов'язків, які можуть бути розділені на три головні напрямки діяльності:

- **Узгодженість:** ЄРЗПД може прийняти юридично обов'язкові рішення у трьох випадках: якщо контролюючий орган висловив відповідне та обґрунтоване заперечення у справах щодо єдиного вікна, якщо виникають суперечки щодо того, який з контролюючих органів має бути керівним та, нарешті, коли контролюючий орган не звертається з вимогою до ЄРЗПД надати висновок або не користується наданим висновком[525]. Головним завданням ЄРЗПД є забезпечення узгодженого застосування ЗРЗПД у ЄС, і також Рада відіграє провідну роль у застосуванні механізму узгодження, описаного в розділі 5.5.
- **Консультації:** завдання ЄРЗПД включають надання порад Комісії щодо будь-яких питань, пов'язаних із захистом персональних даних у Союзі, як, наприклад, зміни до ЗРЗПД, перевірка законодавства ЄС, яке охоплює обробку даних та яке може суперечити правилам захисту персональних даних ЄС, або щодо рішень Комісії про відповідність, які надають можливість передачі персональних даних третій державі або міжнародній організації.
- **Керівні настанови:** Рада також видає настанови, рекомендації та узагальнює інформацію щодо кращої практики для підтримки узгодженого застосування регламенту та сприяння взаємодії та обміну знаннями між контролюючими органами. Крім того, вона має заохочувати об'єднання контролерів або операторів створювати кодекси поведінки, а також встановлювати механізм сертифікації та штампів.

Рішення ЄРЗПД можуть бути оскаржені до СЄС.

523 Там само, стаття 68 (4) та (5).

524 Там само, стаття 73 та 75.

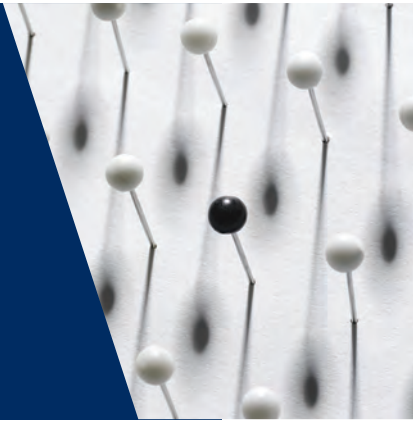
525 Там само, стаття 65.

5.5 Механізм узгодженості ЗРЗПД

ЗРЗПД встановлює механізм узгодженості для забезпечення узгодженого, послідовного застосування регламенту в усіх державах-членах, завдяки якому контролюючі органи взаємодіють один з одним та, якщо необхідно, з Комісією. Механізм узгодження використовується в двох випадках. Перший стосується висновків ЄРЗПД у разі, якщо компетентний орган має намір вжити заходів, наприклад таких, як затвердження переліку операцій з обробки, які вимагають оцінки впливу на захист персональних даних (ОВЗПД) або визначення стандартів договірних умов. Другий випадок стосується обов'язкових рішень ЄРЗПД для контролюючих органів у справах щодо єдиного вікна та невиконання контролюючим органом положень висновку ЄРЗПД або не звернення за ним.

6

Права суб'єктів даних та їх реалізація



ЄМ	Питання, що висвітлюються	РЄ
Право бути поінформованим		
Загальний регламент захисту персональних даних, стаття 12 СЄС, C-473/12, «Професійний інститут агентів з нерухомості (IPI) проти Джеффрі Енглберта та інших», (*Institut professionnel des agents immobiliers (IPI) v. Englebert*) 2013 СЄС, C-201/14, «Смаранда Бара та інші проти Національного фонду медичного страхування та інших», (*Smaranda Bara and Others v. Casa Naţională de Asigurări de Sănătate and Others*), 2015	**Прозорість інформації**	Оновлена Конвенція 108, стаття 8
Загальний регламент захисту персональних даних, стаття 13 (1) і (2) та стаття 14 (1) і (2)	**Зміст інформації**	Оновлена Конвенція 108, стаття 8 (1)
Загальний регламент захисту персональних даних, стаття 13 (1) та стаття 14 (3)	**Час надання інформації**	Оновлена Конвенція 108, стаття 9 (1) (b).

ЄМ	Питання, що висвітлюються	РЄ
Загальний регламент захисту персональних даних, стаття 12 (1), (5) і (7)	**Засоби інформування**	Оновлена Конвенція 108, стаття 9 (1) (b).
Загальний регламент захисту персональних даних, стаття 13 (2) (d) та стаття 14 (2) (e), статті 77, 78 і 79	**Право на оскарження**	Оновлена Конвенція 108, стаття 9 (1) (f)
Право на доступ		
Загальний регламент захисту персональних даних, стаття 15 (1) СЄС, C-553/07, «Мер та члени міської ради Роттердама проти М.Е.Е. Рейкебура», (*College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer*), 2009 СЄС, об'єднані справи C-141/12 та C-372/12, «YS проти Міністра з питань імміграції, інтеграції та притулку» та «Міністр з питань імміграції, інтеграції та притулку проти M. та S.», (*YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S*), 2014 СЄС, C-434/16, «Пітер Новак проти Комісара із захисту персональних даних», (*Peter Nowak v. Data Protection Commissioner*), 2017 Загальний регламент захисту персональних даних, стаття 15 (1)	**Право на доступ до власних даних**	Оновлена Конвенція 108, стаття 9 (1) (b) ЄСПЛ, «Леандер проти Швеції», (*Leander v. Sweden*), № 9248/81, 1987
Право на виправлення		
Загальний регламент захисту персональних даних, стаття 16	**Виправлення неточних персональних даних**	Оновлена Конвенція 108, стаття 9 (1) (e) ЄСПЛ, «Джемалеттін Джанлі проти Туреччини»,

ЄМ	Питання, що висвітлюються	РЄ
		(Cemalettin Canli v. Turkey) № 22427/04, 2008 ЄСПЛ, «Чуботару проти Молдови», *(Ciubotaru v. Moldova)* № 27138/04, 2010
Право на видалення		
Загальний регламент захисту персональних даних, стаття 17 (1)	**Видалення персональних даних**	Оновлена Конвеція 108, стаття 9 (1) (e) ЄСПЛ, «Зегерштед-Віберг та інші проти Швеції», *(Segerstedt Wiberg and Others v. Sweden)* № 62332/00, 2006
СЄС, C-131/12, «"Google Spain SL", "Google Inc." проти Іспанського агентства захисту даних (AEPD) та Маріо Костеха Гонсалеса» (*Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*), [ВП], 2014 СЄС, C-398/15, «Торгово-промислова та сільськогосподарська палата м. Лечче проти Сальваторе Манні» (*Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*), 2017	**Право бути забутим**	
Право на обмеження обробки		
Загальний регламент захисту персональних даних, стаття 18 (1)	**Право обмежувати використання персональних даних**	
Загальний регламент захисту персональних даних, стаття 19	**Обов'язок повідомлення**	
Право на мобільність даних		
Загальний регламент захисту персональних даних, стаття 20	**Право на мобільність даних**	

ЄМ	Питання, що висвітлюються	РЄ
Право на заперечення		
Загальний регламент захисту персональних даних, стаття 21 (1) СЄС, C-398/15, «Торгово-промислова та сільськогосподарська палата м. Лечче проти Сальваторе Манні» (*Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*), 2017	**Право на заперечення з огляду на індивідуальну ситуацію суб'єкта даних**	Рекомендації щодо профайлінгу, стаття 5.3 Оновлена Конвенція 108, стаття 9 (1) (d)
Загальний регламент захисту персональних даних, стаття 21 (2)	**Право на заперечення використання персональних даних з метою прямого маркетингу**	Рекомендації щодо прямого маркетингу, стаття 4.1
Загальний регламент захисту персональних даних, стаття 21 (5)	**Право на заперечення автоматизованими засобами**	
Права, пов'язані з автоматизованим прийняттям рішень і профайлінгом		
Загальний регламент захисту персональних даних, стаття 22 Загальний регламент захисту персональних даних, стаття 21 Загальний регламент захисту персональних даних, стаття 13 (2) (f)	**Права, пов'язані з автоматизованим прийняттям рішень і профайлінгом** **Право заперечувати проти автоматизованого прийняття рішень** **Права на змістовне роз'яснення**	Оновлена Конвенція 108, стаття 9 (1) (a) Оновлена Конвенція 108, стаття 9 (1) (c)
Засоби юридичного захисту, відповідальність, санкції та відшкодування		
Хартія, стаття 47 СЄС, C-362/14, «Максиміліан Шремс проти Уповноваженого із захисту персональних даних» (*Maximillian Schrems v. Data Protection Commissioner*) [ВП], 2015	**Порушення національного законодавства про захист персональних даних**	ЄСПЛ, стаття 13 (лише для держав – членів РЄ) Оновлена Конвенція 108, стаття 9 (1) (f), 12, 15, 16-21 ЄСПЛ, «K.U. проти Фінляндії», (*K.U. v. Finland*) № 2872/02, 2008

ЄМ	Питання, що висвітлюються	РЄ
Загальний регламент захисту персональних даних, стаття 77–84		ЄСПЛ, «Бірюк проти Литви», (*Biriuk v. Lithuania*), № 23373/03, 2008
Регламент інститутів ЄС про захист персональних даних, стаття 34 та 49 СЄС, C-28/08 P, «Європейська Комісія проти "The Bavarian Lager Co. Ltd"» [ВП] (*European Commission v. The Bavarian Lager Co. Ltd*), 2010	**Порушення законодавства ЄС інституціями та органами ЄС**	

Ефективність правових норм у цілому та прав суб'єктів даних зокрема значною мірою залежить від існування відповідних механізмів їх реалізації. У цифрову епоху обробка даних стає повсюдною та все важче зрозумілою людям. Для зменшення дисбалансу між можливостями суб'єктів даних та контролерів фізичні особи були наділені певними правами для здійснення кращого контролю над обробкою своїх персональних даних. Право на доступ до власних даних і право на їх виправлення закріплені у статті 8 (2) Хартії основних прав ЄС, документі, який є частиною первинного законодавства ЄС і має засадниче значення у правовій системі ЄС. Вторинне законодавство ЄС, зокрема, Загальний регламент захисту персональних даних, запровадило цілісну правову базу, яка вповноважує суб'єктів даних шляхом надання їм прав відносно контролерів. Окрім прав на доступ до власних даних і виправлення, ЗРЗПД визначено ряд інших прав, таких як право на видалення даних («право бути забутим»), права на заперечення або обмеження обробки персональних даних, а також права, пов'язані з автоматизованим прийняттям рішень та профайлінгом. Подібні гарантії, що дозволяють суб'єктам даних здійснювати ефективний контроль за обробкою своїх персональних даних, також включені до Оновленої Конвенції 108. У статті 9 перераховані права, які фізичні особи повинні мати змогу реалізувати відносно обробки своїх персональних даних. Договірні Сторони повинні гарантувати, що такі права є доступними для кожного суб'єкта даних у межах їхньої юрисдикції та супроводжуються ефективними юридичними та практичними засобами, які дозволяють

їх реалізовувати. Окрім наділення фізичних осіб правами, не менш важливим є запровадження механізмів, що нададуть можливість суб'єктам даних оскаржувати порушення своїх прав, притягувати контролерів до відповідальності та вимагати відшкодування. Право на ефективний засіб юридичного захисту, гарантоване ЄКПЛ та Хартією, вимагає, щоб кожному були доступними судові засоби захисту.

6.1. Права суб'єктів даних

Ключові моменти

- Кожний суб'єкт даних має право на інформацію про будь-яку обробку контролером його персональних даних, окрім обмеженої кількості винятків.
- Суб'єкти даних мають право на:
  - доступ до власних персональних даних та отримання певної інформації про обробку;
  - виправлення своїх персональних даних контролером, який здійснює обробку цих даних, якщо вони є неточними;
  - видалення своїх персональних даних контролером, у тих випадках, якщо такі дані ним обробляються неправомірно;
  - тимчасове обмеження обробки;
  - передачу своїх даних іншому контролеру за певних умов.
- Крім того, суб'єкти даних мають право на заперечення проти обробки:
  - з підстав, що стосуються їхньої індивідуальної ситуації;
  - своїх персональних даних з метою прямого маркетингу.
- Суб'єкти даних мають право не підпорядковуватися рішенням, які ґрунтуються виключно на автоматизованій обробці, в тому числі профайлінгу, та мають юридичні наслідки для них або подібним чином істотно впливають на них. Суб'єкти даних також мають право:
  - на людське втручання з боку контролера;
  - висловлювати свою думку та оскаржувати рішення, яке ґрунтується на автоматизованій обробці.

6.1.1 Право бути поінформованим

Відповідно до **права РЄ** та **ЄС** контролери операцій з обробки зобов'язані інформувати суб'єкта даних під час збирання персональних даних про заплановану обробку. Цей обов'язок не залежить від запиту суб'єкта даних, контролер повинен заздалегідь виконувати його, незалежно від того, чи виявляє суб'єкт даних інтерес до інформації.

Відповідно до права РЄ, а також згідно зі статтею 8 Оновленої Конвенції 108, Договірні Сторони повинні забезпечити, щоб контролери інформували суб'єктів даних про ідентифікаційні дані контролера та їхнє місце розташування, юридичні підстави та мету обробки, категорії персональних даних, які підлягають обробці, одержувачів їхніх персональних даних (якщо такі є), а також про те, як скористатися своїми правами відповідно до статті 9, що включає право на доступ, виправлення та засіб юридичного захисту. Будь-яка інша додаткова інформація, яка вважається необхідною для забезпечення чесної та прозорої обробки персональних даних, має бути також повідомлена суб'єкту даних. Пояснювальна записка до Оновленої Конвенції 108 уточнює, що надана суб'єкту даних інформація «має бути легкодоступною, чіткою, зрозумілою та адаптованою для відповідних суб'єктів даних»[526].

Відповідно до права ЄС, принцип прозорості вимагає, щоб будь-яка обробка персональних даних була, за загальним правилом, прозорою для фізичних осіб. Фізичні особи мають право знати, яким чином та які персональні дані збираються, використовуються або обробляються іншим способом, а також бути поінформовані про ризики, гарантії та права стосовно обробки[527]. Стаття 12 ЗРЗПД, таким чином, встановлює широкий комплексний обов'язок контролерів надавати прозору інформацію та/або повідомляти, як саме суб'єкт даних може скористатися своїми правами[528]. Інформація повинна бути стислою, прозорою, доступною для розуміння та поданою в доступній формі, з використанням чітких і простих формулювань. Вона має надаватись у письмовій формі, у тому числі, за потреби, в електронній формі, а також може надаватися навіть усно на запит суб'єкта даних, якщо його особу встановлено беззаперечно. Інформація має бути надана без надмірної затримки чи вимог оплати[529].

526 Пояснювальна записка до Оновленої Конвенції 108, п. 68.

527 Загальний регламент захисту персональних даних, п. 39 преамбули.

528 Там само, стаття 13 та 14; Оновлена Конвенція 108, стаття 8 (1) (b).

529 Загальний регламент захисту персональних даних, стаття 12 (5); Оновлена Конвенція 108, стаття 9 (1) (b).

Статті 13 та 14 ЗРЗПД розглядають право суб'єктів даних бути поінформованими, як у випадках, коли персональні дані отримані від них безпосередньо, так і якщо дані були отримані не від них.

Обсяг права на інформацію та його обмеження відповідно до права ЄС було роз'яснено у практиці Суду ЄС.

Приклад: у справі «*Професійний інститут агентів з нерухомості (IPI) проти Джеффрі Енглберта та інших*»[530] СЄС повинен був розтлумачити статтю 13 (1) Директиви 95/46. Ця стаття надавала державам-членам вибір, чи ухвалювати законодавчі заходи з метою обмеження обсягу права суб'єкта даних бути поінформованим, якщо це необхідно для захисту, серед іншого, прав та свобод інших осіб, запобігання і розслідування злочинів чи порушень етичних стандартів певних професій. IPI – це професійний орган агентів з нерухомості в Бельгії, відповідальний за забезпечення належної діяльності агентів з нерухомості. Він звернувся до національного суду з вимогою визнати, що відповідачі порушили професійні правила, та зобов'язати їх припинити різні види діяльності агентства з нерухомості. Позов ґрунтувався на доказах, наданих приватними детективами, послуги яких IPI використав.

Національний суд мав сумніви щодо цінності доказів детективів, враховуючи можливість того, що вони були зібрані без дотримання вимог бельгійського законодавства про захист персональних даних, зокрема обов'язку інформування суб'єкта даних про обробку його персональних даних до початку збору такої інформації. СЄС звернув увагу, що відповідно до статті 13 (1) держави-члени «можуть», але не зобов'язані передбачати у своєму національному законодавстві винятки щодо обов'язку інформувати суб'єктів даних про обробку їхніх даних. Оскільки стаття 13 (1) включає запобігання, розслідування, виявлення і судове переслідування злочинів чи порушень етики як підстави, на яких держави-члени можуть обмежити права фізичних осіб, діяльність такого органу як IPI та приватних детективів, що діють від його імені, може ґрунтуватися на цьому положенні. Однак, якщо держава-член не передбачила такого винятку, суб'єкт персональних даних має бути поінформований.

530 Рішення Суду ЄС, C-473/12, «Професійний інститут агентів з нерухомості (IPI) проти Джеффрі Енглберта та інших» (*Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert and Others*), від 07 листопада 2013 р.

Приклад: у справі «*Смаранда Бара та інші проти Національного фонду медичного страхування та інших*»[531] СЄС роз'яснив, чи забороняє законодавство ЄС національному державному виконавчому органу передавати персональні дані іншому державному виконавчому органу для подальшої обробки без інформування суб'єкта даних про таку передачу та обробку. У цій справі Національне агентство з питань управління не поінформувало заявників, що воно передало їхні дані до Національного фонду медичного страхування до моменту передачі. СЄС постановив, що вимога законодавства ЄС стосовно інформування суб'єкта даних про обробку його персональних даних має «особливо важливе значення, оскільки це впливає на реалізацію суб'єктами даних свого права на доступ до даних, права на виправлення даних, що обробляються [...], та права на заперечення проти обробки цих даних». Принцип чесної обробки вимагає інформування суб'єкта даних про передачу його даних до іншого державного органу для подальшої обробки останнім. Відповідно до статті 13 (1) Директиви 95/46, держави-члени можуть обмежити право бути поінформованим, якщо це вважається необхідним для захисту важливого економічного інтересу держави, включаючи податкові питання. Однак такі обмеження мають бути передбачені на рівні законодавства. Оскільки законодавством не було визначено ані даних, які мають передаватись, ані детальних умов передачі, а, навпаки, обмеження були передбачені лише протоколом між двома державними органами, умови відступу відповідно до законодавства ЄС не були дотримані. Заявників повинні були заздалегідь інформувати про передачу їхніх даних до Національного фонду медичного страхування та подальшу обробку цих даних вказаним органом.

Зміст інформації

Відповідно до статті 8 (1) Оновленої Конвенції 108 контролер зобов'язаний надавати суб'єкту даних будь-яку інформацію, яка забезпечує чесну та прозору обробку персональних даних, в тому числі про:

- ідентифікаційні дані контролера та його місце розташування або осідок;
- юридичні підстави та цілі запланованої обробки;
- категорії оброблюваних персональних даних;

531 Рішення Суду ЄС, C-201/14, «Смаранда Бара та інші проти Національного фонду медичного страхування та інших» (*Smaranda Bara and Others v. Casa Naţională de Asigurări de Sănătate and Others*) від 01 жовтня 2015 р.

- одержувачів або категорії одержувачів персональних даних, якщо такі є;
- способи реалізації суб'єктами даних своїх прав.

Згідно з ЗРЗПД, якщо персональні дані отримуються від суб'єкта даних, контролер під час отримання персональних даних зобов'язаний надати йому наступну інформацію[532]:

- ідентифікаційні та контактні дані контролера, в тому числі дані відповідальних осіб із питань захисту персональних даних, якщо такі є;
- мета та правові підстави обробки, тобто угода чи юридичний обов'язок;
- легітимний інтерес контролера, якщо це є підставою обробки;
- кінцеві одержувачі або категорії одержувачів персональних даних;
- чи будуть дані передані до третьої країни або міжнародної організації, чи ґрунтується це на рішенні про відповідність або на належних гарантіях;
- період зберігання персональних даних, або якщо встановлення такого періоду неможливе, критерії, за якими він визначатиметься;
- права суб'єктів даних щодо обробки, такі як права на доступ, виправлення, видалення та права на обмеження чи заперечення проти обробки;
- надання персональних даних вимагається на підставі закону чи угоди, чи зобов'язаний суб'єкт даних надавати свої дані, наслідки у випадку ненадання персональних даних;
- наявність автоматизованого прийняття рішень, в тому числі профайлінгу;
- право подавати скаргу до контрольного органу;
- наявність права на відкликання згоди.

У випадках автоматизованого прийняття рішень, в тому числі профайлінгу, суб'єкти даних повинні отримати змістовну інформацію про логіку профайлінгу, значення та передбачувані для них наслідки обробки.

У випадках, коли персональні дані отримуються не від суб'єкта даних безпосередньо, контролер повинен повідомити фізичну особу про джерело походження персональних даних. У будь-якому випадку, контролер повинен, серед іншого, поінформувати суб'єкта даних про наявність автоматизованого

532 Загальний регламент захисту персональних даних, стаття 13 (1); Оновлена Конвенція 108, стаття 7-1.

прийняття рішень, в тому числі профайлінгу[533]. На завершення, якщо контролер має намір здійснювати обробку персональних даних для досягнення іншої мети, ніж та, яку було зазначено суб'єкту даних спочатку, принципи обмеження мети та прозорості вимагають від контролера надавати суб'єкту даних інформацію про таку нову мету. Контролери мають надавати інформацію перед будь-якою подальшою обробкою. Інакше кажучи, у випадках, коли суб'єкт даних надав згоду на обробку даних, контролер повинен отримати оновлену згоду, якщо мета обробки змінюється або додається нова мета.

Час надання інформації

ЗРЗПД розрізняє два варіанти та два моменти часу, коли контролер має надати суб'єкту даних інформацію:

- Якщо персональні дані отримуються від суб'єкта даних, контролер повинен повідомити його про всю пов'язану інформацію та права відповідно до ЗРЗПД в момент отримання даних[534]. Якщо контролер має намір у подальшому обробляти дані з іншою метою, він має надати всю відповідну інформацію до початку обробки.
- Якщо персональні дані отримані не від суб'єкта даних, контролер зобов'язаний надати йому інформацію про обробку «в розумний строк після отримання персональних даних, але не пізніше одного місяця», або до розкриття даних третій стороні[535].

У пояснювальній записці до Оновленої Конвенції 108 міститься застереження, що у разі, якщо інформування суб'єкта даних при початку обробки є неможливим, це може бути зроблено на більш пізньому етапі, наприклад, коли з'явиться контакт контролера з суб'єктом даних з будь-якої причини[536].

Різні способи надання інформації

Відповідно до права РЄ та ЄС, інформація, яку має надавати контролер, повинна бути стислою, прозорою, доступною для розуміння та поданою в доступній формі. Вона повинна бути надана в письмовому або в будь-якому

533 Загальний регламент захисту персональних даних, стаття 13 (2) та 14 (2) (f).

534 Там само, стаття 13 (1) і (2), загальна частина, у якій Загальний регламент захисту персональних даних посилається на інформацію про обов'язок, який має виконуватись у «момент отримання інформації».

535 Там само, стаття 13 (3) та 14 (3); див. також згадування щодо розумних строків та відсутності значних затримок у статті 8 (1) (b) Оновленої Конвенції 108.

536 Пояснювальна записка до Оновленої Конвенції 108, п. 70.

іншому вигляді формі, в тому числі в електронній формі, з використанням чітких, простих та легкозрозумілих формулювань. Під час надання інформації контролер може використовувати стандартизовані іконки з метою передання її в доступній для візуального сприйняття та розуміння формі[537]. Наприклад, іконка у вигляді замкà може бути використаною для повідомлення про те, що дані збираються безпечно та/або зашифровуються. Суб'єкти даних можуть вимагати надати інформацію в усній формі. Інформація має бути безоплатною, крім якщо запити суб'єкта даних є явно необґрунтованими або надмірними (тобто повторювального характеру)[538]. Вільний доступ до інформації є вкрай важливим для здатності суб'єктів даних реалізовувати свої права, передбачені законодавством ЄС про захист персональних даних.

Принцип чесної обробки вимагає викладення інформації в доступній для розуміння суб'єктів даних формі. Мова, якою викладено інформацію, має бути зрозумілою тим, кому вона адресується. Її рівень і тип мають відрізнятися залежно від цільової аудиторії, наприклад, дорослі або діти, широка громадськість або наукові експерти. Питання, як збалансувати цей аспект доступної для розуміння інформації, розглядається у висновку Робочої групи «Стаття 29» щодо більш гармонізованих інформаційних положень, у якому підтримується ідея так званих багаторівневих повідомлень[539], які надають можливість суб'єкту даних вирішити, якому рівню деталізації він або вона надає перевагу. Втім цей спосіб представлення інформації не звільняє контролера від його обов'язку відповідно до статей 13 та 14 ЗРЗПД. Контролер, однак, має надати суб'єкту даних повну інформацію.

Один з найефективніших способів надання інформації є розміщення на домашній сторінці контролера відповідних інформаційних повідомлень, як, наприклад, щодо політики конфіденційності вебсайту. Однак в інформаційній політиці компаній або державних органів має враховуватися, що існує велика частина населення, яка не користується інтернетом.

537 Європейська Комісія буде надалі встановлювати перелік інформації, яка має бути представлена у вигляді іконок, та процедури запровадження стандартизованих іконок шляхом ухвалення делегованих актів; див. Загальний регламент захисту персональних даних, стаття 12 (8).

538 Загальний регламент захисту персональних даних, стаття 12 (1), (5) і (7) та Оновлена Конвенція 108, стаття 9 (1) (b).

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

Повідомлення щодо конфіденційного характеру обробки персональних даних на вебсторінці може виглядати наступним чином:

Про нас

Контролером обробки даних є компанія «Bed and Breakfast C&U», заснована у (адреса місця знаходження: xxx); тел.: xxx; факс: xxx; електронна адреса: *info@c&u.com*, контактні дані спеціаліста з питань захисту персональних даних: [xxx].

Інформаційне повідомлення щодо персональних даних є частиною положень та умов, які регулюють надання послуг у нашому готелі.

Які ваші дані ми просимо від вас?

Ми просимо від вас такі ваші персональні дані: ім'я, поштову адресу, номер телефона, електронну адресу, інформацію про місце перебування, номер дебетової та кредитної картки та IP-адресу чи доменні імена комп'ютерів, використаних вами для з'єднання з нашим вебсайтом.

Чому ми просимо ваші дані?

Ми обробляємо дані на підставі вашої згоди та з метою здійснення бронювання, укладання та виконання угод щодо послуг, які ми вам пропонуємо, а також на виконання вимог, встановлених законодавством, зокрема Закону про місцеві збори, який зобов'язує нас збирати ваші персональні дані для забезпечення сплати місцевого податку на проживання.

Яким чином ми обробляємо ваші дані?

Ваші персональні дані зберігатимуться протягом трьох місяців. Ваші дані не підлягають автоматизованим процедурам прийняття рішень.

Компанія «Bed and Breakfast C&U» дотримується суворих процедур безпеки для уникнення пошкодження, знищення або розголошення третій стороні ваших даних без дозволу та запобігання несанкціонованому доступу до них. Комп'ютери, які зберігають інформацію, утримуються в захищеному місці з обмеженим фізичним доступом. Ми використовуємо надійні захисні системи та інші засоби обмеження електронного доступу. Якщо дані мають бути передані третій стороні, ми вимагаємо, щоб та вжила подібних заходів захисту ваших персональних даних.

Вся інформація, яку ми збираємо та фіксуємо, доступна лише нашим працівникам. Доступ до персональних даних надається лише особам, яким інформація необхідна для виконання обов'язків згідно з цією угодою. Ми безпосередньо звернемось до вас у разі необхідності отримання інформації для встановлення особи. Ми можемо просити вас взаємодіяти з нашою системою перевірки безпеки до розкриття Вам інформації. Ви можете оновити надану нам інформацію у будь-який час, зв'язавшись з нами безпосередньо.

Які ваші права?

Ви маєте право на доступ до власних даних, отримувати копії ваших даних, звертатись із вимогою їх видалити або виправити чи передати іншому контролеру.

Ви можете звернутися до нас із запитами на адресу *info@c&u.com*. Відповідь буде надана протягом місяця, але якщо в запиті будуть порушені досить складні питання або ми отримаємо занадто багато інших запитів, ми проінформуємо вас про те, що цей період може бути продовжено ще на два місяці.

Доступ до власних персональних даних

Ви маєте право на доступ до власних даних, які надаються на вимогу, право бути обізнаним про підстави обробки даних, вимагати їх виправлення або видалення, а також право не бути суб'єктом суто автоматизованого рішення без врахування вашої думки.

Ви можете звернутися до нас із запитами на електронну адресу *info@c&u.com*. Ви також маєте право на заперечення проти обробки, право відкликати Вашу згоду, подати скаргу до національного контролюючого органу, у разі якщо Ви вважаєте, що обробка даних порушує законодавство, та вимагати відшкодування за шкоду, заподіяну внаслідок неправомірної обробки.

Право на оскарження

ЗРЗПД вимагає від контролера інформувати суб'єкта даних про механізми захисту згідно з національним законодавством та законодавством ЄС у

випадках порушення умов безпеки обробки персональних даних. Контролер має проінформувати суб'єкта даних про його право подати скаргу щодо порушення захисту персональних даних до контролюючого органу та, за необхідності, до національного суду[540]. Право РЄ також встановлює право суб'єкта даних бути проінформованим про засоби реалізації своїх прав, у тому числі права на засіб юридичного захисту, закріпленого в статті 9 (1) (f).

Винятки з обов'язку інформувати

ЗРЗПД передбачає виняток з обов'язку інформувати. Відповідно до статті 13 (4) та статті 14 (5) ЗРЗПД обов'язок інформувати суб'єкта даних не застосовується, у разі якщо суб'єкт даних уже має всю відповідну інформацію[541]. Крім того, у випадках отримання персональних даних не від суб'єкта даних, обов'язок інформувати не буде застосовуватись, якщо надання інформації є неможливим або непропорційним, зокрема, відносно обробки персональних даних для досягнення цілей у суспільних інтересах, цілей наукового чи історичного дослідження або статистичних цілей[542].

Більше того, відповідно до ЗРЗПД держави-члени мають свободу розсуду щодо обмеження обов'язків та прав, наданих фізичним особам Регламентом, якщо це необхідний та пропорційний захід у демократичному суспільстві, наприклад, для охорони національної та громадської безпеки, оборони, захисту судових розслідувань і проваджень або захисту економічних та фінансових інтересів, а також приватних інтересів, які переважають інтереси захисту персональних даних[543].

Будь-які винятки або обмеження повинні бути необхідними в 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[544]. Однак, як мінімальний рівень захисту, національне законодавство має забезпечувати дотримання сутності основних прав і свобод, захищених правом ЄС[545]. Право

540 Загальний регламент захисту персональних даних, стаття 13 (2) (d) та 14 (2) (e); Оновлена Конвенція 108, стаття 8 (1) (f).

541 Там само, стаття 13 (4) та 14 (5) (a).

542 Там само, стаття 14 (5) (b)–(e).

543 Загальний регламент захисту персональних даних, стаття 23 (1).

544 Загальний регламент захисту персональних даних, стаття 15.

545 Загальний регламент захисту персональних даних, стаття 23 (1).

ЄС вимагає, щоб національне законодавство містило спеціальні положення, які визначають мету обробки, категорії персональних даних, які охоплюються, гарантії та інші процедурні вимоги[546].

У випадку збору даних у цілях наукового або історичного дослідження, статистичних цілях або для досягнення цілей у суспільних інтересах, законодавством Союзу або держави-члена можуть бути передбачені відступи від обов'язку інформувати, якщо такий обов'язок, ймовірно, унеможливить або серйозно обмежить досягнення відповідних цілей[547].

Подібні обмеження містяться в нормативних документах РЄ, відповідно до яких права, гарантовані статтею 9 Оновленої Конвенції 108, можуть бути звужені згідно зі статтею 11 Оновленої Конвенції 108 за жорстких умов. Більше того, відповідно до статті 8 (2) Оновленої Конвенції 108 обов'язок щодо прозорості обробки, покладений на контролерів, не застосовується, якщо суб'єкт даних вже має інформацію.

Право на доступ до власних даних

Відповідно до права РЄ право на доступ до власних персональних даних прямо визнається статтею 9 Оновленої Конвенції 108. Згідно з цією статтею кожна фізична особа має право отримувати на вимогу інформацію про обробку персональних даних, що стосуються її або його особисто, у доступній для розуміння формі. Право на доступ до власних даних визнано не лише нормами Оновленої Конвенції 108, а й практикою ЄСПЛ. 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[548]. Однак право на доступ до персональних даних, які зберігаються державними або приватними установами, може за певних обставин обмежуватися[549].

Відповідно до права ЄС право на доступ до власних даних прямо визнається статтею 15 ЗРЗПД, а також закріплене як елемент основного права на захист

546 Там само, стаття 23 (2).

547 Там само, стаття 89 (2) і (3).

548 Рішення ЄСПЛ у справах «Гаскін проти Сполученого Королівства» (*Gaskin v. the United Kingdom*), № 10454/83, від 07 липня 1989 р.; ЄСПЛ, «Одієвр проти Франції (*Odièvre v. France*) [ВП), № 42326/98, від 13 лютого 2003 р.; ЄСПЛ, «К. Г. та інші проти Словаччини» (*K.H. and Others v. Slovakia*), № 32881/04, від 28 квітня 2009 р.; ЄСПЛ, «Годеллі проти Італії» (*Godelli v. Italy*), № 33783/09, від 25 вересня 2012 р.

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

персональних даних у статті 8 (2) Хартії основних прав ЄС[550]. Право особи отримувати доступ до своїх власних персональних даних є ключовим елементом європейського законодавства про захист персональних даних[551].

ЗРЗПД передбачає, що кожен суб'єкт даних має право на доступ до своїх персональних даних та певної інформації щодо обробки, які мають надавати контролери[552]. Зокрема, кожен суб'єкт даних має право отримати (від контролера) підтвердження, чи обробляються дані, що стосуються його або її особисто, а також принаймні інформацію про наступне:

- мету обробки;
- категорії відповідних персональних даних;
- одержувачів чи категорії одержувачів персональних даних;
- запланований період зберігання даних, або, якщо це неможливо, критерії визначення такого періоду;
- наявність прав на виправлення або видалення персональних даних, на обмеження обробки персональних даних;
- право подавати скаргу до наглядового органу;
- будь-яку наявну інформацію про джерело персональних даних, що підлягають обробці, якщо вони були отримані не від суб'єкта даних;
- у разі прийняття автоматизованих рішень про логіку, що застосовується у процесі будь-якої автоматизованої обробки даних.

Контролер зобов'язаний надавати суб'єкту даних копії персональних даних, які обробляються. Будь-яка інформація, що передається суб'єкту даних, має надаватись у доступній для розуміння формі, тобто контролер має забезпечити, щоб суб'єкт даних міг зрозуміти інформацію, яка надається. Наприклад,

550 Див. також рішення Суду ЄС, об'єднані справи C-141/12 та C-372/12, «YS проти Міністра з питань імміграції, інтеграції та притулку» та «Міністр з питань імміграції, інтеграції та притулку проти M. та S.» (*YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S*), від 17 липня 2014 р.; ЄСПЛ, C-615/13 P, «ClientEarth, Мережа боротьби з пестицидами Європи проти Європейського агентства з безпечності харчових продуктів, Європейської Комісії» (*ClientEarth, Pesticide Action Network Europe (PAN Europe) v. European Food Safety Authority (EFSA), European Commission*), від 16 липня 2015 р.

551 Рішення Суду ЄС, об'єднані справи C-141/12 та C-372/12, «YS проти Міністра з питань імміграції, інтеграції та притулку» та «Міністр з питань імміграції, інтеграції та притулку проти M. та S.» (*YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S*), від 17 липня 2014 р.

552 Загальний регламент захисту персональних даних, стаття 15 (1).

зазначення технічних скорочень, кодованих термінів або абревіатур у відповіді на запит на доступ буде, як правило, недостатнім без роз'яснення значення цих термінів. У разі здійснення автоматизованого прийняття рішень, в тому числі профайлінгу, необхідно буде пояснити загальну логіку, що застосовується в автоматизованому процесі прийнятті рішень, а також критерії, які бралися до уваги в процесі оцінювання суб'єкта даних. Такі ж вимоги містяться **у праві РЄ**[553].

Приклад: доступ до своїх персональних даних допоможе суб'єкту даних визначити, чи є ці дані точними. Тому дуже важливо, щоб суб'єкт даних був поінформований у доступній для розуміння формі не лише про дійсні персональні дані, що обробляються, а й про категорії даних, за якими здійснюється їх обробка, таких як ім'я, IP-адреса, геолокаційні дані, номер кредитної картки та ін.

Інформація про джерело даних, якщо вони були отримані не від суб'єкта даних, повинна надаватись у відповідь на запит на надання доступу, якщо ця інформація наявна. Це положення слід розглядати в контексті принципів чесності, прозорості та підзвітності. Контролер не може знищити інформацію про джерело даних, щоб бути звільненим від необхідності розкривати її; якщо видалення мало місце, незважаючи на отримання запиту на надання доступу, він все одно має дотримуватись загальних вимог «підзвітності».

Як визначено в судовій практиці СЄС, право на доступ до персональних даних не може надмірно обмежуватись у часі. Суб'єкту даних має також бути надана достатня можливість отримати інформацію про операції обробки даних, що мали місце в минулому.

Приклад: у справі «*Рейкебура*»[554] СЄС мав визначити, чи може право фізичної особи на доступ до інформації про одержувачів чи категорій одержувачів персональних даних, а також про зміст даних, і чи може це право бути обмежене на строк до одного року до подання нею запиту на отримання доступу.

553 Див. Оновлену Конвенцію 108, стаття 8 (1) (c).

554 Рішення Суду ЄС, C-553/07, «Мер та члени міської ради Роттердама проти М.Е.Е. Рейкебура» (*College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer*), від 07 травня 2009 р.

Для того щоб визначити, чи дозволяє законодавство ЄС таке часове обмеження, Суд ЄС вирішив витлумачити статтю 12 у світлі цілей Директиви. Насамперед СЄС заявив, що право на доступ є необхідним для того, щоб суб'єкт даних мав можливість реалізувати право на виправлення контролером його даних, видалення чи блокування або повідомлення третіх осіб, яким були розкриті дані, про таке виправлення, видалення чи блокування. Ефективне право на доступ є також необхідним для забезпечення реалізації суб'єктом даних права на заперечення обробки його персональних даних або права подавати скаргу та вимагати відшкодування[555].

Для забезпечення практичного характеру прав, наданих суб'єкту даних, СЄС постановив, що «це право повинно неодмінно стосуватися минулого. В іншому випадку суб'єкт даних не міг би ефективно реалізовувати своє право на виправлення, видалення чи блокування персональних даних, що, як стверджується, неправомірно обробляються або неточні, або право ініціювати судовий розгляд та отримати відшкодування за завдану шкоду».

6.1.2 Право на виправлення

Відповідно до права ЄС та **РЄ** суб'єкти даних мають право на виправлення своїх персональних даних. Точність персональних даних дуже важлива для забезпечення захисту суб'єктів персональних даних[556].

Приклад: у справі «*Чуботару проти Молдови*»[557] заявник не зміг змінити в офіційних документах реєстраційний запис щодо свого етнічного походження з молдовського на румунське, як стверджувалося, через те, що він не обґрунтував свою вимогу. ЄСПЛ визнав прийнятним для держав вимагати об'єктивні докази під час реєстрації етнічної ідентичності особи. Якщо така заява була основана винятково на суб'єктивних і необґрунтованих підставах, органи влади могли відмовити в її виконанні. Однак вимога заявника була заснована більше ніж на суб'єктивному

555 Загальний регламент захисту персональних даних, стаття 15 (1) (c) та (f), 16, 17 (2) та 21, а також Розділ VIII.

556 Там само, стаття 16 та п. 65 преамбули; Оновлена Конвенція 108, стаття 9 (1) (e).

557 Рішення ЄСПЛ у справі «Чуботару проти Молдови» (*Ciubotaru v. Moldova*), № 27138/04, від 27 квітня 2010 р., пп. 51 та 59.

сприйнятті власної етнічної належності; він міг вказати на об'єктивно підтверджувані зв'язки з румунською етнічною групою, як-от мова, ім'я, співпереживання та інші. Проте відповідно до національного законодавства заявник був зобов'язаний надати докази того, що його батьки належали до румунської етнічної групи. З урахуванням історичних реалій Молдови така вимога створила непереборний бар'єр для реєстрації етнічної ідентичності, іншої, ніж та, яку було вказано при реєстрації його батьків за часів радянської влади. Перешкоджаючи в розгляді вимоги заявника з урахуванням доказів, які можуть бути об'єктивно підтверджені, держава не виконала свого позитивного зобов'язання щодо гарантування заявнику дійсної поваги до приватного життя. Суд вирішив, що мало місце порушення статті 8 ЄКПЛ.

В деяких випадках суб'єкту даних буде достатньо просто звернутися з вимогою виправити, наприклад, написання його імені, змінити його адресу або номер телефона. Відповідно до **права ЄС** та **РЄ** неточні персональні дані повинні бути виправлені без неправомірної або надмірної затримки[558]. Однак, якщо вимоги пов'язані з юридично важливими питаннями, наприклад, юридичною ідентифікацією суб'єкта даних або точною адресою його місця проживання для направлення йому юридичних документів, лише самих вимог щодо виправлення може бути недостатньо, і контролер може вимагати докази стверджуваної неточності. Такі вимоги контролерів не повинні покладати надмірний тягар на суб'єкта даних і тим самим позбавляти його можливості виправити свої дані. ЄСПЛ визнав порушення статті 8 ЄКПЛ у декількох справах, у яких заявник не зміг оскаржити неточність інформації, що зберігалась у таємних реєстрах[559].

Приклад: у справі *«Джемалеттін Джанлі проти Туреччини»*[560] ЄСПЛ встановив порушення статті 8 ЄКПЛ стосовно неточної звітності поліції в кримінальному провадженні.

Заявник двічі був учасником кримінальних проваджень через підозру в членстві в нелегальних організаціях, але не був засуджений. Коли

558 Загальний регламент захисту персональних даних, стаття 16; Оновлена Конвенція 108, стаття 9 (1).

559 Рішення ЄСПЛ у справі «Ротару проти Румунії» (*Rotaru v. Romania*) [ВП], № 28341/95, від 04 травня 2000 р.

560 Рішення ЄСПЛ у справі «Джемалеттін Джанлі проти Туреччини» (*Cemalettin Canli v. Turkey*), № 22427/04, від 18 листопада 2008 р., пп. 33 та 42–43; рішення ЄСПЛ у справі «Даля проти Франції» (*Dalea v. France*), № 964/07, від 2 січня 2010 р.

заявник був знову заарештований та звинувачений в іншому кримінальному правопорушенні, поліція подала на розгляд до кримінального суду звіт під назвою «Довідка щодо попередніх правопорушень», де заявник був зазначений як член двох нелегальних організацій. Подання заявником клопотання щодо внесення змін до звіту та досьє поліції було безрезультатним. ЄСПЛ постановив, що інформація, зазначена в довідці поліції, підпадала під дію статті 8 ЄКПЛ, оскільки публічна інформація, яка систематично збирається та зберігається в архівах органів влади, також може підпадати під поняття «приватне життя». Більше того, поліцейська довідка була неналежно складеною, і її подання до кримінального суду не відповідало національному законодавству. Суд дійшов висновку, що мало місце порушення статті 8.

Під час цивільного процесу або провадження державного органу щодо вирішення, чи є персональні дані правильними, суб'єкт даних може звернутися з проханням внести окремий запис або примітку у файл з його даними про те, що точність даних оскаржується і офіційне рішення ще не прийнято[561]. Протягом цього періоду контролер даних не повинен представляти дані як достовірні та остаточні, особливо третім особам.

6.1.3 Право на видалення даних («право бути забутим»)

Надання суб'єктам даних права на видалення їхніх персональних даних є надзвичайно важливим для ефективного застосування принципів захисту персональних даних, а особливо принципу мінімізації даних (персональні дані мають зводитися до того, що необхідно для досягнення мети обробки). У зв'язку з цим право на видалення даних міститься у правових документах як РЄ, так і ЄС[562].

Приклад: у справі *«Зегерштед-Віберг та інші проти Швеції»*[563] заявники були пов'язані з певними ліберальними та комуністичними політичними

561 Загальний регламент захисту персональних даних, стаття 16, друге речення статті 18 та п. 67 преамбули.

562 Там само, стаття 17.

563 Рішення ЄСПЛ у справі «Зегерштед-Віберг та інші проти Швеції» (*Segerstedt-Wiberg and Others v. Sweden*), № 62332/00, від 6 червня 2006 р., пп. 89 та 90; див. також, наприклад, рішення ЄСПЛ усправі «М. К. проти Франції» (*M.K. v. France*), № 19522/09, від 18 квітня 2013 р.

партіями. Вони підозрювали, що інформація про них була внесена до матеріалів служби безпеки та вимагали її видалити. ЄСПЛ впевнився в тому, що зберігання даних, про які йшла мова, мало юридичні підстави та переслідувало легітимну мету. Однак стосовно деяких заявників ЄСПЛ встановив, що тривале зберігання даних було непропорційним втручанням у їхнє право на приватне життя. Наприклад, щодо одного із заявників державні органи зберігали інформацію про те, що у 1969 році він нібито виступав за жорсткий опір контролю поліції під час демонстрацій. ЄСПЛ вирішив, що ця інформація не могла переслідувати жодного відповідного інтересу національної безпеки, особливо враховуючи її давній характер. Суд визнав порушення статті 8 ЄКПЛ стосовно чотирьох з п'яти заявників, оскільки з огляду на тривалий проміжок часу з моменту ствержуваних дій заявників продовжуване зберігання їх даних не було відповідним.

Приклад: у справі *«Брюне проти Франції»*[564] заявник піддав критиці зберігання його персональної інформації в базі даних поліції, яка містила відомості про засуджених, обвинувачених і жертв. Хоч кримінальне провадження проти нього було зупинено, інформація про нього з'явилась у базі даних. ЄСПЛ встановив, що мало місце порушення статті 8 ЄКПЛ. Приймаючи таке рішення, Суд вважав, що на практиці в заявника не було можливості видалити свої персональні дані з бази даних. ЄСПЛ також розглянув характер інформації, внесеної до бази даних, та визнав її такою, що втручається у приватне життя заявника, оскільки вона містить відомості про його ідентичність та особистість. Більше того, він вирішив, що термін зберігання персональних досьє в базі даних, який становив 20 років, був надмірно тривалим, тим більше, що жодним судом заявник ніколи не був засуджений.

Оновлена Конвенція 108 прямо визнає право фізичних осіб на видалення неточних, неправдивих або даних, які неправомірно обробляються[565].

У праві ЄС стаття 17 ЗРЗПД надає право суб'єктам даних вимагати видалення даних з можливістю відновлення або видалення без можливості відновлення. Право на видалення персональних даних без надмірної затримки виникає, якщо:

- немає більше потреби в персональних даних для досягнення мети, заради якої їх збирали чи іншим чином обробляли;

564 Рішення ЄСПЛ у справі «Брюне проти Франції» (*Brunet v. France*), № 21010/10, від 18 вересня 2014 р.

565 Оновлена Конвенція 108, стаття 9 (1) (e).

- суб'єкт даних відкликає згоду, на якій ґрунтується обробка, та відсутні інші законні підстави для обробки;
- суб'єкт даних заперечує проти обробки та немає жодних переважних правомірних підстав для обробки;
- персональні дані оброблялися незаконно;
- персональні дані необхідно видалити для дотримання юридичного зобов'язання, закріпленого в законодавстві ЄС або держави-члена, яке поширюється на контролера;
- персональні дані були зібрані в зв'язку з пропонуванням послуг інформаційного суспільства дітям відповідно до статті 8 ЗРЗПД[566].

Тягар доведення правомірності обробки покладається на контролерів даних, оскільки вони є відповідальними за законність обробки[567]. Відповідно до принципу підзвітності контролер має бути спроможним у будь-який час довести наявність обґрунтованої правової підстави для обробки ним даних, інакше обробку має бути припинено[568]. ЗРЗПД визначає винятки із права бути забутим, у тому числі у випадках, де обробка персональних даних необхідна:

- для реалізації права на свободу вираження поглядів та інформації;
- для дотримання встановленого законом зобов'язання, що вимагає обробку згідно з законодавством ЄС або держави-члена, яке поширюється на контролера, або для виконання завдання в суспільних інтересах або здійснення офіційних повноважень, покладених на контролера;
- на підставах публічного інтересу у сфері охорони здоров'я;
- для досягнення цілей у суспільних інтересах, цілей наукового чи історичного дослідження або статистичних цілей;
- для формування, здійснення чи захисту юридичних вимог[569].

СЄС підтвердив важливість права на видалення даних для забезпечення високого рівня захисту персональних даних.

566 Загальний регламент захисту персональних даних, стаття 17 (1).

567 Там само.

568 Там само, стаття 5 (2).

569 Там само, стаття 17 (3).

Приклад: у справі «*Google Spain*»[570] перед СЄС було порушено питання, чи потрібно компанії «Google» видалити з результатів пошуку застарілу інформацію щодо фінансових труднощів заявника. Серед іншого, компанія «Google» заперечувала свою відповідальність, стверджуючи, що вона лише надає гіперпосилання на вебсайт видавця, де розміщено інформацію, в цьому випадку газети, яка повідомляла про неплатоспроможність заявника[571]. «Google» стверджувала, що вимога щодо видалення застарілої інформації з вебсторінки має бути направлена до адміністратора вебсторінки, а не до «Google», яка лише надає посилання на сторінку-першоджерело. Суд ЄС дійшов висновку, що «Google» під час пошуку в мережі інформації та вебсторінок, а також індексування змісту для надання результатів пошуку, стає контролером даних, на якого покладаються відповідальність та зобов'язання відповідно до законодавства ЄС.

Суд ЄС роз'яснив, що пошукові системи інтернету та результати пошуку, що надають персональні дані, можуть створити детальний профіль фізичної особи[572]. Пошукові системи надають інформації, що знаходиться в переліку результатів пошуку, характеру повсюдності. Зважаючи на потенційну небезпечність, таке втручання не може бути виправдане лише економічним інтересом оператора відповідної системи в такій обробці. Необхідно досягти справедливого балансу, зокрема, між легітимним інтересом інтернет-користувачів у доступі до інформації та фундаментальними правами суб'єкта персональних даних, передбаченими статтею 7 та 8 Хартії основних прав ЄС. У суспільстві, яке все більше оцифровується, вимога, щоб персональні дані були точними та не виходили за межі необхідного (тобто публічної інформації), є фундаментальною для забезпечення фізичним особам високого рівня захисту персональних даних. «Стосовно такої обробки контролер у межах своїх обов'язків, повноважень та можливостей має забезпечити, щоб така обробка відповідала вимогам» законодавства ЄС таким

570 Рішення Суду ЄС, C-131/12, «"Google Spain SL", "Google Inc." проти Іспанського агентства захисту даних (AEPD) та Маріо Костеха Гонсалеса» (*Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC]), від 13 травня 2014 р, пп. 55–58.

571 Google також оскаржувала застосовність норм про захист персональних даних ЄС так, як корпорація «Google» заснована у США і обробка персональних даних, щодо яких йшла мова в цій справі, також здійснювалась у США. Другий аргумент щодо незастосовності законодавства про захист персональних даних ЄС пов'язаний із твердженням, що пошукові системи не можуть розглядатись як «контролери» щодо відомостей, відображених у їхніх результатах, оскільки вони не мають даних та не здійснюють контроль над ними. Суд ЄС відхилив обидва аргументи, вважаючи, що Директива 95/46/ЕС застосовна в цій справі, та продовжив досліджувати гарантовані нею обсягу прав, зокрема права на видалення персональних даних.

572 Там само, пп. 36, 38, 80–81 та 97.

чином, щоб встановлені правові гарантії були в повній мірі ефективними[573]. Це означає, що право на видалення власних персональних даних у випадку, якщо обробка застаріла або в ній немає більше потреби, також стосується контролерів, які відтворюють інформацію[574].

Вирішуючи питання, чи необхідно було «Google» видалити посилання, які стосувалися заявника, СЄС вважав, що за певних обставин фізична особа має право вимагати видалити персональні дані. Це право може бути використане у випадку, якщо інформація стосовно фізичної особи неточна, неадекватна, не відповідна або надмірна щодо цілей обробки персональних даних. Суд ЄС визнав, що це право не є абсолютним; має бути встановлено баланс між ним та іншими правами та інтересами, зокрема з інтересом громадськості щодо доступу до певної інформації. Кожна вимога видалення даних має підлягати оцінці в кожному окремому випадку шляхом встановлення балансу між основоположними правами на захист персональних даних і приватного життя суб'єкта даних, з одного боку, та легітимними інтересами всіх інтернет-користувачів, в тому числі видавців, – з іншого. СЄС надав вказівки щодо факторів, які мають бути враховані під час знаходження такого балансу. Характер відповідної інформації є особливо важливим фактором. Якщо інформація стосується приватного життя фізичної особи, при цьому суспільний інтерес до неї відсутній, захист персональних даних і приватне життя переважатиме над правом громадськості на доступ до інформації. І, навпаки, якщо виявиться, що суб'єкт даних є публічною особою або характер запитуваної інформації виправдовує її доступність для широкої громадськості, переважний суспільний інтерес щодо доступу до інформації може виправдати втручання в основні права на захист персональних даних та приватне життя суб'єкта даних.

573 Там само, пп. 81–83.

574 Суд ЄС, C-131/12, «"Google Spain SL", "Google Inc." проти Іспанського агентства захисту даних (AEPD) та Маріо Костеха Гонсалеса» (*Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC]), від 13 травня 2014 р., п. 88. Див. також Рекомендації Робочої групи «Стаття 29» щодо виконання рішення Суду ЄС «"Google Spain SL", "Google Inc." проти Іспанського агентства із захисту даних (ІАЗД), Маріо Костея Гонсалеса [GC]» (*Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*), (2014), РГ 225, Брюссель, від 26 листопада 2014 р. та Рекомендація Комітету міністрів Ради Європи CM/Rec 2012(3) про захист прав людини у зв'язку з використанням пошукових систем, від 04 квітня 2012 р.

Після ухвалення рішення Робоча група «Стаття 29» затвердила рекомендації щодо виконання постанови Суду ЄС[575]. Рекомендації включають перелік загальних критеріїв для використання контролюючими органами під час розгляду скарг, пов'язаних із вимогами суб'єктів даних на видалення, з поясненнями наслідків права на видалення та порядку знаходження балансу між правами. У рекомендаціях знову наголошується, що оцінка має здійснюватися в кожному окремому випадку. Оскільки право бути забутим не є абсолютним, результат розгляду вимоги може відрізнятися залежно від конкретних обставин. Це також можна побачити у практиці Суду ЄС після розгляду справи «Google».

Приклад: у справі *«Торгово-промислова та сільськогосподарська палата м. Лечче проти Сальваторе Манні»*[576] Суд ЄС мав розглянути питання, чи має фізична особа право на видалення своїх персональних даних, опублікованих у Державному реєстрі компаній, якщо її компанія припинила існування. Пан Манні звернувся до Торгово-промислової палати м. Лечче з проханням видалити його персональні дані з вказаного реєстру після того, як виявив, що потенційні клієнти можуть звернутися по довідкову інформацію до реєстру та дізнатися, що він керував компанією, яка була оголошена банкрутом понад 10 років тому. Заявник вважав, що така інформація буде відлякувати потенційних клієнтів.

Під час балансування права пана Манні на захист його персональних даних і суспільного інтересу в доступі до відповідної інформації Суд ЄС спочатку дослідив мету існування публічного реєстру. Він вказав на той факт, що розкриття здійснювалося на підставі закону, зокрема Директиви ЄС, яка має на меті зробити інформацію про компанії більш доступною для третіх осіб. Таким чином, треті особи повинні мати доступ і можливість вивчати установчі документи компанії та іншу інформацію стосовно неї, а «особливо щодо осіб, які мають повноваження створювати для компанії зобов'язання». Метою розкриття інформації також було забезпечення юридичної визначеності у зв'язку з розширенням торгівлі між державами-членами шляхом надання третім особам доступу до всієї відповідної інформації про компанії на всій території ЄС. Крім того, Суд ЄС зазначив, що навіть з плином часу або

575 Робоча група «Стаття 29» (2014), *Рекомендації щодо виконання рішення Суду ЄС «"Google Spain SL", "Google Inc". проти Іспанського агентства захисту даних (AEPD) та Маріо Костеха Гонсалеса» C-131/12*, РГ 225, Брюссель, від 26 листопада 2014 р.

576 Рішення Суду ЄС, C-398/15, «Торгово-промислова та сільськогосподарська палата м. Лечче проти Сальваторе Манні» (*Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*), від 09 травня 2017 р.

після ліквідації компанії права та юридичні обов'язки, які стосуються компанії, часто продовжують існувати. Спори, пов'язані з ліквідацією, можуть бути тривалими, і питання стосовно компанії, її керівників та ліквідаторів можуть виникати протягом багатьох років після припинення її існування. Суд ЄС постановив, що з огляду на широке коло можливих варіантів та відмінностей строків позовної давності, встановлених кожною державою-членом, «вбачається, що наразі неможливо встановити єдиний проміжок часу, починаючи з моменту ліквідації компанії, після закінчення якого включення таких даних до реєстру та їх розкриття не буде вже необхідним». З огляду на легітимну мету розкриття даних та складнощі в установленні періоду, по закінченні якого персональні дані можуть бути видалені з реєстру без заподіяння шкоди інтересам третіх осіб, Суд ЄС визнав, що норми захисту персональних даних ЄС не гарантують права на видалення персональних даних особам у випадках, аналогічних до ситуації пана Манні.

У разі, якщо контролер опублікував персональні дані, і до нього звернулися з вимогою видалити інформацію, такий контролер даних зобов'язаний та має вжити «розумних» заходів для інформування інших контролерів, які обробляють ті самі персональні дані, про вимогу суб'єкта даних видалити інформацію щодо нього. Дії контролера мають враховувати наявні технології та витрати на їх реалізацію[577].

6.1.4 Право на обмеження обробки

Стаття 18 ЗРЗПД надає суб'єктам даних право тимчасово обмежити обробку контролером їхніх персональних даних. Суб'єкти даних можуть вимагати в контролера обмежити обробку у випадках, якщо:

- оскаржується точність персональних даних;
- обробка даних є неправомірною і суб'єкт даних вимагає обмеження використання його персональних даних замість видалення;
- персональні дані мають зберігатися для здійснення чи захисту юридичних вимог;
- триває процес прийняття рішення щодо того, чи переважають легітимні інтереси контролера даних над інтересами суб'єкта даних[578].

577 Загальний регламент захисту персональних даних, стаття 17 (2) та п. 66 преамбули.

578 Там само, стаття 18 (1).

Способи обмеження обробки персональних даних можуть включати, наприклад, тимчасове перенесення обраних даних до іншої системи обробки, що робить їх недоступними для користувачів, або тимчасове вилучення персональних даних[579]. Контролер повинен сповістити суб'єкта даних про зняття обмеження на обробку до моменту такого зняття[580].

Обов'язок інформувати щодо виправлення чи видалення персональних даних або обмеження обробки

Контролер повинен повідомляти про будь-яке виправлення чи видалення персональних даних або обмеження обробки кожного одержувача, якому контролер розкрив персональні дані, якщо це не є неможливим та диспропорційним[581]. Контролер має надати на вимогу суб'єкта даних інформацію про таких одержувачів[582].

6.1.5 Право на мобільність даних

Відповідно до ЗРЗПД суб'єкти даних мають право на мобільність даних у випадках, якщо надані ними контролеру персональні дані обробляються автоматизованими засобами на підставі згоди, або якщо обробка є автоматизованою та необхідна для виконання умов договору. Це означає, що право на мобільність даних не може застосовуватись у випадках, якщо обробка персональних даних ґрунтується на іншій, ніж згода чи угода, правовій підставі[583].

Якщо право на мобільність даних застосовне, суб'єкти даних мають право на передання своїх даних безпосередньо від одного контролера до іншого за наявності технічної можливості[584]. Для сприяння цьому контролер має створити технічно сумісні формати, які роблять дані мобільними[585]. ЗРЗПД уточнює, що такі формати мають бути структурованими, широко використовуваними та придатними для машинного читання, що полегшує сумісність[586]. Сумісність у

579 Там само, п. 67 преамбули.

580 Там само, стаття 18 (3).

581 Спеціальний комітет з питань захисту персональних даних (CAHDATA), Пояснювальна записка до Оновленої Конвенції про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних, п. 79; там само, стаття 19.

582 Там само.

583 Там само, п. 68 преамбули та стаття 20 (1).

584 Там само, стаття 20 (2).

585 Там само, п. 68 преамбули та стаття 20 (1).

586 Там само, п. 68 преамбули.

широкому розумінні може бути визначена як здатність інформаційних систем обмінюватися даними та ділитися інформацією[587]. В той час, як метою використання форматів визначено досягнення сумісності даних, ЗРЗПД не містить особливих рекомендацій щодо конкретних форматів, які мають встановлюватися: вони можуть відрізнятись у різних секторах[588].

Відповідно до рекомендацій Робочої групи «Стаття 29» право на мобільність даних «підтримує вибір користувача, контроль користувача та розширення прав та можливостей користувача» з метою надання суб'єктам даних контролю над власними персональними даними[589]. Рекомендації роз'яснюють основні складові мобільності даних, до яких належать:

- право суб'єкта даних на отримання своїх персональних даних, оброблених контролером, у структурованому, широко використовуваному, машинночитаному та сумісному форматі;
- право на передачу персональних даних від одного контролера даних до іншого без перешкод, якщо це технічно можливо;
- режим контрольованості – коли контролер задовольняє вимогу надання мобільних даних, він діє за вказівками суб'єкта даних; це означає, що він не несе відповідальності за дотримання одержувачем законодавства про захист персональних даних, оскільки саме суб'єкт даних вирішує, кому передаються дані;
- реалізація права на мобільність даних здійснюється без шкоди для будь-яких інших прав, як і стосовно інших передбачених ЗРЗПД прав.

6.1.6 Право на заперечення

Суб'єкти даних можуть скористатися своїм правом на заперечення проти обробки персональних даних з підстав, пов'язаних з їхньою особистою ситуацією, та проти обробки з метою прямого маркетингу. Право на заперечення може бути реалізоване автоматизованими засобами.

587 Європейська Комісія, Комюніке щодо більш сильних та інтелектуалізованих інформаційних систем для кордонів та безпеки, COM(2016) 205 остаточне, від 02 квітня 2016 р.

588 Робоча група «Стаття 29» (2016), Рекомендації щодо права на мобільність даних, РГ 242, від 13 грудня 2016 р., зі змінами від 05 квітня 2017 р., п. 13.

589 Там само.

Право на заперечення з підстав, пов'язаних з особистою ситуацією суб'єкта даних

Загального права суб'єктів даних на заперечення проти обробки своїх даних не існує[590]. Стаття 21 (1) ЗРЗПД наділяє суб'єкта персональних даних правом висувати заперечення на підставах, пов'язаних з його особистою ситуацією, у випадках, коли юридичною підставою обробки є виконання контролером завдань у суспільних інтересах, або обробка здійснюється в легітимних інтересах контролера[591]. Право на заперечення поширюється на діяльність з профайлінгу. Подібне право було визнано Оновленою Конвенцією 108[592].

Право на заперечення на підставах, пов'язаних з особистою ситуацією суб'єкта даних, спрямоване на досягнення правильного балансу між правами суб'єкта на захист персональних даних і легітимними правами інших стосовно обробки його даних. Втім, СЄС роз'яснив, що права суб'єкта даних переважають «за загальним правилом» над економічними інтересами контролера даних залежно від «характеру інформації, про яку йдеться, та її чутливості для приватного життя суб'єкта даних, а також інтересу громадськості в доступі до такої інформації»[593]. Відповідно до ЗРЗПД тягар доведення покладено на контролерів, які зобов'язані навести вагомі підстави для продовження обробки[594]. Так само в Пояснювальній записці до Оновленої Конвенції 108 уточнюється, що законні підстави для обробки даних (які можуть подолати право суб'єкта даних на заперечення) мають бути доведені в кожному випадку окремо[595].

590 Див. також рішення ЄСПЛ у справі «М. С. проти Швеції» (*M.S. v. Sweden*), № 20837/92, від 27 серпня 1997 (у якій медичні дані було повідомлено без згоди чи можливості висунути заперечення); рішення ЄСПЛ у справі «Леандер проти Швеції» (*Leander v. Sweden*), № 9248/81, від 26 березня 1987 р.; рішення ЄСПЛ у справі «Мослі проти Сполученого Королівства» (*Mosley v. the United Kingdom*), № 48009/08, від 10 травня 2011 р.

591 Загальний регламент захисту персональних даних, п. 69 преамбули; стаття 6 (1) (e) та (f).

592 Оновлена Конвенція 108, стаття 9 (1) (d); Рекомендації щодо профайлінгу, стаття 5 (3).

593 Рішення Суду ЄС , C-131/12, «"Google Spain SL", "Google Inc." проти Іспанського агентства захисту даних (AEPD) та Маріо Костеха Гонсалеса» (*Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC]), від 13 травня 2014 р. п. 81.

594 Див. також Оновлену Конвенцію 108, стаття 9 (1) (d), у якій зазначається, що суб'єкт даних має право на заперечення проти обробки його даних «крім випадків, коли контролер продемонструє легітимні підстави для обробки, які переважають його або її інтереси або права і основоположні свободи».

595 Пояснювальна записка до Оновленої Конвенції 108, п. 78.

Приклад: у справі «*Манні*»[596] СЄС вирішив, що з огляду на легітимну мету розкриття персональних даних у реєстрі компаній, зокрема, необхідність захищати інтереси третіх осіб і забезпечувати юридичну визначеність, в принципі, пан Манні не мав права на видалення його персональних даних з відповідного реєстру. Втім Суд визнав існування права на заперечення проти обробки, зазначивши, що «не може бути виключено [...] існування окремих ситуацій, у яких переважні та правомірні підстави, пов'язані з окремою ситуацією відповідної особи, винятково виправдовують те, що доступ до персональних даних, внесених до реєстру, обмежується після закінчення достатньо тривалого періоду часу [...] для третіх осіб, які можуть виявити інтерес до ознайомлення з ними».

СЄС вважав, що обов'язком національних судів є надання належної оцінки кожному конкретному випадку, з урахуванням усіх відповідних обставин фізичної особи та існування легітимних і переважних підстав, які можуть винятково виправдати обмеження доступу третім особам до персональних даних, що містяться в реєстрах компаній. Однак Суд уточнив, що у випадку пана Манні сам лише факт твердження про негативний вплив розкриття його персональних даних на клієнтуру не може вважатися правомірною та переважною підставою. Потенційні клієнти пана Манні мають легітимний інтерес в отриманні доступу до інформації про банкрутство його колишньої компанії.

В результаті здійснення успішного заперечення контролер більше не може обробляти відповідні дані. Однак операції обробки, які були здійснені до висунення заперечення, залишаються правомірними.

Право на заперечення проти обробки персональних даних з метою прямого маркетингу

Стаття 21 (2) ЗРЗПД передбачає окреме право на заперечення проти використання персональних даних з метою прямого маркетингу, вносячи додаткові роз'яснення до статті 13 Директиви про конфіденційність та електронні комунікації. Таке право також закріплено в Оновленій Конвенції 108, а також

596 Рішення Суду ЄС, C-398/15, «Торгово-промислова та сільськогосподарська палата м. Лечче проти Сальваторе Манні» (*Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*), від 09 березня 2017, пп 47 та 60.

рекомендаціях РЄ щодо прямого маркетингу[597]. У Пояснювальній записці до Оновленої Конвенції 108 роз'яснено, що заперечення проти обробки персональних даних з метою прямого маркетингу мають призвести до безумовного видалення або вилучення таких даних[598].

Суб'єкт даних має право заперечувати проти використання його персональних даних з метою прямого маркетингу в будь-який час та безоплатно. Інформація про таке право має бути надана йому в зрозумілій формі окремо від будь-якої іншої інформації.

Право на заперечення автоматизованими засобами

Якщо особиста інформація використовується та обробляється для послуг інформаційного суспільства, суб'єкт даних може скористатися правом на заперечення проти обробки своїх персональних даних за допомогою автоматизованих засобів.

Послуги інформаційного суспільства – це будь-яка послуга, яка зазвичай надається за винагороду, дистанційно, електронними засобами та за індивідуальним запитом отримувача послуг[599].

Контролери даних, які пропонують послуги інформаційного суспільства, повинні мати в наявності належні технічні механізми та процедури для забезпечення ефективної реалізації права на заперечення за допомогою автоматизованих засобів[600]. Наприклад, до них може належати блокування файлів cookies на вебсторінці або вимкнення відстеження вебперегляду.

Право на заперечення в цілях наукового чи історичного дослідження або статистичних цілях

Відповідно до законодавства ЄС наукове дослідження необхідно тлумачити в широкому сенсі, включно з, наприклад, технологічними розробками і демонстраціями, фундаментальними дослідженнями, прикладними

597 Рада Європи, Комітет міністрів (1985), Рекомендація Rec(85)20 державам-членам про захист персональних даних, які використовуються з метою прямого маркетингу, від 25 жовтня 1985, стаття 4 (1).

598 Пояснювальна записка до Оновленої Конвенції 108, п. 79.

599 Директива 98/34/ЄС із змінами, внесеними Директивою 98/48/ЄС «Про встановлення порядку надання інформації у сфері технічних стандартів та регламентів», стаття 1 (2).

600 Загальний регламент захисту персональних даних, стаття 21 (5).

дослідженнями і дослідженнями за фінансової підтримки з боку приватного сектору[601]. Історичне дослідження також включає дослідження для генеалогічних цілей, зважаючи на те, що регламент не повинен застосовуватися до померлих осіб[602]. Під статистичними цілями розуміється будь-яка операція щодо збирання та обробки персональних даних, необхідних для статистичних опитувань або для підготовки статистичних результатів[603]. Знову ж таки, індивідуальна ситуація суб'єкта даних є юридичною підставою для права на заперечення проти обробки персональних даних в інтересах дослідження[604]. Єдиним винятком є необхідність обробки даних для виконання завдань у суспільних інтересах. Однак право на видалення не має застосовуватись, якщо обробка необхідна (з наявністю суспільного інтересу або без нього) для цілей наукового чи історичного дослідження або статистичних цілей[605].

ЗРЗПД врівноважує потреби наукового, статистичного чи історичного дослідження та права суб'єктів даних, вказуючи на певні гарантії та відступи в статті 89. Таким чином, законодавство ЄС або держави-члена може передбачати обмеження права на заперечення, якщо таке право може зробити неможливим чи серйозно зменшити досягнення цілей дослідження, і таке звуження є необхідним для повного досягнення цих цілей.

Відповідно до **права РЄ**, стаття 9 (2) Оновленої Конвенції 108 встановлює, що обмеження прав суб'єктів даних, в тому числі права на заперечення, може бути передбачено законодавством стосовно обробки даних у цілях архівування в суспільних інтересах, цілях наукового чи історичного дослідження або статистичних цілях, якщо відсутній ризик порушення прав та основоположних свобод суб'єктів даних.

Втім у Пояснювальній записці (пункт 41) також визнається, що суб'єкти даних повинні мати можливість надати свою згоду лише на визначені напрямки дослідження або частини науково-дослідних проєктів в обсягах, дозволених запланованою метою, та заперечувати у випадку, якщо вони вбачають, що обробка здійснюється з надмірним втручанням у їхні права та свободи без правомірної підстави.

601 Там само, п. 159 преамбули.

602 Там сао, п. 160 преамбули.

603 Там само, п. 162 преамбули.

604 Там само, стаття 21 (6).

605 Там само, стаття 17 (3) (d).

Інакше кажучи, така обробка вважатиметься *a priori* сумісною за умови, що існують інші гарантії, і що операції в принципі виключають будь-яке використання отриманої інформації для рішень чи заходів стосовно конкретної особи.

6.1.7 Автоматизоване прийняття рішень, в тому числі профайлінг

Автоматизованими рішеннями є рішення, прийняті з використанням персональних даних, оброблених виключно автоматизованими засобами без будь-якого втручання людини. Відповідно **до права ЄС**, суб'єкти даних не мають підлягати автоматизованим рішенням, які приводять до правових чи інших істотних наслідків. Якщо такі рішення можуть мати істотний вплив на життя фізичних осіб, оскільки вони стосуються, наприклад, кредитоспроможності, електронного підбору персоналу, продуктивності на роботі або аналізу поведінки чи надійності, для уникнення негативних наслідків необхідний спеціальний захист. Автоматизоване прийняття рішень включає профайлінг, який складається з будь-яких форм автоматизованого оцінювання «особистих аспектів, що стосуються фізичної особи, зокрема для аналізу або передбачення аспектів стосовно продуктивності суб'єкта даних на роботі, економічної ситуації, здоров'я, особистих уподобань чи інтересів, надійності чи поведінки, місця знаходження чи пересування»[606].

Приклад: для швидкої оцінки кредитоспроможності майбутнього клієнта, кредитні довідкові агенції (CRAs) збирають певні дані, наприклад, як клієнт вів свої кредитні та сервісні/комунальні рахунки, деталі щодо попередніх адрес клієнта, а також інформацію з відкритих джерел, як-от реєстр виборців, офіційна документація (в тому числі судові рішення) або відомості щодо банкрутства чи неплатоспроможності. Ці дані надалі вносяться до алгоритму оцінювання, який обчислює загальне значення, що дає уявлення про кредитоспроможність потенційного клієнта.

Як зазначається Робочою групою «Стаття 29», право не бути суб'єктом рішень, які ґрунтуються виключно на автоматизованій обробці та можуть спричинити правові наслідки для суб'єкта даних чи істотно вплинути на нього чи неї,

606 Там само, п. 71, стаття 4 (4) та стаття 22.

прирівнюється до загальної заборони і не вимагають, щоб суб'єкт даних заздалегідь звертався із запереченням проти такого рішення[607].

Однак, відповідно до ЗРЗПД, автоматизоване прийняття рішень з юридичними наслідками або таке, що істотно впливає на фізичних осіб, може бути прийнятним, якщо це необхідно для укладення чи виконання контракту між контролером і суб'єктом даних, або якщо суб'єкт даних надав явну згоду. Також автоматизоване прийняття рішень прийнятне, якщо воно дозволене законодавством, і права, свободи та легітимні інтереси суб'єкта даних належним чином захищені[608].

ЗРЗПД також передбачає, що серед обов'язків контролера щодо надання інформації у випадку збирання персональних даних є інформування суб'єкта даних про наявність автоматизованого прийняття рішень, в тому числі профайлінгу[609]. Право на доступ до персональних даних, що обробляються контролером, залишається незмінним[610]. Інформація має не лише вказувати на те, що буде здійснюватися профайлінг, а й включати змістовну інформацію про логіку, що застосовується в профайлінгу, та передбачувані наслідки такої обробки для фізичних осіб[611]. Наприклад, медична страхова компанія, яка використовує автоматизоване прийняття рішень щодо заяв, має надавати суб'єктам даних загальну інформацію про те, як діє алгоритм та які фактори ним використовуються для підрахунку їхніх страхових премій. Так само, реалізуючи своє «право на доступ», суб'єкти даних можуть звернутися до контролера з вимогою надати інформацію про наявність автоматизованого прийняття рішень або змістовну інформацію про логіку, що застосовується[612].

Інформування суб'єктів даних покликане забезпечити прозорість і надати можливість таким суб'єктам дати поінформовану згоду, якщо це потрібно, або домогтися втручання людини. Контролер повинен вжити належних заходів для гарантування охорони прав, свобод та легітимних інтересів суб'єктів даних, до яких щонайменше належить право на людське втручання з боку

607 Робоча група «Стаття 29», Рекомендації щодо автоматизованого прийняття рішень та профайлінгу для цілей Регламенту 2016/679, РГ 251, від 03 жовтня 2017р., п. 15.

608 Загальний регламент захисту персональних даних, стаття 22 (2).

609 Там само, стаття 12.

610 Там само, стаття 15.

611 Там само, стаття 13 (2) (f).

612 Там само, стаття 15 (1) (h).

контролера, можливість висловлювати свою думку та оскаржувати рішення, які ґрунтуються на автоматизованій обробці даних таких суб'єктів[613].

Робоча група «Стаття 29» надала додаткові вказівки щодо використання автоматизованого прийняття рішень у рамках ЗРЗПД[614].

Відповідно до права РЄ фізичні особи мають право не бути суб'єктами рішень, які можуть істотно вплинути на них і проводяться виключно на основі автоматизованої обробки, без врахування їхньої думки[615]. Вимога щодо врахування думки суб'єктів даних у випадку, якщо рішення ґрунтуються виключно на автоматизованій обробці, означає, що вони мають право оскаржувати такі рішення, а також мають бути в змозі оскаржити будь-яку неточність у своїх персональних даних, використаних контролером, а також ставити під сумнів доцільність застосованого профілю[616]. Однак фізична особа не може реалізувати це право, якщо автоматизоване рішення передбачене законом, що поширюється на контролера, а також передбачає належні заходи для захисту прав, свобод та легітимних інтересів суб'єкта даних. Більше того, суб'єкти даних мають право на вимогу отримувати обґрунтування підстав обробки, що здійснюється[617]. У Пояснювальній записці до Оновленої Конвенції 108 наведено приклад нарахування кредитних балів. Фізичні особи повинні мати право знати не лише про позитивне чи негативне рішення щодо нарахування кредитних балів, але й *логіку* обробки їхніх даних, за результатами якої було прийнято таке рішення. «Розуміння цих елементів сприяє ефективній реалізації інших дуже важливих гарантій, як-от права на заперечення та права на подання скарги до компетентного органу»[618].

Рекомендація з профайлінгу, хоч і не обов'язкова до виконання, встановлює умови для збирання та обробки персональних даних у контексті профайлінгу[619]. Вони включають положення про необхідність забезпечення того, щоб обробка в контексті профайлінгу була чесною, законною, пропорційної та здійснювалася для визначених і легітимних цілей. Там також містяться

613 Там само, стаття 22 (3).

614 Робоча група «Стаття 29», *Рекомендації щодо автоматизованого прийняття рішень та профайлінгу для цілей Регламенту 2016/679*, РГ 251, від 03 жовтня 2017р.

615 Оновлена Конвенція 108, стаття 9 (1) (a).

616 Пояснювальна записка до Оновленої Конвенції 108, п. 75.

617 Оновлена Конвенція 108, стаття 9 (1) (c).

618 Пояснювальна записка до Оновленої Конвенції 108, п. 77.

619 Рада Європи, *Рекомендація CM/Rec(2010)13* Комітету міністрів державам-членам щодо захисту фізичних осіб відносно обробки персональних даних у контексті профайлінгу, стаття 5 (5).

положення щодо інформації, яку контролери мають надавати суб'єктам даних. Крім того, у Рекомендації наводиться принцип якості даних, який вимагає від контролера вживати заходів для виправлення факторів, що призводять до неточності даних, зменшувати ризики чи помилки, які може спричинити профайлінг, а також через певні проміжки часу здійснювати оцінку якості даних та алгоритмів, що використовуються.

6.2 Засоби юридичного захисту, відповідальність, штрафи та відшкодування

Ключові моменти

- Відповідно до Оновленої Конвенції 108 національне законодавство Договірних Сторін повинно забезпечувати належні засоби юридичного захисту та санкції за порушення права на захист персональних даних.
- У праві ЄС ЗРЗПД передбачає засоби захисту для суб'єктів даних у випадку порушення їхніх прав, так само як санкції щодо контролерів та операторів, які не дотримуються вимог Регламенту. Він також передбачає право на відшкодування та відповідальність.
  - Суб'єкт даних має право подавати скаргу до контролюючого органу щодо ймовірних порушень Регламенту, а також право на ефективний судовий засіб захисту та отримання відшкодування.
  - Під час реалізації права на ефективний засіб юридичного захисту фізичні особи можуть бути представлені неприбутковими організаціями, які здійснюють діяльність у сфері захисту персональних даних.
  - Контролер та оператор несе відповідальність за будь-яку матеріальну та нематеріальну шкоду, заподіяну внаслідок порушення.
  - Контролюючі органи мають повноваження накладати адміністративні штрафи за порушення Регламенту в розмірі до 20 млн євро, а у випадку підприємства – до 4 % загального річного світового обігу підприємства, залежно від того, яка сума є вищою.
- За певних умов суб'єкти даних можуть звертатися до ЄСПЛ як до останньої інстанції щодо порушень законодавства про захист персональних даних.
- Будь-яка фізична чи юридична особа має право подати позов про скасування будь-яких рішень Європейської Ради з питань захисту персональних даних до Суду ЄС за умов, передбачених Договорами.

Ухвалення правових інструментів недостатньо для забезпечення захисту персональних даних у межах Європи. Для досягнення ефективності європейських правил щодо захисту персональних даних необхідно запровадити механізми, які нададуть можливість фізичним особам протистояти порушенням своїх прав та вимагати компенсації шкоди. Також важливо, щоб наглядові органи мали повноваження накладати санкції, які є ефективними, стримувальними та пропорційними до відповідних порушень.

Права, передбачені законодавством про захист персональних даних, можуть здійснюватися особою, права якої знаходяться під загрозою, тобто особою, що є суб'єктом персональних даних. Однак інші особи, які відповідають вимогам національного законодавства, також можуть представляти суб'єктів даних у реалізації їхніх прав. Відповідно до низки національних законів, дітей та осіб з порушеннями інтелектуального розвитку повинні представляти їхні опікуни[620]. Відповідно до права ЄС про захист персональних даних, суб'єктів даних у контролюючому органі або суді може також представляти об'єднання, легітимна мета якого полягає в підтримці прав на захист персональних даних[621].

6.2.1 Право на подання скарги до контролюючого органу

Відповідно до **права РЄ** та **ЄС,** фізичні особи мають право на подання запитів та скарг до компетентного контролюючого органу, якщо вони вважають, що обробка їхніх персональних даних здійснюються не у відповідності із законодавством.

Оновлена Конвенція 108 визнає право суб'єктів даних користуватися допомогою контролюючого органу в реалізації своїх прав незалежно від їхнього громадянства чи місця проживання[622]. Запит на допомогу може бути відхилений у виняткових випадках, а суб'єкти даних не повинні відшкодовувати витрати та збори, пов'язані з наданням допомоги[623].

Подібні положення містяться у правовій системі ЄС. ЗРЗПД вимагає, щоб контролюючі органи вживали заходів з метою полегшення подання скарги,

620 FRA (2015), *Посібник з європейського права щодо прав дитини*, Люксембург, Управління публікацій; FRA (2013), *Правоздатність осіб з порушенням інтелектуального розвитку та осіб з проблемами психічного здоров'я* , Люксембург, Управління публікацій.

621 Загальний регламент захисту персональних даних, стаття 80.

622 Оновлена Конвеція 108, стаття 18.

623 Там само, стаття 16–17.

наприклад створення електронної форми подання скарги[624]. Суб'єкт даних може подати скаргу до контролюючого органу в державі-члені за місцем його постійного проживання, місця роботи чи місця вчинення ймовірного порушення[625]. Скарги мають бути розслідувані, а відповідну особу поінформовано контролюючим органом про результати провадження за заявою[626].

Можливі порушення інституціями чи органами ЄС можуть бути доведені до відома Європейського інспектора із захисту даних (ЄІЗПД)[627]. У разі відсутності відповіді від ЄІЗПД протягом шести місяців скарга вважається відхиленою. Скарги на рішення ЄІЗПД можна подати до Суду ЄС у рамках Регламенту (ЄС) № 45/2001, що покладає на інституції та органи ЄС обов'язок дотримуватися правил захисту персональних даних.

Повинна існувати можливість звернення до суду для оскарження рішень національного контролюючого органу. Це стосується суб'єкта персональних даних, а також контролерів та операторів, які були стороною у провадженні наглядового органу.

Приклад: у вересні 2017 року Державний орган захисту персональних даних Іспанії наклав штраф на «Facebook» за порушення декількох нормативних актів щодо захисту персональних даних. Контролюючий орган звинуватив соціальну мережу у зборі, зберіганні та обробці персональних даних, в тому числі спеціальних категорій персональних даних, з метою реклами та без отримання згоди суб'єктів даних. Рішення ґрунтувалося на розслідуванні, проведеному з ініціативи контролюючого органу.

6.2.2 Право на ефективний засіб судового захисту

Окрім права подати скаргу до контролюючого органу фізичні особи повинні мати право на ефективний засіб судового захисту та на подання позову до суду. Право на засіб правового захисту закріплене в європейській правовій

624 Загальний регламент захисту персональних даних, стаття 57 (2).

625 Там само, стаття 77 (1).

626 Там само, стаття 77 (2).

627 Регламент Європейського Парламенту і Ради (ЄС) № 45/2001 від 18 грудня 2000 р. про захист фізичних осіб у зв'язку з обробкою персональних даних інституціями та органами Співдружності і про вільне переміщення таких даних, OJ 2001 L 8.

традиції та визнається як фундаментальне, як статтею 47 Хартії основних прав ЄС, так і статтею 13 ЄКПЛ[628].

В праві ЄС важлива роль надання ефективних засобів юридичного захисту суб'єктам даних у випадку порушення їхніх прав підкреслюється положеннями ЗРЗПД, які встановлюють право на ефективний засіб судового захисту проти контролюючих органів, контролерів та операторів, а також практикою Суду ЄС.

Приклад: у справі «*Шремса*»[629] Суд ЄС визнав рішення про відповідність «Безпечної гавані» недійсним. Це рішення надавало дозвіл на транскордонну передачу даних з ЄС до організацій у США, які отримали сертифікати за схемою «Безпечна гавань». Суд ЄС вирішив, що у схеми «Безпечна гавань» є декілька недоліків, які несуть загрозу для основоположних прав громадян ЄС на захист приватності, захист персональних даних і права на ефективний юридичний захист.

Стосовно порушення прав на приватність та захист персональних даних Суд ЄС підкреслив, що законодавство США дозволяє певним державним органам отримувати доступ до персональних даних, переданих державами-членами до США, та обробляти їх у спосіб, несумісний з початковою метою передачі та виходячи за межі того, що є вкрай необхідним та пропорційним для захисту національної безпеки. Щодо права на ефективний засіб захисту прав Суд зазначив, що суб'єкти даних не мали адміністративних чи судових засобів юридичного захисту для уможливлення доступу до даних, які їх стосувалися, виправлення чи видалення таких даних залежно від обставин. Суд ЄС дійшов висновку, що законодавство, яке не передбачає можливості застосування засобів юридичного захисту для доступу, виправлення чи видалення персональних даних осіб «не поважає суті основоположного права на ефективний судовий захист, яке закріплене у статті 47 Хартії». Він підкреслив, що наявність судового засобу захисту, який гарантує дотримання правових норм, є невід'ємною частиною правовладдя.

628 Див., наприклад, рішення ЄСПЛ у справі «Карабейоглу проти Туреччини» (*Karabeyolu v. Turkey*), № 30083/10, від 07 червня 2016 р.; рішення ЄСПЛ у справі «Мустафа Сержін Танрікулу проти Туреччини» (*Mustafa Sezgin Tanrıkulu v. Turkey*), № 27473/06, від 18 липня 2017 р.

629 Рішення Суду ЄС, C-362/14, «Максиміліан Шремс проти Уповноваженого із захисту персональних даних» (*Maximillian Schrems v. Data Protection Commissioner*) [ВП], від 06 жовтня 2015 р.

Фізичні особи, контролери та оператори, які мають заперечення щодо юридично зобов'язального рішення контролюючого органу, можуть ініціювати судове провадження[630]. Поняття «рішення» необхідно тлумачити в широкому сенсі, охоплюючи здійснення контролюючим органом слідчих, санкційних та дозвільних повноважень, а також рішення про відхилення чи відмову в задоволенні скарги. Однак заходи, які не є юридично зобов'язальними, такі як надання контролюючим органом висновків чи консультацій, не можуть бути предметом позову до суду[631]. Судові провадження мають здійснюватись у судах держави-члена, у якій засновано контролюючий орган[632].

У випадках порушення прав суб'єктів даних контролером чи оператором, вони наділені правом звернутися зі скаргою до суду[633]. У провадженнях, ініційованих щодо контролера чи оператора, особливо важливо надати фізичним особам вибір місця подання позову. Вони можуть вирішити зробити це в державі-члені, де контролер чи оператор мають осідок, або в державі-члені за місцем постійного проживання цих суб'єктів даних[634]. Другий варіант значно полегшує реалізацію своїх прав суб'єктами даних, оскільки надає їм можливість подавати до суду в державі, де вони проживають, та в межах добре відомої їм юрисдикції. Зведення місця здійснення провадження щодо контролерів чи операторів до держави-члена, де останні мають осідок, може перешкоджати суб'єктам даних, що проживають в іншій державі-члені, подавати позов, оскільки це призвело б до необхідності подорожувати та до додаткових витрат, а провадження могли б здійснюватись іноземною мовою та в межах іноземної юрисдикції. Єдиним винятком є випадки, коли контролер чи оператор є публічним органом і обробка здійснюється в межах виконання ним публічних повноважень. У такому разі розглядати позов мають лише суди держави відповідного державного органу[635].

Хоч здебільшого справи щодо захисту персональних даних вирішуються судами держав-членів, деякі справи можуть бути порушені в Суді ЄС. Перший варіант можливий, коли суб'єкт даних, контролер, оператор чи наглядовий орган бажають подати позов про скасування рішення ЄРЗПД. Однак такий позов підпадає під умови статті 263 ДФЄС. Це означає, що для визнання позову

630 Загальний регламент захисту персональних даних, стаття 78.

631 *Там само*, п. 143 загальної частини.

632 *Там само*, стаття 78 (3).

633 *Там само*, стаття 79.

634 *Там само*, стаття 79 (2).

635 *Там само*.

прийнятним вказані суб'єкти даних та юридичні особи мають довести, що рішення Ради стосується їх особисто.

Другий варіант стосується справ щодо незаконної обробки даних інституціями та органами ЄС. У випадках, якщо інституціями ЄС було порушено законодавство про захист персональних даних, суб'єкт даних може подати позов прямо до Загального Суду ЄС (Загальний Суд входить до складу Суду ЄС). Загальний Суд в якості першої інстанції відповідальний за розгляд скарг про порушення законодавства ЄС інституціями ЄС. Таким чином, скарги як відносно ЄІЗПД, так і відносно інституцій ЄС, можуть бути подані до Загального Суду[636].

Приклад: у справі *«The Bavarian Lager Co. Ltd»*[637] компанія попросила Європейську Комісію надати доступ до повного протоколу засідання, проведеного Комісією, яке, як стверджувалося, стосувалося правових питань, що мали відношення до цієї компанії. Комісія відмовила в задоволенні запиту компанії на отримання доступу з огляду на переважні інтереси захисту персональних даних[638]. Компанія «The Bavarian Lager» подала до Суду першої інстанції (попередника Загального суду) скаргу на це рішення на підставі статті 32 Регламенту інститутів ЄС про захист персональних даних. У своєму рішенні у справі T-194/04 «"The Bavarian Lager" проти Європейської Комісії» Суд першої інстанції скасував рішення Комісії про відмову в задоволенні запиту на доступ. Європейська Комісія подала апеляцію на це рішення до Суду ЄС.

Суд ЄС виніс рішення (у складі Великої Палати), яким скасував рішення Суду першої інстанції та підтримав відмову Європейської Комісії в задоволенні запиту на надання доступу до повного протоколу засідання з метою захисту персональних даних осіб, які були присутні на цьому засіданні. Суд ЄС вважав, що Комісія вчинила правильно, відмовляючи в розкритті такої інформації, оскільки учасники не надали згоди на розголошення своїх персональних даних. Більше того, компанія «The Bavarian Lager» не довела необхідність доступу до такої інформації.

636 Регламент (ЄС) № 45/2001, стаття 32 (3).

637 Рішення Суду ЄС, C-28/08 P, «Європейська Комісія проти "The Bavarian Lager Co. Ltd"» (*European Commission v. The Bavarian Lager Co. Ltd* [GC]), 2010.

638 Для аналізу доводів див. ЄІЗПД (2011), «Правила публічного доступу до документів, що містять персональні дані після рішення у справі "The Bavarian Lager"» (*Public access to documents containing personal data after the Bavarian Lager ruling*), Брюссель, ЄІЗПД.

Крім того, у ході провадження на національному рівні, суб'єкти даних, контролюючі органи, контролери або оператори можуть просити національні суди звернутися по роз'яснення до Суду ЄС щодо тлумачення та чинності актів інституцій, органів, управлінь чи агентств ЄС. Такі роз'яснення відомі як преюдиціальні або попередні рішення. Вони не є безпосереднім засобом юридичного захисту для заявника, але дозволяють національним судам переконатися в тому, що вони застосовують правильне тлумачення права ЄС. Саме завдяки механізму преюдиціальних рішень до Суду ЄС дійшли такі вагомі справи як «"Digital Rights Ireland" та Земельний уряд Каринтії та інші»[639] та «*Шремс*»[640], які значною мірою вплинули на розвиток законодавства про захист персональних даних ЄС.

Приклад: справа «*"Digital Rights Ireland" та Земельний уряд Каринтії та інші*»[641] це об'єднана справа, подана Верховним Судом Ірландії та Конституційним Судом Австрії щодо відповідності Директиви 2006/24/ЕС законодавству про захист персональних даних ЄС. Конституційний Суд Австрії звернувся до Суду ЄС з питанням щодо чинності статей 3–9 Директиви 2006/24/ЕС з огляду на положення статей 7, 9 та 11 Хартії основних прав ЄС. До них було включено питання щодо сумісності певних положень австрійського федерального закону, який імплементував Директиву про зберігання даних, з аспектами дійсної на той час Директиви про захист персональних даних та Регламентом захисту персональних даних інституціями ЄС.

Приклад: у справі «*Земельний уряд Каринтії та інші*» пан Зайтлінгер один із заявників у провадженні Конституційного Суду стверджував, що він використовував телефон, інтернет та електронну пошту в цілях роботи, а також у приватному житті. Відповідно, інформація, яку він надсилав, проходила через суспільні телекомунікаційні мережі. Згідно з Законом Австрії про телекомунікації 2003 року, телекомунікаційний провайдер

639 Рішення Суду ЄС, об'єднані справи C-293/12 та C-594/12, «"Digital Rights Ireland Ltd." проти Міністра зв'язку, морських та природних ресурсів та інших та Земельний уряд Каринтії та інші» (*Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*) [ВП], від 08 квітня 2014р.

640 Рішення Суду ЄС, C-362/14, «Максиміліан Шремс проти Уповноваженого із захисту персональних даних» (*Maximilian Schrems v. Data Protection Commissioner*) [ВП], від 06 жовтня 2015р.

641 Рішення Суду ЄС, об'єднані справи C-293/12 та C-594/12, «"Digital Rights Ireland Ltd." проти Міністра зв'язку, морських та природних ресурсів та інших та Земельний уряд Каринтії та інші» (*Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*) [ВП], від 08 квітня 2014р.

заявника був юридично зобов'язаний збирати та зберігати дані про використання ним мережі. Пан Зайтлінгер був переконаний, що збирання та зберігання його даних не було необхідним для технічних цілей відправлення чи отримання інформації через мережу. Збирання та зберігання таких даних також не було потрібне для виставлення рахунків. Пан Зайтлінгер стверджував, що він не надавав згоди на таке використання персональних даних, які були зібрані та збережені виключно завдяки дії Закону Австрії про комунікації 2003 року.

З огляду на вказане пан Зайтлінгер звернувся з позовом до Конституційного Суду Австрії, у якому він стверджував, що встановлені законодавством зобов'язання телекомунікаційного провайдера порушували його основоположне право, передбачене статтею 8 Хартії основних прав ЄС. З огляду на те, що законодавство Австрії імплементувало законодавство ЄС (Директиву про зберігання даних, що діяла на той час), Конституційний Суд Австрії передав справу до Суду ЄС для вирішення питання щодо сумісності Директиви з правами на приватне життя та захист персональних даних, закріплених Хартією основних прав ЄС.

Справу розглядала Велика Палата Суду ЄС, в результаті чого Директиву про зберігання даних було скасовано. Суд ЄС виявив, що Директива спричиняла особливо серйозне втручання в основоположні права на приватність і захист персональних даних, не обмежуючись крайньою необхідністю. Директива переслідувала легітимну мету, оскільки дозволяла національним державним органам мати додаткові можливості для розслідування та переслідування тяжких злочинів, та, відповідно, була цінним інструментом у кримінальних розслідуваннях. Однак Суд ЄС зауважив, що обмеження основоположних прав можливе лише за крайньої необхідності і має супроводжуватися зрозумілими та чіткими правилами стосовно їхніх меж разом з гарантіями захисту фізичних осіб.

Відповідно до позиції Суду ЄС Директива не пройшла такий іспит на необхідність. По-перше, вона не встановлювала зрозумілих та чітких правил обмеження ступеня втручання. Замість вимоги щодо взаємозв'язку між зберіганням даних і тяжким злочином Директива поширювалася на всі метадані всіх користувачів електронних засобів зв'язку. Таким чином, вона являла собою втручання в права на приватність та захист персональних даних практично всього населення ЄС, що не могло вважатися пропорційним. Вона не містила ані умов обмеження кола осіб, які

мали право доступу до персональних даних, ані процедурних умов, таких як, наприклад, вимога мати дозвіл виконавчого органу або суду на доступ. Нарешті, Директива не встановлювала чітких гарантій захисту даних, що зберігались. Таким чином, вона не забезпечувала ефективного захисту даних від ризику зловживань, неправомірного доступу та використання[642].

В принципі, Суд ЄС повинен дати відповідь на поставлені йому запитання. Він не може відмовитися винести преюдиціальне рішення на тій підставі, що така відповідь не може бути ані значущою, ані своєчасною для початкової справи. Він може, однак, відмовитися, якщо питання не входить до сфери його компетенції[643]. Суд ЄС приймає рішення лише стосовно складових елементів запиту на надання попереднього рішення, тоді як національний суд залишається компетентним приймати рішення в початковій справі[644].

Відповідно до права РЄ Договірні Сторони мають запровадити належні судові та позасудові засоби захисту щодо порушень положень Оновленої Конвенції 108[645]. Твердження про порушення права на захист персональних даних, які суперечать зобов'язанням Договірної Сторони за статтею 8 ЄКПЛ, можуть також бути подані до ЄСПЛ після вичерпання всіх національних засобів юридичного захисту. Заява до ЄСПЛ про порушення статті 8 ЄКПЛ повинна також відповідати іншим критеріям прийнятності (статті 34–35 ЄКПЛ)[646].

Хоча заяви до ЄСПЛ подаються лише проти Договірних Сторін, вони можуть також опосередковано стосуватися дій чи бездіяльності приватних осіб, якщо Договірна Сторона не виконала свого позитивного зобов'язання відповідно до ЄКПЛ та не забезпечила в своєму національному законодавстві достатній рівень захисту від порушень прав на захист персональних даних.

642 Рішення Суду ЄС, об'єднані справи C-293/12 та C-594/12, «"Digital Rights Ireland Ltd." проти Міністра зв'язку, морських та природних ресурсів та інших та Земельний уряд Каринтії та інші» (*Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*) [ВП], від 08 квітня 2014 р., п. 69.

643 Рішення Суду ЄС, C-244/80, «Паскаль Фолья проти Маріелли Новелло» (*Pasquale Foglia v. Mariella Novello*) *(№ 2)*, від 16 грудня 1981р.; рішення Суду ЄС, C-467/04, «Кримінальне провадження проти Гаспаріні та інших» (*Criminal Proceedings against Gasparini and Others*), від 28 вересня 2006 р.

644 Рішення Суду ЄС, C-438/05, «*Міжнародна федерація працівників транспортної сфери, Фінська спілка моряків проти компаній "Viking Line ABP", "OÜ Viking Line Eesti"*» (*International Transport Workers' Federation, Finnish Seamen's Union v. Viking Line ABP, OÜ Viking Line Eesti*) [ВП], від 11 грудня 2007р., п. 85.

645 Оновлена Конвенція 108, стаття 12.

646 ЄКПЛ, *ctammi 34–37*.

Приклад: у справі «*K.U. проти Фінляндії*»[647] неповнолітній заявник скаржився, що на інтернет-сайті про нього було розміщено оголошення сексуального характеру. Постачальник послуг не розкрив відомості про особу, яка розмістила інформацію, у зв'язку із зобов'язаннями дотримуватися вимог конфіденційності згідно з законодавством Фінляндії. Заявник стверджував, що законодавство Фінляндії не забезпечувало належного рівня захисту від дій приватної особи, яка розміщувала в інтернеті відомості, що компрометували заявника. ЄСПЛ постановив, що держави повинні не лише утримуватися від свавільного втручання в приватне життя фізичних осіб, а й можуть також мати позитивні зобов'язання, які передбачають «вжиття заходів, призначених гарантувати повагу до приватного життя навіть у сфері міжособистісних відносин». У справі заявника його практичний та ефективний захист вимагав вжиття ефективних заходів для виявлення порушника та притягнення його до відповідальності. Однак держава не надала такого захисту, відповідно, Суд дійшов висновку, що мало місце порушення статті 8 ЄКПЛ.

Приклад: у справі *«Кьопке проти Німеччини»*[648] заявницю підозрювали в крадіжці на робочому місці та здійснювали за нею приховане відеоспостереження. ЄСПЛ дійшов висновку, що «ніщо не вказувало на те, що національні органи влади не змогли в межах своєї свободи розсуду досягти справедливого балансу між правом заявниці на повагу до її приватного життя, передбаченого статтею 8 ЄКПЛ, та інтересом її роботодавця в захисті своїх майнових прав і державним інтересом у належному здійсненні правосуддя». У зв'язку з цим заяву 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 (стаття 46 ЄКПЛ). Заходи з виконання повинні передусім покласти край порушенню та виправити, наскільки це можливо, його негативні наслідки для заявника. Виконання рішень також може потребувати здійснення загальних заходів для запобігання порушенням, подібним до тих, які встановив Суд, шляхом внесення змін до законодавства, судової практики чи іншими шляхами.

647 Рішення ЄСПЛ у справі «K.U. проти Фінляндії» (*K.U. v. Finland*), № 2872/02, від 02 грудня 2008 р.

648 Рішення ЄСПЛ у справі «Кьопке проти Німеччини» (*Köpke v. Germany*) (пом.), № 420/07, від 05 жовтня 2010 р.

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

Право на уповноваження неприбуткової організації, установи чи об'єднання

ЗРЗПД надає фізичним особам право під час подання скарги до контролюючого органу чи звернення до суду з позовом уповноважувати неприбуткові організації, установи чи об'єднання на представництво своїх інтересів[649]. Такі неприбуткові організації повинні мати статутні завдання у сфері публічних інтересів та здійснювати активну діяльність у царині захисту персональних даних. Вони можуть подати скаргу чи реалізувати право на судовий засіб захисту від імені суб'єкта (суб'єктів) даних. Регламент залишає за державами-членами право вирішувати на рівні національного законодавства питання стосовно можливості подання скарг юридичною особою від імені суб'єктів даних без їхнього доручення.

Право на представництво дає змогу фізичним особам скористатися досвідом, організаційними та фінансовими можливостями таких неприбуткових організацій, тим самим значно полегшуючи реалізацію своїх прав. ЗРЗПД дозволяє таким організаціям подавати колективні скарги від імені багатьох суб'єктів даних. Це також приносить користь функціонуванню та ефективності судової системи, оскільки подібні позови групуються та розглядаються разом.

6.2.3 Відповідальність та право на відшкодування

Право на ефективний засіб захисту дозволяє фізичним особам вимагати компенсації шкоди, яку було заподіяно внаслідок обробки їхніх персональних даних з порушенням відповідного законодавства. Відповідальність контролерів та операторів за незаконну обробку чітко визначена у ЗРЗПД[650]. Регламент надає фізичним особам право отримувати від контролера чи оператора компенсацію як матеріальної, так і нематеріальної шкоди, а в преамбулі Регламенту зазначено, що «поняття шкоди необхідно тлумачити в широкому сенсі через судову практику Суду Справедливості у спосіб, що повністю

649 Загальний регламент захисту персональних даних, стаття 80.

650 Там само, стаття 82.

відображає цілі цього Регламенту»[651]. Контролери несуть відповідальність та є суб'єктами вимог про відшкодування у випадку невиконання ними зобов'язань, передбачених Регламентом. Оператори несуть відповідальність за шкоду, заподіяну обробкою лише у разі невиконання ними обов'язків, передбачених для них Регламентом, чи якщо вони діють поза чи всупереч законним вказівкам контролера. Якщо контролер чи оператор сплатили відшкодування в повному розмірі, ЗРЗПД передбачає, що вони можуть вимагати від інших контролерів та операторів, залучених до тієї ж самої обробки, повернення тієї частини відшкодування, яка відповідає частці їхньої відповідальності за шкоду[652]. Водночас винятки звільнення від відповідальності є дуже вузькими та вимагають доведення, що контролер чи оператор жодним чином не несуть відповідальності за подію, яка спричинила шкоду.

Відшкодування повинно бути «повним та ефективним» щодо заподіяної шкоди. У випадках, коли шкода була спричинена діями декількох контролерів та операторів, кожен контролер чи оператор повинен нести відповідальність за шкоду в повному обсязі. Це правило має на меті забезпечення належної компенсації шкоди суб'єктам даних і координаційного підходу до порозуміння контролерів та операторів, залучених до діяльності з обробки даних.

Приклад: суб'єкти даних не зобов'язані порушувати справу та вимагати компенсацію від всіх суб'єктів, відповідальних за шкоду, оскільки це може мати наслідком великі витрати та тривалі провадження. Досить порушити справу проти одного із співконтролерів, яких може бути пізніше притягнуто до відповідальності за шкоду в повному обсязі. У таких випадках контролер чи оператор, який компенсував шкоду, згодом має право стягнути сплачену суму з інших осіб, залучених до обробки та відповідальних за порушення, у розмірі частки їхньої відповідальності за шкоду. Такі провадження між різними співконтролерами та операторами здійснюються після отримання суб'єктом даних відшкодування, а суб'єкт даних не є їхнім учасником.

У рамках права РЄ стаття 12 Оновленої Конвенції 108 вимагає від Договірних Сторін запровадити належні засоби юридичного захисту стосовно порушень національного закону, яким імплементуються вимоги Конвенції. Пояснювальна записка до Оновленої Конвенції 108 визначає, що засоби

651 Там само, п. 146 преамбули.

652 Там само, стаття 82 (2) та (5).

юридичного захисту повинні передбачати можливість судового оскарження рішень чи дій, при цьому також мають бути доступними позасудові засоби захисту[653]. Питання модальності та різних правил щодо доступу до таких засобів правового захисту, а також порядку, якого необхідно дотримуватися, залишено на розсуд кожної Договірної Сторони. Договірні Сторони та національні суди мають також враховувати положення щодо фінансового відшкодування матеріальної та нематеріальної шкоди, заподіяної обробкою, а також можливості подання колективних позовів[654].

6.2.4 Санкції

Відповідно до права РЄ стаття 12 Оновленої Конвенції передбачає, що кожна Договірна Сторона повинна встановити належні санкції та засоби юридичного захисту стосовно порушень положень національного права, які запроваджують основоположні принципи захисту персональних даних, визначені в Конвенції 108. Конвенція не встановлює та не нав'язує конкретних санкцій. Навпаки, вона чітко вказує, що кожна Договірна Сторона має свободу розсуду в установленні судового чи позасудового характеру санкцій, які можуть бути кримінальними, адміністративними чи цивільними. Пояснювальна записка до Оновленої Конвенції 108 передбачає, що санкції мають бути ефективними, пропорційними та стримувальними[655]. Договірні Сторони повинні дотримуватися цього принципу, визначаючи характер та суворість санкцій, наявних у їхньому національному правопорядку.

Відповідно до права ЄС стаття 83 ЗРЗПД наділяє контролюючі органи держав-членів повноваженнями накладати адміністративні штрафи за порушення Регламенту. Рівень штрафів, обставини, які національні органи беруть до уваги під час вирішення питання про накладення штрафу, в тому числі загальні максимальні розміри такого штрафу також визначені в цій статті. Таким чином, режим застосування санкцій гармонізовано в усьому ЄС.

ЗРЗПД дотримується багаторівневого підходу до штрафів. Контролюючі органи мають повноваження накладати адміністративні штрафи за порушення Регламенту в розмірі до 20 000 000 євро або до 4 % загального річного світового обігу підприємства, залежно від того, яка сума є вищою. Порушення, які можуть досягти такого рівня штрафу, включають порушення основних

653 Пояснювальна записка до Оновленої Конвенції 108, п. 100.

654 Там само.

655 Там само.

принципів обробки та умов щодо надання згоди, порушення прав суб'єктів даних і положень Регламенту, які регулюють передачу персональних даних одержувачам у третіх країнах. За інші порушення контролюючі органи можуть накласти штрафи в розмірі до 10000000 євро чи 2 % загального річного світового обігу підприємства, залежно від того, яка сума є вищою.

Вирішуючи питання щодо типу та рівня штрафу, який має бути накладено, контролюючі органи повинні врахувати низку факторів[656]. Наприклад, вони мають належним чином враховувати суть, ступінь тяжкості та тривалість порушення, категорії персональних даних, яких стосується порушення, його умисний або недбалий характер. Вжиття контролером чи оператором заходів для зменшення шкоди, заподіяної суб'єкту даних, також має братися до уваги. Так само рівень співпраці з контролюючим органом після порушення, спосіб, у який контролюючому органу стало відомо про порушення (наприклад, повідомлення від спеціаліста із захисту персональних даних чи від суб'єкта даних, чиї права були порушені) є іншими факторами, якими керуються контролюючі органи, приймаючи відповідне рішення[657].

Крім можливості накладення адміністративних штрафів, контролюючі органи мають у своєму розпорядженні широкий спектр інших повноважень для виправлення ситуації. Так звані «виправні» повноваження контролюючих органів визначені у статті 58 ЗРЗПД. Вони різняться від видачі приписів, попереджень та зауважень контролерам та операторам до встановлення тимчасової чи навіть постійної заборони діяльності з обробки.

Щодо санкцій за порушення права ЄС з боку інституцій або органів ЄС, у зв'язку зі спеціальною сферою застосування Регламенту про захист персональних даних інститутами ЄС, санкції передбачено лише у вигляді дисциплінарного стягнення. Відповідно до статті 49 Регламенту, «за будь-яке невиконання зобов'язань за цим Регламентом, навмисно чи з необережності, посадова особа або інший службовець Європейського Співтовариства має нести дисциплінарну відповідальність [...]».

656 Загальний регламент захисту персональних даних, стаття 83 (2).

657 Робоча група «Стаття 29» (2017), *Рекомендації щодо застосування та встановлення адміністративних штрафів в цілях Регламенту 2016/679*, РГ 253, від 03 жовтня 2017 р.

7 Міжнародна передача даних та потоки персональних даних

ЄС	Питання, що висвітлюються	РЄ
Передача персональних даних		
Загальний регламент захисту персональних даних, стаття 44	**Концепція**	Оновлена Конвенція 108, стаття 14 (1) та (2)
Вільний потік персональних даних		
Загальний регламент захисту персональних даних, стаття 1 (3) та пункт 170 преамбули	**Між державами-членами ЄС**	
	Між Договірними Сторонами Конвенції 108	Оновлена Конвенція 108, стаття 14 (1)
Передача персональних даних до третіх країн чи міжнародних організацій		
Загальний регламент захисту персональних даних, стаття 45 СЄС, C-362/14, «Максиміліан Шремс проти Уповноваженого із захисту персональних даних» (*Maximillian Schrems v. Data Protection Commissioner*) [ВП], 2015	**Рішення про відповідність/ треті країни чи міжнародні організації з належним рівнем захисту**	Оновлена Конвенція 108, стаття 14 (2)

ЄС	Питання, що висвітлюються	РЄ
Загальний регламент захисту персональних даних, стаття 46 (1) та 46 (2)	**Належні гарантії захисту, в тому числі права, забезпечені санкцією, та засоби юридичного захисту суб'єктів даних, які забезпечуються стандартними договірними положеннями, зобов'язальними корпоративними правилами, кодексами поведінки та механізмами сертифікації**	Оновлена Конвенція 108, стаття 14 (2), (3), (5) та (6)
Загальний регламент захисту персональних даних, стаття 46 (3)	**Погодження контролюючим органом: договірні положення та умови, включені до адміністративних домовленостей між органами влади**	
Загальний регламент захисту персональних даних, стаття 46 (5)	**Наявні дозволи на основі Директиви 95/46**	
Загальний регламент захисту персональних даних, стаття 47	**Зобов'язальні корпоративні правила**	

ЄС	Питання, що висвітлюються	РЄ
Загальний регламент захисту персональних даних, стаття 49	**Відступи в конкретних ситуаціях**	Оновлена Конвенція 108, стаття 14 (4)
Приклади: Угода між ЄС та США щодо реєстраційних даних пасажирів (PNR) Угода між ЄС та США щодо системи SWIFT	**Міжнародні угоди**	Оновлена Конвенція 108, стаття 14 (3) (a)

Відповідно до права ЄС Загальний регламент захисту персональних даних забезпечує вільний потік даних у межах Європейського Союзу. Втім у ньому містяться особливі вимоги стосовно передачі персональних даних третім країнам поза межами ЄС та міжнародним організаціям. Регламент визнає важливість таких передач, особливо з огляду на міжнародну торгівлю та співробітництво, але також визнає підвищений ризик для персональних даних. У зв'язку з цим Регламент має на меті забезпечити такий рівень захисту персональних даних, переданих до третіх країн, який вони мають у межах ЄС[658]. Право РЄ також визнає важливість впровадження правил для транскордонних потоків даних, заснованих на вільному рухові даних між сторонами та спеціальних вимогах до передачі державам, які не є її сторонами.

7.1 Характер передачі персональних даних

Ключові моменти

- Право ЄС та РЄ містить правила передачі персональних даних одержувачам у третіх країнах або міжнародним організаціям.
- Забезпечення захисту прав суб'єктів даних при передачі персональних даних за межі ЄС надає можливість захисним гарантіям законодавства ЄС розповсюджуватися на персональні дані, які походять з ЄС.

658 Загальний регламент захисту персональних даних, п. 101 та 116 преамбули.

У **праві РЄ** транскордонні потоки персональних даних описуються як передача персональних даних одержувачам, які підпадають під юрисдикцію іноземної держави[659]. Транскордонні потоки персональних даних до одержувача, який не знаходиться під юрисдикцією Договірної Сторони, дозволені лише за умови забезпечення належного рівня захисту[660].

Право ЄС регулює передачу «персональних даних, які перебувають у процесі обробки чи призначені для обробки після передачі третій країні або міжнародній організації [...]»[661]. Такі потоки даних дозволені лише у разі дотримання правил, встановлених главою V ЗРЗПД.

Транскордонні потоки персональних даних можуть спрямовуватися до одержувачів, які підпадають під юрисдикцію Договірної Сторони чи держави-члена згідно з правом РЄ чи ЄС, відповідно. Обидві правові системи дозволяють передачу даних до країни, яка не є Договірною Стороною чи державою-членом, у разі виконання певних умов.

7.2 Вільний рух/потік персональних даних між державами-членами чи Договірними Сторонами

Ключові моменти

- Потік персональних даних на території ЄС, як і передача персональних даних між Договірними Сторонами Оновленої Конвенції 108 мають бути необмеженими. Однак, оскільки не всі Договірні Сторони Оновленої Конвенції 108 є державами-членами ЄС, передача з держави-члена ЄС до третьої країни, яка є Договірною Стороною Конвенції 108, неможлива без дотримання умов, встановлених у ЗРЗПД.

Відповідно до права РЄ між Договірними Сторонами Оновленої Конвенції 108 повинен існувати вільний потік персональних даних. Однак передача може бути заборонена у разі, якщо існує «реальний і серйозний ризик того, що

659 Пояснювальна записка до Оновленої Конвенції 108, п. 102.

660 Оновлена Конвенція 108, стаття 14 (2).

661 Загальний регламент захисту персональних даних, стаття 44.

передача до іншої Сторони, призведе до невиконання положень Конвенції», або якщо Сторона зобов'язана вчинити так за «узгодженими правилами захисту, що є спільними для держав, які належать до регіональної міжнародної організації»[662].

Відповідно до права ЄС обмеження або заборона вільного руху персональних даних між державами-членами ЄС з міркувань захисту фізичних осіб стосовно обробки персональних даних не дозволяється[663]. Зону вільного обміну персональними даними було розширено Угодою про створення Європейського економічного простору (ЄЕП)[664], за якою Ісландію, Ліхтенштейн і Норвегію було включено до внутрішнього ринку.

Приклад: якщо філія міжнародної групи компаній, зареєстрованих у декількох державах-членах ЄС, до яких входять Словенія та Франція, передає персональні дані зі Словенії до Франції, такий потік даних не повинен обмежуватися або заборонятися національним законодавством Словенії на підставі захисту персональних даних.

Проте якщо та ж словенська філія бажає передати ті самі персональні дані до материнської компанії в Малайзію, словенський експортер даних повинен враховувати правила, наведені в главі V ЗРЗПД. Ці положення покликані захищати персональні дані суб'єктів даних, які підпадають під юрисдикцію ЄС.

Відповідно до права ЄС потоки персональних даних до держав-членів ЄЕП у цілях запобігання, розслідування, виявлення чи переслідування за вчинення кримінальних правопорушень або для виконання кримінальних покарань підпадають під дію Директиви 2016/680[665]. Обмін персональними даними між

662 Оновлена Конвенція 108, стаття 14 (1).

663 Загальний регламент захисту персональних даних, стаття 1 (3).

664 Рішення Ради ЄС та Європейської Комісії від 13 грудня 1993 р. про укладення Угоди про Європейський економічний простір між Європейським Співтовариством, його державами-членами та Республікою Австрією, Фінляндською Республікою, Республікою Ісландією, Князівством Ліхтенштейном, Королівством Норвегією, Королівством Швецією та Швейцарською Конфедерацією, OJ 1994 L 1.

665 *Директива (ЄС) 2016/680* Європейського Парламенту та Ради від 27 квітня 2016 р. щодо захисту фізичних осіб стосовно обробки персональних даних компетентними органами в цілях запобігання, розслідування, виявлення чи переслідування кримінальних правопорушень або виконання кримінальних покарань, а також вільний потік таких даних та скасування рамкового рішення Ради 2008/977/JHA, OJ 2016 L119.

компетентними органами в межах ЄС також не обмежується та не забороняється на підставі захисту персональних даних. Відповідно до права РЄ до сфери дії Конвенції потрапляє обробка всіх персональних даних (в тому числі їх транскордонний обмін з іншими сторонами Конвенції 108) без винятків щодо цілей чи сфер діяльності, хоча винятки можуть бути встановлені Договірними Сторонами. Всі члени ЄЕП є також сторонами Конвенції 108.

7.3 Передача персональних даних до третіх країн/несторін або до міжнародних організацій

Ключові моменти

- **РЄ** та **ЄС** дозволяють передачу персональних даних третім країнам чи міжнародним організаціям при дотриманні певних умов захисту персональних даних.
  - **Відповідно до права РЄ** належний рівень захисту може бути гарантований законодавством держави чи міжнародної організації або за наявності належних стандартів.
  - **Відповідно до права ЄС** передача може мати місце, якщо третя країна забезпечує відповідний рівень захисту, або контролер чи оператор даних надає належні гарантії, в тому числі забезпечені санкцією права та засоби юридичного захисту, за допомогою стандартних положень про захист персональних даних чи зобов'язальних корпоративних правил.
- **Право РЄ та ЄС** передбачає положення про відступи, відповідно до яких дозволяється передача персональних даних за окремих обставин, навіть у разі відсутності достатнього рівня захисту чи належних гарантій.

Хоч і право РЄ, і право ЄС допускають рух даних до третіх країн або міжнародних організацій, вони містять різні умови. Кожен набір умов враховує різну структуру та цілі організації.

Відповідно до **права ЄС**, в принципі існує два способи дозволити передачу персональних даних до третіх країн чи міжнародних організацій. Передача персональних даних може мати місце на підставі: рішення Європейської комісії про відповідність[666]; або, за відсутності такого рішення, якщо контролер

666 Загальний регламент захисту персональних даних, стаття 45.

чи оператор надає належні гарантії, в тому числі права, забезпечені санкцією, та засоби юридичного захисту для суб'єкта даних[667]; Існує низка відступів у ситуаціях, коли відсутнє рішення про відповідність або належні гарантії.

Втім відповідно до права **РЄ** вільна передача даних до держав, що не є сторонами Конвенції, дозволена лише на підставі:

- законодавства цієї держави або міжнародної організації, включаючи застосовні міжнародні договори або угоди, які надають відповідні гарантії;
- тимчасових або затверджених стандартизованих гарантій, забезпечених юридично зобов'язальними та такими, що можуть бути виконаними, інструментами, які приймаються та запроваджуються особами, залученими до передачі та подальшої обробки даних[668].

Подібно до права ЄС, існує низка відступів у разі відсутності належного рівня захисту персональних даних.

7.3.1 Передача на підставі рішення про відповідність

Відповідно до права ЄС, вільний рух персональних даних до третіх країн з належним рівнем захисту персональних даних передбачено в статті 45 ЗРЗПД. Суд ЄС роз'яснив, що поняття «належний рівень захисту» вимагає забезпечення третьою країною такого рівня захисту основних прав та свобод, який є «по суті рівнозначним»[669] гарантіям, що забезпечені правом ЄС. Водночас засоби, на які покладається третя країна з метою досягнення такого рівня захисту, можуть відрізнятися від тих, які використовуються в ЄС, стандарт відповідності не вимагає точного копіювання правил[670].

Європейська Комісія оцінює рівень захисту персональних даних в іноземних країнах, вивчаючи їхнє законодавство та застосовні міжнародні зобов'язання. Також враховується участь держави в багатосторонніх чи регіональних системах, зокрема, щодо захисту персональних даних. Якщо Європейська Комісія

667 Там само, стаття 46.

668 Оновлена Конвенція 108, стаття 14 (3) (a) та (b).

669 Рішення Суду ЄС, C-362/14, «Максиміліан Шремс проти Уповноваженого із захисту персональних даних» (*Maximillian Schrems v. Data Protection Commissioner*) [ВП], від 06 жовтня 2015р., п. 96.

670 Там само, п. 74. Див. також, Європейська Комісія (2017), Комюніке Комісії до Європейського Парламенту та Ради «Обмін та захист персональних даних у глобалізованому світі», COM(2017)7 фінальне від 10 січня 2017 р., п. 6.

встановить, що третя країна чи міжнародна організація забезпечує належний рівень захисту, вона може прийняти рішення про відповідність, яке є обов'язковим[671]. Однак Суд ЄС вирішив, що контролюючі органи вже ж мають повноваження розглядати скарги особи щодо захисту персональних даних, переданих до третьої країни, яка була визнана Комісією такою, що забезпечує належний рівень захисту, якщо особа незгодна з тим, що чинні законодавство та практика відповідної країни забезпечують такий рівень захисту[672].

Європейська Комісія також може оцінити відповідність на всій території третьої країни чи обмежитися певними секторами, як, наприклад, у справі щодо комерційного законодавства Канади[673]. Існують також висновки про відповідність, які ґрунтуються на угодах між ЄС та третіми країнами. Ці рішення стосуються винятково одного типу передачі даних, а саме передачі реєстраційних даних пасажирів авіакомпаніями іноземним органам прикордонного контролю, коли авіакомпанія забезпечує переліт з ЄС до певних іноземних країн (див. *розділ 7.3.4*)

Рішення про відповідність підлягають моніторингу на постійній основі. Європейська Комісія постійно переглядає такі рішення для відстеження тенденцій розвитку подій, що можуть вплинути на їхній стан. Тож якщо Європейська Комісія встановить, що третя країна чи міжнародна організація більше не відповідає умовам, які підтверджують рішення про відповідність, вона може внести зміни, тимчасово зупинити чи скасувати рішення. Комісія також може вступити в переговори з такою третьою країною чи міжнародною організацією для вирішення проблеми, що спричинила таке рішення.

Рішення про відповідність, прийняті Європейською комісією на основі Директиви 95/46/ЄС, залишаються чинними до внесення змін, заміни чи скасування рішенням Комісії, ухваленим відповідно до правил статті 45 ЗРЗПД.

Наразі Європейська Комісія визнала такими, що забезпечують відповідний захист, Андорру, Аргентину, Канаду (комерційні організації, які підпадають під дію Акта про захист персональної інформації та електронні

671 Постійно оновлюваний список країн, які отримали висновки про відповідність, див. на головній сторінці *European Commission, Directorate-General for Justice*.

672 Рішення Суду ЄС, C-362/14, «Максиміліан Шремс проти Уповноваженого із захисту персональних даних» (*Maximillian Schrems v. Data Protection Commissioner [*GC]), від 06 жовтня 2015 р., пп. 63 та 65– 66.

673 Європейська Комісія (2002), Рішення 2002/2/ЕС від 20 грудня 2001 р., прийняте відповідно до Директиви 95/46/ЄС Європейського Парламенту і Ради (ЄС), щодо відповідного рівня захисту персональних даних, передбаченого Актом про захист персональної інформації та електронні документи Канади, OJ 2002 L 2.

документи – PIPEDA), Фарерські острови, Гернсі, Острів Мен, Ізраїль, Джерсі, Нову Зеландію, Швейцарію та Уругвай. Щодо передачі даних до США, Європейська Комісія ухвалила у 2000 році рішення про відповідність, яке дозволяло передачу компаніям, що самосертифікували (подали відповідне повідомлення) свій захист персональних даних, переданих з ЄС, та відповідали так званим «Принципам безпечної гавані»[674]. Суд ЄС визнав недійсним це рішення у 2015 році, а в липні 2016 року було прийнято нове рішення про відповідність, яке дозволило компаніям приєднуватися з 01 серпня 2016 року.

Приклад: у справі «*Шремс*»[675], Максиміліан Шремс, громадянин Австрії, був користувачем соціальної мережі Facebook декілька років. Частина або всі дані, надані паном Шремсом до Facebook, були передані з ірландського дочірнього підприємства «Facebook» на сервери, розміщені в США, де вони оброблялись. Пан Шремс подав скаргу до органу захисту персональних даних Ірландії, вважаючи, що з огляду на викриття, зроблені американським програмістом Едвардом Сноуденом стосовно ведення спостереження спецслужбами США, законодавство та практика США не передбачає достатній захист даних, переданих до цієї країни. Ірландський орган влади відмовив у задоволенні скарги на підставі того, що відповідно до рішення Комісії від 26 липня 2000 року за схемою «Безпечна гавань» США забезпечує відповідний рівень захисту переданих персональних даних. Справу розглядав Верховний Суд Ірландії, який звернувся до Суду ЄС по преюдиціальне рішення.

Суд ЄС постановив, що рішення Комісії про відповідність системи «Безпечна гавань» є недійсним. Суд ЄС насамперед зазначив, що рішення дозволяло обмежити застосування принципів захисту персональних даних «Безпечна гавань» для забезпечення вимог національної безпеки, суспільного інтересу чи правоохоронних органів або на підставі національного законодавства США. Таким чином, рішення уможливлювало втручання в основоположні права осіб, персональні даних яких були

674 *Рішення Європейської Комісії 2000/520/ЄС* від 26 липня 2000 р., прийняте відповідно до Директиви 95/46/ЄС Європейського Парламенту та Ради, щодо відповідності захисту, передбаченого принципами конфіденційності «Безпечна гавань», та пов'язаних з ними типових питань, виданих Департаментом торгівлі США, OJ L 215. У справі C-632/14 «Максиміліан Шремс проти Уповноваженого із захисту персональних даних» (*Maximilian Schrems v. Data Protection Commissioner*) [ВП]) Судом ЄС рішення було визнано недійсним.

675 Рішення Суду ЄС, C-362/14, «Максиміліан Шремс проти Уповноваженого із захисту персональних даних» (*Maximilian Schrems v. Data Protection Commissioner*) [ВП]), від 06 жовтня 2015 р.

чи могли бути передані до США[676]. Надалі він зазначив, що рішення не містить жодних висновків про наявність у США правил, спрямованих на обмеження такого втручання, чи будь-якого ефективного юридичного захисту від нього[677]. СЄС підкреслив, що рівень захисту основоположних прав і свобод, гарантований у межах ЄС, вимагає від нормативних актів, які стосуються статей 7 та 8, встановлення чітких і точних правил щодо визначення обсягу та застосовності заходів, а також закріплення мінімальних гарантій, відступів та обмежень стосовно захисту персональних даних[678]. Оскільки в рішенні Комісії не було зазначено про фактичне забезпечення США такого рівня захисту в національному законодавстві країни чи її міжнародних зобов'язаннях, СЄС дійшов висновку, що рішення Комісії не відповідає вимогам відповідних положень Директиви про захист персональних даних щодо передачі даних та, відповідно, визнав його нечинним[679].

Таким чином, рівень захисту США не був «по суті рівнозначним» для забезпечення основних прав і свобод, гарантованих ЄС[680]. Суд ЄС стверджував про порушення декількох статей Хартії основних прав ЄС. По-перше, було поставлено під загрозу суть статті 7, оскільки законодавство США «дозволяло державним органам влади на загальних підставах мати доступ до змісту електронних повідомлень». По-друге, суть статті 47 було також порушено, оскільки законодавство не передбачало для фізичних осіб засобів юридичного захисту стосовно доступу до персональних даних, їх виправлення чи видалення. Нарешті, враховуючи порушення механізмом «Безпечна гавань» вказаних статей, персональні дані вже більше не оброблялися законним чином, що призводило до порушення статті 8.

Після визнання Судом ЄС механізму «Безпечна гавань» недійсною Комісія та США домовилися про нову систему «Щит приватності» (the EU-U.S. Privacy Shield). У липні 2016 Комісія прийняла рішення, у якому визнавалося, що США

676 Там само, п. 84.

677 Там само, пп. 88–89.

678 Там само, пп. 91–92.

679 Там само, пп. 96–97.

680 Там само, пп. 73–74 та 96.

забезпечує належний рівень захисту персональних даних, переданих із ЄС до організацій у США в межах системи «Щит приватності»[681].

Аналогічно до системи «Безпечна гавань», система «Щит приватності» покликана захистити персональні дані, які передаються з ЄС до США у комерційних цілях[682]. Американські компанії можуть добровільно сертифікувати суворе дотримання ними всіх гарантій «Щита приватності», зобов'язуючись дотримуватися стандартів захисту персональних даних. Компетентні органи США здійснюють моніторинг та перевірку відповідності сертифікованих компаній таким стандартам.

Зокрема, схема «Щит приватності» передбачає:

- обов'язки компаній, які отримують персональні дані з ЄС, щодо захисту персональних даних;
- захист та відшкодування збитків для фізичних осіб, зокрема запровадження інституту омбудсмена, що є незалежним від спецслужб США та розглядає скарги осіб, які вважають, що їхні персональні дані були незаконно використані органами влади США у сфері національної безпеки;
- щорічний спільний огляд для моніторингу виконання правил системи[683]: перший огляд було проведено у вересні 2017 року[684].

Уряд США надав у письмовій формі зобов'язання та гарантії, які долучені до рішення «Щит приватності». Вони передбачають обмеження та гарантії щодо доступу уряду США до персональних даних в цілях правоохоронної діяльності та національної безпеки.

---

681 *Рішення Європейської Комісії про впровадження (EU) 2016/1250* від 12 липня 2016 р., прийняте відповідно до Директиви 95/46/ЄС Європейського Парламенту і Ради, щодо відповідності захисту, передбаченого системою «Щит приватності» (EU-U.S. Privacy Shield), OJ L 207. Робоча група «Стаття 29» підтримала поліпшення, які передбачав механізм «Щит приватності» в порівнянні з рішенням «Безпечна гавань», та рекомендувала Європейській Комісії та державним органам США під час прийняття остаточного варіанту документів «Щит приватності» врахувати занепокоєння, висловлені в її Висновку РГ 238 щодо проєкту рішення про відповідність системи «Щит приватності» (EU-U.S. Privacy Shield). Втім було підкреслено низку невирішених проблем. Більше деталей див. Робоча група «Стаття 29», *Висновок 01/2016 щодо проєкту рішення про відповідність системи «Щит приватності» (EU-U.S. Privacy Shield)*, прийнятий 13 квітня 2016 р., 16/EN РГ 238.

682 Для додаткової інформації див. *EU-U.S. Privacy Shield factsheet*.

683 Для додаткової інформації див. вебсторінку Європейської Комісії підрозділ *EU-U.S. Privacy Shield*.

684 Європейська Комісія, *Звіт Комісії до Європейського Парламенту та Ради щодо першого щорічного огляду функціонування системи «Щит приватності» (EU–U.S. Privacy Shield)*, COM(2017) 611 остаточний, від 18 жовтня 2017 р. Див. також Робоча група «Стаття 29», «Щит приватності» (*EU–U.S. Privacy Shield)* – перший щорічний спільний огляд, прийнятий 28 листопада 2017 р., 17/EN WP 255.

7.3.2 Передача на підставі належних гарантій

Як у **праві РЄ**, так і в **праві ЄС** належні гарантії, що існують між контролером, що експортує дані, та одержувачем у третій країні або міжнародною організацією визнаються як можливий засіб забезпечення одержувачем достатнього рівня захисту персональних даних.

Відповідно до **права ЄС**, передача персональних даних до третьої країни чи міжнародної організації дозволяється, якщо контролер або оператор надає належні гарантії та права, забезпечені правовою санкцією, а суб'єктам даних доступні ефективні засоби юридичного захисту[685]. Перелік прийнятних «належних гарантій» наводиться виключно законодавством ЄС про захист персональних даних. Належні гарантії можуть бути встановлені:

- обов'язковими та такими, що підлягають примусовому виконанню, юридичними документами, прийнятими державними органами та установами;
- зобов'язальними корпоративними правилами;
- стандартними положеннями щодо захисту персональних даних, затвердженими Європейською комісією та контролюючим органом;
- кодексами поведінки;
- механізмами сертифікації[686].

Іншими засобами забезпечення належних гарантій є договірні положення між контролером або оператором у ЄС та одержувачем даних у третій країні. Однак такі договірні положення мають бути погоджені контролюючим органом, перш ніж вони можуть бути використані як підстава для передачі даних. Так само державні органи можуть використовувати положення про захист персональних даних, включені до їхніх адміністративних угод за умови погодження їх контролюючим органом[687].

Відповідно до права РЄ, потік даних до країни чи міжнародної організації, яка не є стороною Оновленої Конвенції 108, дозволяється за умови забезпечення належного рівня захисту. Такий рівень може бути досягнуто:

- законодавством держави чи міжнародної організації;

685 Загальний регламент захисту персональних даних, стаття 46.

686 Загальний регламент захисту персональних даних, статті 46 (1) (c), (d), (2) (a), (b), (e), (f) та 47.

687 Там само, стаття 46 (3).

- ad hoc чи стандартизованими гарантіями, які є частиною юридично зобов'язального документа[688].

Передача на підставі договірних положень

Як у **праві РЄ**, так і в **праві ЄС** договірні положення між контролером, що експортує дані, та одержувачем у третій країні визнаються як можливий засіб забезпечення одержувачем достатнього рівня захисту персональних даних[689].

На **рівні ЄС** Європейська Комісія за допомогою Робочої групи «Стаття 29» розробила стандартні положення про захист персональних даних, які були офіційно затверджені Рішенням Комісії як доказ відповідного рівня захисту персональних даних[690]. Оскільки рішення Комісії є обов'язковими для держав-членів у повному обсязі, національні органи, які здійснюють контроль за передачею даних, повинні визнати ці стандартні договірні положення у своїх процедурах[691]. Таким чином, якщо контролер, який експортує дані, та одержувач у третій країні домовляються і підписують такі положення, це має надати наглядовому органу достатні докази того, що гарантії належного рівня захисту забезпечено. Але у справі «*Шремса*» Суд ЄС постановив, що до компетенції Європейської комісії не входить обмеження повноважень національних контролюючих органів здійснювати нагляд за передачею персональних даних до третьої країни, щодо якої було винесено рішення Комісії про відповідність[692]. Таким чином, національний контролюючий орган не має перешкод у виконанні своїх повноважень, у тому числі зупиняти чи забороняти передачу персональних даних, якщо вона здійснюється з порушенням законодавства ЄС чи національного законодавства про захист персональних даних, наприклад, коли імпортер даних не дотримується стандартних договірних положень[693].

---

688 Оновлена Конвенція 108, стаття 14 (3) (b).

689 Загальний регламент захисту персональних даних, стаття 46 (3); Оновлена Конвенція 108, стаття 14(3)(b).

690 Там само, стаття 46 (2) (b) та стаття 46 (5).

691 Там само, стаття 46 (32) (c); Договір про функціонування Європейського Союзу, стаття 288); Ad hoc Комітет із захисту персональних даних (CAHDATA), Пояснювальна записка до Оновленої Конвенції про захист фізичних осіб відносно автоматизованої обробки персональних даних, п. 105.

692 Рішення Суду ЄС, C-362/14, «Максиміліан Шремс проти Уповноваженого із захисту персональних даних» (*Maximilian Schrems v. Data Protection Commissioner*) [ВП], від 06 жовтня 2015 р., пп. 96–98 та 102–105.

693 З метою врахування позиції Суду ЄС у справі *Шремса*, Європейська Комісія внесла зміни до Рішення про стандартні договірні положення. *Рішення Європейської Комісії про впровадження (ЄС) 2016/2297* від 16 грудня 2016, яким внесено зміни до Рішення 2001/497/ЄС та 2010/87/ЄС про стандартні договірні положення для передачі персональних даних до третіх країн та операторів, які мають осідок у таких країнах, прийняте відповідно до Директиви 95/46/ЄС Європейського Парламенту і Ради, OJ 2016 L344.

Існування стандартних договірних положень у нормативній базі ЄС не забороняє контролерам формулювати інші спеціальні договірні положення *ad hoc* до того, як контролюючий орган затвердить такі положення[694]. Вони, однак, повинні забезпечувати такий самий рівень захисту, який забезпечують стандартні договірні положення. При затвердженні спеціальних положень контролюючі органи зобов'язані застосовувати механізм узгодження з метою забезпечення єдиного регуляторного підходу в усьому ЄС[695]. Це означає, що компетентний орган повинен надіслати проєкт свого рішення щодо положень до ЄРЗПД. ЄРЗПД надасть висновок з цього питання, який має бути максимально врахований контролюючим органом під час прийняття рішення. Якщо орган не має наміру дотримуватися висновку ЄРЗПД, у рамках ЄРЗПД буде запущено механізм вирішення спорів і Рада прийме обов'язкове рішення[696].

Найважливішими характеристиками стандартних договірних положень є:

- положення про бенефіціара третьої сторони, яке надає можливість суб'єктам персональних даних здійснювати свої договірні права, навіть якщо вони не є стороною договору;
- одержувач чи імпортер даних, який погоджується підпорядковуватися національному контролюючому органу та/або, у разі виникнення спору, суду контролера, що експортує дані.

Наразі доступні два набори стандартних положень передачі даних від контролера до контролера, один з яких може обрати контролер, що експортує дані[697]. Для передачі даних від контролера до оператора існує тільки один набір стандартних договірних положень[698]. Однак наразі вказані стандартні договірні положення є предметом судового розгляду.

694 Загальний регламент захисту персональних даних, стаття 46 (3) (a).

695 Там само, стаття 63 та стаття 64 (1) (e).

696 Там само, стаття 64 та стаття 65.

697 І набір міститься в додатку до Рішення Європейської Комісії (2001) 2001/497/ЄС від 15 June 2001 р. про стандартні положення передачі персональних даних до третіх країн, прийняте відповідно до Директиви 95/46/ЄС, OJ 2001 L 181; ІІ набір міститься в додатку до Рішення Європейської Комісії (2004) 2004/915/ЄС від 27 грудня 2004 р. із змінами, внесеними Рішенням 2001/497/ЄС, щодо введення альтернативного набору стандартних договірних положень для передачі персональних даних до третіх країн, OJ 2004 L 385.

698 Європейська Комісія (2010), Рішення Комісії 2010/87 від 05 лютого 2010 р. про стандартні договірні положення для передачі персональних даних до процесорів, які мають осідок у третіх країнах, прийняте відповідно до Директиви 95/46/ЄС Європейського Парламенту і Ради, OJ 2010 L 39. На час підготовки посібника питання щодо використання стандартних договірних положень, як підстави для передачі персональних даних до США, перебувало на розгляді Верховного Суду Ірландії.

Приклад: після визнання СЄС рішення «Про безпечну гавань» недійсним[699] передача персональних даних до США більше не могла здійснюватися на його підставі. Поки тривали переговори з владою США до прийняття нового рішення про відповідність (врешті-решт прийнятого 12 липня 2016 року)[700], передача могла здійснюватися лише на інших правових підставах, таких як стандартні договірні положення чи зобов'язальні корпоративні правила. Декілька компаній, в тому числі «Facebook Ireland» (проти якої було порушено справу, що призвела до визнання недійсним рішення «Про безпечну гавань»), перейшли на стандартні договірні положення для продовження передачі даних з ЄС до США.

Пан Шремс подав скаргу до контролюючого органу Ірландії з вимогою припинити передачу даних до США на підставі стандартних договірних положень. По суті він стверджував про відсутність гарантій захисту своїх даних у випадку, якщо його персональні дані будуть передані з ірландської дочірньої компанії «Facebook» до компанії «Facebook Inc.» та на розташовані в США сервери. Компанія «Facebook Inc.» підпорядковується американським законам, відповідно до яких вона може бути зобов'язана розкрити персональні дані американським правоохоронним органам, а для європейців недоступні судові засоби захисту для оскарження такої практики[701]. Саме з цієї причини Суд ЄС дійшов висновку, що рішення «Про безпечну гавань» є недійсним, і хоча судове рішення обмежувалося лише цим висновком, заявник вважав порушені питання доречними під час передачі даних на підставі договірних положень. На час написання цього посібника справа перебувала на розгляді Верховного Суду Ірландії. Заявник, напевно, має намір передати справу до СЄС з метою оскарження рішення Європейської комісії щодо стандартних договірних положень. Як зазначалось у главі 5, лише Суд ЄС має компетенцію визнати акт ЄС нечинним.

699 Рішення Суду ЄС, C-362/14, «Максиміліан Шремс проти Уповноваженого із захисту персональних даних» (*Maximilian Schrems v. Data Protection Commissioner*) [ВП]), від 06 жовтня 2015 р.

700 Рішення Комісії про впровадження (ЄС) 2016/1250 від 12 липня 2016 р., прийняте відповідно до Директиви 95/46/ЄС Європейського Парламенту і Ради щодо відповідності захисту, передбаченого системою «Щит приватності» (EU-U.S. Privacy Shield), OJ L 207.

701 Для отримання додаткової інформації див. *виправлену скаргу* проти компанії «Facebook Ireland Ltd», яку було подано до Уповноваженого із захисту персональних даних Ірландії Максиміліаном Шремсом 01 грудня 2015 р.

Передача на підставі обов'язкових корпоративних правил

Право ЄС також дозволяє передачу персональних даних на підставі обов'язкових корпоративних правил для міжнародних передач, які здійснюються в межах однієї групи компаній або підприємств, що здійснюють спільну господарську діяльність[702]. Перш ніж зобов'язальні корпоративні правила можуть бути використані як підстава для передачі персональних даних, компетентний контролюючий орган повинен затвердити їх згідно з зобов'язальними корпоративними правилами з використанням механізму узгодженості.

Для того, щоб бути затвердженими, зобов'язальні корпоративні правила повинні бути юридично обов'язковими, охоплювати всі основні принципи захисту персональних даних, поширюватися на кожного члена групи та виконуватися ним. Вони мають прямо надавати суб'єктам даних права, забезпечені санкцією, включати всі основні принципи захисту персональних даних та відповідати певним формальним вимогам, наприклад чітко вказувати структуру зобов'язань, описувати передачу даних та зазначати, яким чином будуть застосовуватися вказані принципи. Відповідна інформація має надаватися суб'єктам даних. Правила повинні точно визначати, серед іншого, права суб'єктів даних і положення щодо відповідальності за їх порушення[703]. При погодженні зобов'язальних корпоративних правил застосовується механізм узгодженості для співпраці контролюючих органів (описаний у главі 5).

У рамках механізму узгодженості головний контролюючий орган перевіряє запропоновані зобов'язальні корпоративні правила, складає проєкт рішення та надсилає його до ЄРЗПД. Рада надає висновок з цього питання, після чого головний контролюючий орган може офіційно затвердити зобов'язальні корпоративні правила, «максимально враховуючи» при цьому, висновок Ради. Цей висновок не є юридично обов'язковим, але якщо контролюючий орган має намір не брати його до уваги, застосовується механізм врегулювання спорів, і Рада буде проводити засідання, щоб двома третинами членів ухвалити юридично зобов'язальне рішення[704].

Відповідно до **права РЄ,** спеціальні чи стандартизовані гарантії, що є частинами юридично обов'язкового документа[705], також включають зобов'язальні корпоративні правила.

---

702 Загальний регламент захисту персональних даних, стаття 47.

703 Див. більш детальний опис у статті 47 Загального регламенту про захист персональних даних.

704 Там само, статті 57 (1) (s), 58 (1) (j), 64 (1) (f), 65 (1) та (2).

705 Оновлена Конвенція 108, стаття 14 (3) (b).

7.3.3 Відступи в особливих ситуаціях

Відповідно до права ЄС, передача персональних даних до третьої країни може бути правомірною навіть у разі відсутності рішення про відповідність чи відсутність таких гарантій, як стандартні договірні положення чи обов'язкові корпоративні правила, за будь-якої з наступних умов:

- надання суб'єктом даних явної згоди на передачу персональних даних;
- якщо суб'єкт даних вступає або готується вступити в договірні правовідносини, для чого необхідна передача даних за кордон;
- у разі укладення договору між контролером та третьою особою в інтересах суб'єкта даних;
- у разі існування важливих цілей суспільного інтересу;
- для формування, пред'явлення та захисту правових претензій;
- для захисту життєво важливих інтересів суб'єктів даних;
- для передачі даних з публічних реєстрів (це приклад переважного інтересу громадськості в тому, щоб мати доступ до інформації, яка зберігається в публічних реєстрах)[706].

Коли жодна з вказаних умов незастосовна і передача не може ґрунтуватися на рішенні про відповідність або належних гарантіях, передача може мати місце лише у випадку, якщо вона є одноразовою, стосується обмеженої кількості суб'єктів даних та є необхідною у цілях обґрунтованих легітимних інтересів контролера даних за умови, що права суб'єктів даних їх не переважають[707]. У таких випадках контролер повинен оцінити обставини, що супроводжують передачу даних, та забезпечити заходи безпеки. Він також повинен поінформувати контролюючий орган та відповідних суб'єктів даних про передачу даних та легітимні інтереси, які її виправдовують.

Той факт, що відступи є крайнім засобом для правомірної передачі[708] (використовуються лише у разі відсутності рішення про відповідність та якщо немає інших гарантій), підкреслює їхній винятковий характер та додатково підкреслюється в пунктах преамбули ЗРЗПД. Відступи визнаються можливими «для передачі даних за особливих обставин» на підставі згоди та у випадку,

706 Загальний регламент захисту персональних даних, стаття 49.

707 Там само.

708 Там само, стаття 49 (1).

якщо «передача є не систематичною та необхідною»[709] в контексті договору чи правової претензії.

Крім того, згідно з рекомендаціями Робочої групи «Стаття 29» посилання на відступи мають бути винятковими, стосуватись окремих ситуацій та не використовуватися для масових чи повторюваних передач[710]. Європейський інспектор із захисту персональних даних також підкреслив винятковий характер відступів, які використовуються як законна підстава передачі відповідно до Регламенту 45/2001, зазначивши, що таке рішення має застосовуватися «в обмежених випадках» та «для несистематичних передач»[711].

Приклад: сервісна компанія «Глобальна дистрибуційна система» (ГДС) із штаб-квартирою в США забезпечує систему онлайн-бронювань для великої кількості авіакомпаній, готелів і круїзів по всьому світу, обробляючи персональні дані десятків мільйонів осіб з ЄС. На початковій стадії передачі даних до серверів у США компанія ГДС посилається на відступ як законну підставу обробки у зв'язку з необхідністю укладення угоди. Таким чином, вона не надає будь-яких інших гарантій для персональних даних з Європи, переданих до США, а потім перерозподілених серед готелів у всьому світі (тобто жодних гарантій для подальших передач також). Компанія ГДС не дотримується вимог ЗРЗПД щодо законної міжнародної передачі даних, оскільки покладається на відступ як на законну підставу для масових передач.

За відсутності рішення про відповідність ЄС або його держави-члени мають повноваження встановлювати обмеження передачі спеціальних категорій даних до третьої країни в суспільних інтересах, незважаючи на наявність інших умов для такої передачі. Такі обмеження мають сприйматися як виняткові, а держави-члени зобов'язані надсилати відповідні положення до Комісії[712].

709 Там само, стаття 49 (1).

710 Робоча група «Стаття 29» (2005), *Робочий документ щодо загального тлумачення статті 26 (1) Директиви 95/46/ЄС95/46/ЄС від 24 жовтня 1995*, РГ 114, Брюссель, від 25 листопада 2005р.

711 Європейський інспектор із захисту персональних даних, *Передача персональних даних до третіх країн та міжнародних організацій інституціями та органами ЄС*, Довідка, Брюссель, від 14 липня 2014 р., п. 15.

712 Див. Загальний регламент захисту персональних даних, стаття 49 (5), особливо *Робочий документ* Робочої групи «Стаття 29» *щодо загального тлумачення статті 26 (1) Директиви 95/46/ЄС95/46/ЄС від 24 жовтня 1995*, РГ 114, Брюссель, від 25 листопада 2005 р.

Право РЄ дозволяє здійснювати рух даних до територій, які не мають належного захисту персональних даних у випадку, якщо:

- суб'єкт даних надав згоду;
- така передача необхідна в інтересах суб'єкта даних;
- наявні переважні легітимні інтереси, зокрема, важливі суспільні інтереси, передбачені законом;
- це є необхідним і пропорційним заходом у демократичному суспільстві[713].

7.3.4 Передача на підставі міжнародних договорів

ЄС може укладати міжнародні договори з третіми країнами, які регулюють передачу персональних даних для конкретних цілей. Такі договори мають включати належні гарантії для забезпечення захисту персональних даних відповідних осіб. ЗРЗПД діє, не завдаючи шкоди таким міжнародним угодам[714].

Держави-члени можуть також укладати міжнародні угоди з третіми країнами чи міжнародними організаціями, які забезпечують належний рівень захисту основних прав і свобод фізичних осіб, тією мірою, якою такі угоди не впливають на застосування ЗРЗПД.

Подібне правило передбачене у статті 12 (3) (a) Оновленої Конвенції 108.

Прикладами міжнародних договорів, що стосуються передачі персональних даних, є угоди про реєстраційні дані пасажирів (PNR; РДП).

Реєстраційні дані пасажирів

Реєстраційні дані пасажирів (РДП) збираються авіаперевізниками в процесі резервування та містять, серед іншого, прізвища, адреси, дані кредитних карток та номери посадкових місць авіапасажирів. Авіаперевізники збирають цю інформацію також задля власних комерційних цілей. ЄС уклав договори з окремими третіми країнами (Австралією, Канадою та США) щодо передачі РДП для запобігання, виявлення, розслідування та переслідування тероризму чи тяжких транснаціональних злочинів. Більше того, у 2016 році ЄС ухвалив

713 Оновлена Конвенція 108, стаття 14 (4).

714 Загальний регламент захисту персональних даних, п. 102 преамбули.

Директиву (ЄС) 2016/861, відому як Директива ЄС-РДП (the EU-PNR Directive)[715]. Ця Директива передбачає правове регулювання для держав-членів ЄС стосовно передачі РДП до компетентних органів у третіх країнах з такою ж метою запобігання, виявлення, розслідування та переслідування тероризму та тяжких злочинів. Передача РДП до органів третьої країни здійснюється в кожному конкретному випадку та підлягає окремій оцінці щодо її необхідності в цілях, визначених у Директиві, за умови дотримання основних прав.

Щодо РДП договорів між ЄС та третіми країнами, їхня сумісність з основними правами на приватність та захист персональних даних, закріплених у Хартії основних прав ЄС, була оскаржена. Коли у 2014 році після проведення переговорів з Канадою ЄС підписав угоду про передачу та обробку РДП, Європейський Парламент вирішив звернутися до Суду ЄС по оцінку законності угоди по відношенню до законодавства ЄС, зокрема статті 7 та 8 Хартії.

Приклад: у своєму висновку щодо законності угоди про РДП між ЄС та Канадою[716] Суд ЄС постановив, що в чинній формі угода, що передбачалася, є несумісною з основоположними правами, визнаними Хартією, і, відповідно, не може бути укладеною. Оскільки угода стосувалась обробки персональних даних, вона становила втручання у право на захист персональних даних, що захищається статтею 8 Хартії. Водночас вона обмежує право на повагу до приватного життя, закріплене у статті 7, враховуючи, що в цілому РДП можуть бути узагальнені та проаналізовані в такий спосіб, який розкриє інформацію про звички подорожування, відносини між різними особами, інформацію про їхній майновий стан, звички харчування та стан здоров'я, таким чином, зазіхаючи на їхнє приватне життя.

Втручання в основні права, яке передбачала запланована угода, переслідувало мету загального інтересу, а саме громадську безпеку та боротьбу з тероризмом та небезпечною транснаціональною злочинністю. Однак Суд ЄС нагадав, що для того, щоб бути виправданим, втручання повинне зводитися до тієї міри, яка є вкрай необхідною для досягнення мети. Проаналізувавши положення запланованої угоди, Суд ЄС вирішив, що вона не відповідає критерію «крайньої необхідності». Серед факторів, які Суд ЄС взяв до уваги, щоб дійти такого висновку, були:

715 *Директива (ЄС) 2016/681* Європейського Парламенту і Ради від 27 квітня 2016 р. про використання відомостей записів реєстрації пасажирів (РДП; PNR) для запобігання, виявлення, розслідування та переслідування тероризму та тяжких злочинів, OJ 2016 L 119.

716 Суд ЄС, *Висновок Суду (Велика Палата)*, від 26 липня 2017 р.

- Той факт, що запланована угода передбачала передачу чутливих персональних даних. РДП, які збиралися відповідно до запланованої угоди, могли містити чутливі дані, наприклад інформацію щодо расової чи етнічної належності, релігійних переконань чи стану здоров'я пасажира. Передача та обробка канадськими органами влади чутливих даних може нести ризик для принципу недискримінації, а отже вимагає точного та серйозного обґрунтування на інших засадах, аніж громадська безпека та боротьба з серйозними злочинами. Запланованою угодою такого обґрунтування надано не було[717].

- Тривале зберігання РДП про всіх пасажирів (протягом 5 років), навіть після від'їзду пасажирів з Канади, також вважалося перевищенням меж крайньої необхідності. Суд ЄС вважав допустимим зберігання канадськими органами влади даних про пасажирів, навіть після їхнього виїзду з Канади, якщо відносно них наявні об'єктивні докази, що вони можуть становити загрозу громадській безпеці. На відміну від цього, зберігання персональних даних *усіх* пасажирів, щодо яких відсутні навіть непрямі докази стосовно ризиків загрози для громадської безпеки з їхнього боку, не є виправданим[718].

Консультативний Комітет Конвенції 108 надав висновок щодо наслідків угод РДП для захисту персональних даних відповідно до права РЄ[719].

Дані щодо передачі повідомлень

Товариство Міжнародної міжбанківської системи передачі інформації та здійснення платежів (SWIFT), яке розташоване в Бельгії та є оператором з обробки даних більшості світових грошових переказів європейських банків, співпрацювало з «дзеркальним» центром у США і зіткнулося з проханням

717 Там само, п. 165.

718 Там само, пп. 204–207.

719 Рада Європи, *Висновок щодо наслідків обробки реєстраційних даних пасажирів для захисту персональних даних* , T-PD(2016)18rev, від 19 серпня 2016 р.

розкрити дані Департаменту фінансів США для проведення розслідування тероризму за програмою відстеження фінансування тероризму[720].

З точки зору ЄС, не було достатньої правової підстави для розкриття цих даних (здебільшого громадян ЄС) Сполученим Штатам лише тому, що там розташовувався один з центрів обробки даних системи SWIFT.

В 2010 році з метою встановлення необхідної правової підстави і забезпечення відповідних стандартів захисту персональних даних між ЄС і США було укладено спеціальну угоду, відому як «SWIFT-угода»[721].

У рамках цієї угоди фінансові дані, що зберігаються системою SWIFT, продовжують надаватися Департаменту фінансів США з метою запобігання, розслідування, виявлення або переслідування тероризму та його фінансування. Департамент фінансів США може надати запит до системи SWIFT щодо надання йому фінансових даних за умови, що цей запит:

- якомога чіткіше ідентифікує фінансові дані;
- чітко обґрунтовує необхідність цих даних;
- сформульований якомога більш вузько, щоб звести до мінімуму обсяг запитуваних даних;
- не вимагає жодних даних стосовно Єдиної європейської платіжної системи (SEPA; ЄЄПС)[722].

Європол повинен отримувати копію кожного запиту Департаменту фінансів США і перевіряти, чи дотримано в ньому принципів SWIFT-угоди[723]. Якщо підтвердиться, що їх було дотримано, система SWIFT повинна надати фінансові дані безпосередньо Департаменту фінансів США. Департамент має зберігати фінансові дані в захищеному фізичному середовищі, де вони будуть доступними лише аналітикам, які розслідують тероризм або його фінансування; фінансові дані не повинні

720 Див., у цьому контексті, Робоча група «Стаття 29» (2011), *Висновок 14/2011 щодо питань захисту персональних даних, пов'язаних з протидією відмиванню коштів та фінансуванню тероризму*, РГ 186, Брюссель, від 13 червня 2011 р.; Робоча група «Стаття 29» (2006), *Висновок 10/2006 щодо обробки персональних даних Товариством Міжнародної міжбанківської системи передачі інформації та здійснення платежів (SWIFT)*, РГ 128, Брюссель, від 22 листопада 2006 р.; Комісія із захисту приватності Бельгії (*Commission de la protection de la vie privée*) (2008), *'Процедура контролю та рекомендацій, розпочата відносно компанії SWIFT scrl'*, Рішення, від 09 грудня 2008 р.

721 Рішення Ради 2010/412/EU від 13 липня 2010 р. про укладення Угоди між Європейським Союзом та Сполученими Штатами Америки про обробку та передачу даних фінансових повідомлень з Європейського Союзу до Сполучених Штатів для цілей Програми відстеження фінансування тероризму, OJ 2010 L 195, пп. 3 та 4. Текст угоди додається до цього рішення, OJ 2010 L 195, пп. 5–14.

722 Там само; стаття 4 (2).

723 Об'єднаний наглядовий орган Європолу *провів аудити такої діяльності Європолу.*

бути поєднані з будь-якими іншими базами даних. Загалом отримані від системи SWIFT фінансові дані повинні видалятися не пізніше ніж через п'ять років з моменту їх отримання. Фінансові дані, які мають відношення до особливих розслідувань або судових переслідувань, можуть зберігатися доти, доки вони є необхідними для цих розслідувань або судових переслідувань

Департамент фінансів США може передавати інформацію про дані, отримані від системи SWIFT, конкретним правоохоронним органам, органам державної безпеки або боротьби з тероризмом у межах чи за межами США 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 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 безпеці громадського порядку.

За дотриманням принципів SWIFT-угоди стежать незалежні наглядачі, в тому числі особа, призначена Європейською комісією. Вони можуть переглядати пошукові запити щодо наданих даних, як у реальному часі, так і за попередні періоди, вимагати додаткову інформацію для обґрунтування зв'язку таких запитів з тероризмом, а також мають повноваження заблокувати будь-який чи всі запити, які виявляються такими, що порушують передбачені угодою гарантії.

Суб'єкти персональних даних мають право отримувати від компетентного контролюючого органу ЄС підтвердження того, що їхні права на захист персональних даних було дотримано. Відповідно до SWIFT-угоди суб'єкти персональних даних також мають право на виправлення, видалення чи блокування своїх даних, які зібрав та зберігає Департамент фінансів США. Проте право суб'єктів персональних даних на доступ може підлягати певним правовим обмеженням. Якщо суб'єкту персональних даних було відмовлено в доступі, його має бути поінформовано в письмовій формі про відмову та про його право на відшкодування в адміністративному і судовому порядку в США.

SWIFT-угода є чинною протягом п'яти років, перший строк її дії тривав до серпня 2015 року. Вона автоматично продовжується на один рік, якщо одна зі сторін принаймні за шість місяців не повідомить іншу про свій намір не продовжувати угоду. Автоматичне продовження дії застосовувалось у серпні 2015, 2016 та 2017 років та забезпечує чинність SWIFT-угоди не менш ніж до серпня 2018 року[724].

724 Там само; стаття 23 (2).

8

Захист персональних даних у контексті діяльності поліції та органів кримінальної юстиції

ЄС	Питання, що висвітлюються	РЄ
Директива про захист персональних даних для поліції та органів кримінальної юстиції	**Загальні питання**	Оновлена Конвенція 108
	Поліція	*Рекомендація щодо використання персональних даних поліцією* *Практичний посібник з використання персональних даних у роботі поліції*
	Стеження	ЄСПЛ, «Б. Б. проти Франції», (*B. B. v. France*), № 5335/06, 2009 ЄСПЛ, «С. та Марпер проти Сполученого Королівства» (*S. and Marper v. the United Kingdom*) (ВП), № 30562/04 і 30566/04, 2008 ЄСПЛ, «Аллан проти Сполученого Королівства» (*Allan v. the United Kingdom*), № 48539/99, 2002

ЄС	Питання, що висвітлюються	РЄ
		ЄСПЛ, «Мелоун проти Сполученого Королівства» *(Malone v. the United Kingdom)*, № 8691/79, 1984 ЄСПЛ, «Класс та інші проти Німеччини» *(Klass and Others v. Germany)* № 5029/71, 1978 ЄСПЛ, «Сабо та Віші проти Угорщини» *(Szabó and Vissy v. Hungary)*,№ 37138/14, 2016 ЄСПЛ, «Веттер проти Франції» *(Vetter v. France)*, № 59842/00, 2005
	Кіберзлочинність	*Конвенція про кіберзлочинність*
Інші спеціальні правові інструменти		
Прюмське рішення	**Стосовно спеціальних даних: відбитки пальців, ДНК, хуліганство, інформація щодо авіапасажирів, дані про телекомунікації тощо.**	Оновлена Конвенція 108, стаття 6 Рекомендація щодо використання персональних даних поліцією, *Практичний посібник з використання персональних даних у роботі поліції*
Шведська ініціатива (Рамкове рішення Ради 2006/960/ЮНА)	**Спрощення обміну інформації та розвідданими між правоохоронними органами**	ЄСПЛ, «С. та Марпер проти Сполученого Королівства» *(S. and Marper v. the United Kingdom)* [ВП], № 30562/04 та 30566/04, 2008
Директива (ЄС) 2016/681 про використання реєстраційних даних пасажирів (РДП) для запобігання, виявлення, розслідування та переслідування за вчинення терористичних актів та серйозних злочинів	**Збереження персональних даних**	ЄСПЛ, «Б. Б. проти Франції» *(B. B. v. France)*, № 5335/06, 2009

ЄС	Питання, що висвітлюються	РЄ
СЄС, об'єднані справи C-293/12 та C-594/12, «"Digital Rights Ireland Ltd." проти Міністра зв'язку, морських та природних ресурсів та інших та Земельний уряд Каринтії та інші» (*Digital Rights Ireland and Kärntner Landesregierung and Others*) [ВП], 2014 СЄС, об'єднані справи C-203/15 та C-698/15, «"Tele2 Sverige AB" проти Державного управління зв'язку та телекомунікації» та «Секретар внутрішніх справ проти Тома Вотсона та інших» (*Tele2 Sverige and Home Department v. Tom Watson and Others*) [ВП], 2016		
Регламент Європолу Рішення про Євроюст	**Спеціальні агенції**	Рекомендація щодо використання персональних даних поліцією
Рішення про ШІС II *Регламент ВІС* *Регламент щодо системи Eurodac* *Рішення про МІС*	**Спеціальні спільні інформаційні системи**	Рекомендація щодо використання персональних даних поліцією ЄСПЛ, «Даля проти Франції» (*Dalea v. France*), № 964/07, 2010

Щоб збалансувати інтереси окремої особи щодо захисту даних та інтереси суспільства щодо збирання даних для боротьби зі злочинністю та забезпечення національної та громадської безпеки, РЄ та ЄС прийняли спеціальні правові інструменти. Ця глава містить огляд права РЄ (розділ 8.1) та ЄС (розділ 8.2) щодо захисту даних у діяльності поліції та органів кримінальної юстиції.

8.1 Право РЄ про захист даних і національну безпеку, поліцію та питання кримінальної юстиції

Ключові моменти

- Оновлена Конвенція 108 та Рекомендація РЄ щодо використання персональних даних поліцією застосовуються до захисту даних у всіх сферах роботи поліції.
- Конвенція про кіберзлочинність (Будапештська конвенція) є зобов'язальним міжнародно-правовим документом, що стосується боротьби зі злочинами, вчиненими проти і за допомогою електронних мереж. Вона також стосується розслідування некіберзлочинів, де фігурують електронні докази.

Важлива різниця між правом РЄ та ЄС полягає в тому, що **право РЄ** на противагу праву ЄС також застосовується у сфері національної безпеки. Це означає, що Договірні Сторони повинні дотримуватися статті 8 ЄКПЛ навіть у діяльності, пов'язаній з національною безпекою. Декілька рішень ЄСПЛ стосуються діяльності держави в чутливих сферах права та правозастосування в царині національної безпеки[725].

Щодо поліції та питань кримінальної юстиції на європейському рівні Оновлена Конвенція 108 охоплює всі сфери обробки персональних даних, а її положення спрямовані на регулювання обробки персональних даних загалом. Таким чином, Оновлена Конвенція 108 застосовується до захисту персональних даних у сферах поліції та кримінальної юстиції. Обробка генетичних даних, персональних даних стосовно вчинення правопорушень, кримінальних проваджень і засуджень, а також будь-яких заходів, пов'язаних з безпекою, біометричних даних, які однозначно ідентифікують особу, та чутливих персональних даних дозволяється лише за наявності належних гарантій запобігання ризикам, які може нести така обробка для інтересів, прав та основоположних свобод суб'єкта; зокрема ризику дискримінації[726].

725 Див., наприклад, рішення ЄСПЛ у справі «Класс та інші проти Німеччини» (*Klass and Others v. Germany*), № 5029/71, від 6 вересня 1978 р.; рішення ЄСПЛ у справі «Ротару проти Румунії» (*Rotaru v. Romania*) [ВП], № 28341/95, від 4 травня 2000 р. та рішення ЄСПЛ у справі «Сабо та Віші проти Угорщини» (*Szabó and Vissy v. Hungary*), № 37138/14, від 12 січня 2016 р.

726 Оновлена Конвенція 108, стаття 6.

Правові завдання поліції та кримінальної юстиції часто вимагають обробки персональних даних, які можуть мати серйозні наслідки для зацікавлених осіб. Рекомендація щодо використання персональних даних поліцією, прийнята РЄ 1987 року, дає настанови державам-членам РЄ про те, як вони мають дотримуватися принципів Конвенції 108 у контексті обробки персональних даних органами поліції[727]. Рекомендація була посилена Практичним посібником з використання персональних даних у роботі поліції, прийнятим Консультативним Комітетом Конвенції 108[728].

Приклад: у справі «*D. Л. проти Болгарії*»[729] соціальна служба помістила заявника до освітнього закладу закритого типу на підставі рішення суду. Письмова кореспонденція та телефонне спілкування в повному обсязі без винятків відстежувались установою. ЄСПЛ вирішив, що статтю 8 було порушено, оскільки такі заходи не були необхідними в демократичному суспільстві. Суд вказав, що має бути зроблено все для того, щоб уможливити ефективний контакт неповнолітніх, вміщених до установи, з зовнішнім світом, оскільки це було невід'ємною частиною їхнього права на гідне ставлення та вкрай важливим у підготовці їхньої інтеграції в суспільство. Це також стосується побачень та листування або телефонного спілкування. Крім того, стеження здійснювалося під час спілкування заявника з членами сім'ї, представниками ГО, які представляли права дитини, та адвокатами. Більше того, рішення відстежувати спілкування не ґрунтувалося на індивідуалізованому аналізі ризиків у кожній окремій справі.

Приклад: у справі «*Драгоєвич проти Хорватії*»[730] заявника підозрювали у причетності до торгівлі наркотиками. Його було визнано винним після того, як слідчий суддя дозволив застосування заходів прихованого стеження у вигляді перехоплення телефонних дзвінків заявника. ЄСПЛ вирішив, що заходи, щодо яких було подано скаргу, становлять втручання у право на повагу до приватного життя та кореспонденції. Дозвіл, наданий слідчим суддею, ґрунтувався просто на твердженні прокуратури про те, що «розслідування не могло здійснюватись іншим чином». ЄСПЛ також

727 Рада Європи, Комітет міністрів (1987), Рекомендація Rec(87)15 державам-членам, яка регулює використання персональних даних у роботі поліції, 17 вересня 1987 р.

728 Рада Європи *(2018), Консультативний Комітет Конвенції 108, Практичний посібник про використання персональних даних у роботі поліції* T-PD(2018)1.

729 Рішення ЄСПЛ у справі «Д. Л. проти Болгарії» (*D. L. v. Bulgaria*), № 7472/14, від 19 травня 2016 р.

730 Рішення ЄСПЛ у справі «*Драгоєвич проти Хорватії*» (*Dragojević v. Croatia*), № 68955/11, від 15 січня 2015 р.

зазначив, що кримінальні суди обмежили свою оцінку щодо використання заходів стеження, і що уряд не надав інформації про інші можливі заходи. Відповідно, стаття 8 була порушена.

8.1.1 Рекомендація щодо використання персональних даних поліцією

ЄСПЛ постійно вказує, що збереження та утримання персональних даних поліцією та національними органами безпеки становить втручання в права, гарантовані п. 1 статті 8 ЄКПЛ. Багато рішень ЄСПЛ стосуються питань обґрунтування такого втручання[731].

Приклад: у справі «*Б. Б. проти Франції*» [732] заявник був засуджений за вчинення сексуальних злочинів проти 15-річних неповнолітніх, довіреною особою яких він був. Він відбув покарання у 2000 році. Через рік він звернувся з вимогою, щоб запис про його покарання було вилучено з його кримінального досьє, однак вимогу було відхилено. 2004 року у Франції було ухвалено закон про запровадження національної судової бази даних про осіб, які вчинили злочини сексуального характеру, і заявника було поінформовано про включення його до цієї бази. ЄСПЛ вирішив, що включення засуджених за злочини сексуального характеру в національну судову базу даних підпадає під дію статті 8 ЄКПЛ. Однак, враховуючи наявність достатніх гарантій захисту даних, таких як право суб'єкта даних вимагати видалення даних, обмежений період зберігання даних та обмежений доступ до таких даних, справедливий баланс між конкурентними приватними та відповідними суспільними інтересами було встановлено. Суд дійшов висновку, що в цій справі порушення статті 8 ЄКПЛ не було.

Приклад: у справі «*С. та Марпер проти Сполученого Королівства*»[733] обидва заявники були обвинувачені у вчиненні злочинів але не засуджені.

731 Див., наприклад, рішення ЄСПЛ у справі «Леандер проти Швеції» (*Leander v. Sweden*), № 9248/81, від 26 березня 1987 р.; рішення ЄСПЛ у справі «М. М. проти Сполученого Королівства» (*M. M. v. the United Kingdom*), № 24029/07, від 13 листопада 2012 р.; рішення ЄСПЛ у справі «М. К. проти Франції» (*M. K. v. France*), № 19522/09, від 18 квітня 2013 р., або рішення ЄСПЛ у справі «Ейкагі проти Франції» (*Aycaguer v. France*), № 8806/12, від 22 червня 2017 р.

732 Рішення ЄСПЛ у справі «Б. Б. проти Франції» (*B.B. v. France*), № 5335/06, від 17 грудня 2009 р.

733 Рішення ЄСПЛ у справі «С. та Марпер проти Сполученого Королівства» (*S. and Marper v. the United Kingdom*) [ВП], №№ 30562/04 та 30566/04, від 4 грудня 2008 р., пп. 119 та 125.

Втім, їхні відбитки пальців, зразки клітин та профілів ДНК були відібрані та зберігались поліцією. Необмежене зберігання вказаних біометричних даних дозволене законом, якщо особа підозрювалась у вчиненні правопорушення, навіть якщо підозрюваний був пізніше виправданий або справа проти нього закрита. ЄСПЛ вирішив, що всеосяжний і нерозбірливий характер зберігання персональних даних, який не був обмеженим в часі та надавав виправданим особам незначні можливості вимагати вилучення даних, становив непропорційне втручання в право заявників на повагу до приватного життя. Суд дійшов висновку, що мало місце порушення статті 8 ЄКПЛ.

Принципово важливим питанням у контексті електронної комунікації є втручання державних органів у право на приватність та право на захист даних. Засоби стеження та перехоплення спілкування, як-от пристрої для прослуховування або запису, дозволені, лише якщо це передбачено законом та якщо вони є необхідними в демократичному суспільстві в інтересах:

- захисту безпеки держави;
- громадської безпеки;
- грошових інтересів держави;
- припинення кримінальних правопорушень;
- захисту суб'єкта даних або прав і свобод інших осіб.

Багато наступних рішень ЄСПЛ стосуються обґрунтування втручання у право на приватність у формі стеження.

Приклад: у справі *«Аллан проти Сполученого Королівства»*[734] органи влади таємно записували приватну розмову ув'язненого з другом у приміщенні в'язниці для побачень та із співобвинуваченим у камері. ЄСПЛ вирішив, що використання аудіо- та відеозаписувальних приладів у камері заявника, у приміщенні для побачень і на співкамернику прирівнюється до втручання у право заявника на повагу до приватного життя. Таке втручання не було визнано законним, оскільки на той час не існувало законодавчого регулювання правил використання поліцією

734 Рішення ЄСПЛ у справі *«Аллан проти Сполученого Королівства»* (*Allan v. the United Kingdom*), № 48539/99, від 5 листопада 2002 р.

прихованих записувальних пристроїв. Суд дійшов висновку, що мало місце порушення статті 8 ЄКПЛ.

Приклад: у справі *«Роман Захаров проти Росії»*[735] заявник ініціював судове провадження проти трьох операторів мобільних мереж. Він стверджував, що його право на приватне телефонне спілкування було порушено, оскільки оператори встановили обладнання, яке дозволяло Федеральній службі безпеки перехоплювати його телефонне спілкування без попереднього судового дозволу. ЄСПЛ вирішив, що національні законодавчі положення, що регулювали перехоплення спілкування, не надавали адекватних та ефективних гарантій проти свавілля та ризику зловживання. Зокрема, національний закон не вимагає видалення даних після досягнення мети їх зберігання. Більше того, навіть якщо судовий дозвіл був потрібний, судовий контроль був обмеженим.

Приклад: у справі *«Сабо та Віші проти Угорщини»*[736] заявник скаржився, що законодавство Угорщини порушувало статтю 8 ЄКПЛ, оскільки воно не було належним чином деталізованим і точним. Крім того, стверджувалося, що законодавство не надавало належних гарантій проти зловживання та свавілля. ЄСПЛ вирішив, що угорський закон не передбачав попереднього судового дозволу для стеження за особою. Суд зазначив, що хоча стеження мало бути погоджене міністром юстиції, такий контроль мав суто політичний характер та не забезпечував проведення аналізу для виявлення «крайньої необхідності». Більше того, національний закон не передбачав судового перегляду, оскільки ніяких повідомлень суб'єкту даних не надсилалося. Суд дійшов висновку, що мало місце порушення статті 8 ЄКПЛ.

Оскільки обробка даних поліцейськими органами може мати значний вплив на зацікавлених осіб, у цій сфері особливо необхідні деталізовані правила захисту щодо обробки персональних даних. Рекомендація РЄ стосовно використання персональних даних поліцією має на меті врегулювати це питання шляхом надання настанов щодо того, як саме мають збиратися персональні дані в ході діяльності поліції; як файли з даними в цій сфері мають

735 Рішення ЄСПЛ у справі «*Роман Захаров проти Росії*» (*Roman Zakharov v. Russia*), № 47143/06, від 4 грудня 2015 р.

736 Рішення ЄСПЛ у справі «*Сабо та Віші проти Угорщини*» (*Szabó and Vissy v. Hungary*), № 37138/14, від 12 січня 2016 р.

зберігатися; кому дозволяється мати доступ до цих файлів, включаючи умови передачі персональних даних поліцейським органам інших держав; як суб'єкт даних може реалізовувати свої права на захист персональних даних; та яким чином має здійснюватися контроль незалежним наглядовим органом. Також розглядається питання щодо того, як має бути забезпечений захист даних. Рекомендація не передбачає необмеженого та нерозбірливого збирання персональних даних поліцейськими органами. Вона обмежує збір персональних даних поліцейськими органами тими, які необхідні для попередження реальної небезпеки або переслідування за конкретне кримінальне правопорушення. Будь-який збір додаткових даних мав би ґрунтуватися на спеціальному національному законодавстві. Обробка чутливих даних має бути обмежена тими, які абсолютно необхідні в контексті конкретного слідства.

Якщо персональні дані збираються без відома суб'єкта даних, його має бути повідомлено про збір, як тільки таке відкриття більше не перешкоджає розслідуванню. Збір даних за допомогою технічних засобів стеження або інших автоматичних засобів повинен відбуватися на спеціальних юридичних засадах.

Приклад: у справі «*Версіні-Кампінкі та Краснянскі проти Франції*»[737] заявниця, адвокатка, мала телефонну розмову з клієнтом, чий телефон прослуховувався на підставі рішення слідчого судді. Розшифровка розмови демонструвала, що вона відкрила інформацію, яка захищалася адвокатською таємницею. Прокурор надіслав цю інформацію до Ради адвокатури, яка наклала на заявницю покарання. ЄСПЛ визнав наявність втручання у право на повагу до приватного життя та кореспонденції не лише тієї особи, чиї телефоні розмови записувались, але також й заявниці, чия розмова була перехоплена та стенографована. Втручання було здійснено відповідно до закону та переслідувало легітимну мету запобігання порушенню правопорядку. Заявниця отримала можливість перегляду питання щодо законності передання стенограми записаної телефонної розмови в контексті дисциплінарного провадження проти неї. Хоча заявниця не домоглася, щоб стенограму телефонної розмови було знищено, ЄСПЛ вирішив, що існував ефективний контроль, здатний обмежити втручання, яке оскаржувалося, до міри, яка була необхідною в демократичному суспільстві. ЄСПЛ визнав, що аргумент з приводу того, що можливість кримінального провадження проти адвокатки на підставі

737 Рішення ЄСПЛ у справі «*Версіні-Кампінкі та Краснянскі проти Франції*» (*Versini-Campinchi and Crasnianski v. France*), № 49176/11, від 16 червня 2016 р.

стенограми міг мати охолоджуючий вплив на свободу спілкування між адвокатом та клієнтом і, відповідно, на права останнього на захист, не є виправданим у випадку, якщо відкриття, здійснене самою адвокаткою, може становити неправомірну поведінку з її боку. Відповідно, порушення статті 8 встановлено не було.

Рекомендація щодо використання персональних даних поліцією передбачає, що при зберіганні персональних даних має бути чітке розділення між адміністративними даними та даними поліції; персональними даними різних видів суб'єктів даних, наприклад підозрюваних, засуджених осіб, потерпілих та свідків; а також між даними, які є достовірними фактами, та тими, які ґрунтуються на підозрах або припущеннях.

Мета використання поліцейських даних має бути чітко визначена. Це впливає на повідомлення поліцейських даних третім особам: передача або повідомлення таких даних у сфері діяльності поліції повинні визначатися тим, чи існує легітимний 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.

Приклад: у справі *«Карабейоглу проти Туреччини»*[738] телефонні лінії заявника, судді, перебували під моніторингом у ході кримінального розслідування щодо незаконної організації, у якій його підозрювали в участі або в наданні їй допомоги та підтримки. Після прийняття рішення про припинення розслідування відповідальний за нього прокурор знищив відповідні записи. Однак копії записів залишились у судових слідчих, які згодом використали відповідний матеріал у контексті дисциплінарного розслідування проти заявника. ЄСПЛ вирішив, що відповідне законодавство було порушено, оскільки інформація була використана для цілей, інших ніж ті, в яких вона збиралася, та не була знищена в передбачені строки. Втручання у право заявника на повагу до приватного життя не відповідало закону в тому, що стосувалося дисциплінарного провадження проти нього.

Міжнародна передача або відкриття даних мають обмежуватися лише іноземними органами поліції та ґрунтуватися на спеціальних законодавчих

738 Рішення ЄСПЛ у справі «Карабейоглу проти Туреччини» (*Karabeyoğlu v. Turkey*), № 30083/10, від 7 червня 2016 р.

положеннях, можливо, на міжнародних договорах, хіба що це необхідно для попередження очікуваної серйозної небезпеки.

Обробка даних поліцією має підлягати незалежному контролю для забезпечення дотримання національного законодавства із захисту персональних даних. Суб'єкти даних повинні мати всі права щодо доступу, які передбачено Оновленою Конвенцією 108. Якщо права суб'єкта даних на доступ обмежуються відповідно до статті 9 Конвенції 108 в інтересах ефективного поліцейського розслідування та виконання кримінальних покарань, суб'єкт даних повинен мати право за національним законом оскаржувати це до національного наглядового органу або до іншого незалежного органу.

8.1.2 Будапештська конвенція про кіберзлочинність

Оскільки в ході злочинної діяльності зловмисники все частіше вдаються до використання електронних систем обробки даних і впливають на їхню 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[739]. До цієї Конвенції також можуть приєднуватися держави, які не є членами Ради Європи, і станом на початок 2018 року сторонами Конвенції були 14 держав за межами РЄ, а сім інших держав, нечленів РЄ, були запрошені до приєднання[740].

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 у контексті боротьби з

739 Рада Європи, Комітет міністрів (2001), Конвенція про кіберзлочинність, CETS № 185, Будапешт, 23 листопада 2001 р., набула чинності 1 липня 2004 р.

740 Австралія, Канада, Чілі, Колумбія, Домініканська Республіка, Ізраїль, Японія, Маврікій, Панама, Сенегал, Шрі-Ланка, Тонга, Туніс та Сполучені Штати. Див. Підписи та ратифікація Договору 185, станом на липень 2017р. (*Chart of signatures and ratifications of Treaty 185, status as of July 2017*).

кіберзлочинністю. Нарешті, вона створює можливості для ефективного міжнародного співробітництва. Додатковий протокол до Конвенції стосується питання криміналізації пропаганди расизму та ксенофобії в 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. Більше того, вона зобов'язує держави-учасниці запровадити законодавчі заходи для надання можливості їхнім національним органам перехоплювати трафік та зміст даних[741]. Вона також зобов'язує Договірні Сторони передбачити при виконанні Конвенції належний рівень захисту прав і свобод людини, у тому числі таких прав, гарантованих ЄКПЛ, як право на захист персональних даних[742]. Договірні Сторони не зобов'язані приєднуватися до Конвенції 108 для того, щоб приєднатися до Будапештської Конвенції про кіберзлочинність.

8.2 Право ЄС щодо захисту персональних даних у сфері діяльності поліції та органів кримінальної юстиції

Ключові моменти

- На рівні ЄС захист персональних даних у секторі поліції та кримінальної юстиції регулюється в контексті як національної, так і транскордонної обробки поліцією і органами кримінальної юстиції держав-сторін, так й діючих суб'єктів ЄС.
- На рівні держав-учасниць Директива про захист персональних даних для поліції та органів кримінальної юстиції потребує імплементації в національне законодавство.
- Існують спеціальні режими захисту даних у діяльності поліції та транскордонній співпраці правоохоронних органів, особливо у сфері боротьби з тероризмом та транснаціональними злочинами.
- Існують спеціальні режими захисту даних для Європейського поліцейського управління (Європол), Європейського бюро судової співпраці (Євроюст) та

741 Рада Європи, Комітет міністрів (2001), Конвенція про кіберзлочинність, CETS № 185, Будапешт, 23 листопада 2001 р., статті 20 та 21.

742 Там само., стаття 15 (1).

новоствореної Європейської прокуратури, які є органами ЄС, що допомагають і сприяють транскордонному правозастосуванню.

- 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. Такими прикладами є Шенгенська інформаційна система II (SIS II), Візова інформаційна система (VIC) і Євродак, централізована система, що містить дані про відбитки пальців громадян третіх країн, які шукають притулку в одній з держав-членів ЄС.
- ЄС наразі знаходиться в процесі оновлення вказаних вище положень щодо захисту даних з тим, щоб вони відповідали положенням Директиви про захист персональних даних для поліції та органів кримінальної юстиції.

8.2.1 Директива про захист персональних даних для поліції та органів кримінальної юстиції

Директива 2016/680/ЕС про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами влади в цілях попередження, розслідування, виявлення кримінальних правопорушень та притягнення до відповідальності за їх вчинення або виконання кримінальних покарань та про вільне переміщення таких даних (Директива про захист персональних даних для поліції та органів кримінальної юстиції)[743] спрямована на захист персональних даних, зібраних та підданих обробці для цілей кримінального правосуддя, включаючи:

- попередження, розслідування, виявлення або переслідування за кримінальні правопорушення або виконання кримінальних покарань, включаючи боротьбу з загрозами громадській безпеці та їх запобіганню;
- виконання кримінальних покарань;
- справи, у яких поліція або інші правоохоронні органи діють для підтримки закону та захисту від загроз громадській безпеці та засадничим правам суспільства, які можуть становити кримінальне правопорушення, а також запобігання таким загрозам.

743 *Директива 2016/680/ЕС* про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами влади в цілях попередження, розслідування, виявлення кримінальних правопорушень та притягнення до відповідальності за їх вчинення або виконання кримінальних покарань та про вільне переміщення таких даних та скасування Рамкового рішення Ради 2008/977/JHA, OJ 2016 L 119, p. 89 (Директива про захист персональних даних для поліції та органів кримінальної юстиції).

Директива про захист персональних даних для поліції та органів кримінальної юстиції захищає різні категорії персональних даних людей, залучених до кримінального провадження, як-от свідків, інформаторів, потерпілих, підозрюваних і співучасників. Поліція та органи кримінальної юстиції зобов'язані дотримуватися положень цієї Директиви за будь-якої обробки персональних даних у правоохоронних цілях як щодо особистого, так і матеріального обсягу Директиви[744].

Водночас використання даних з іншою метою також дозволено за певних обставин. Обробка даних для іншої правоохоронної мети, ніж та, для якої вони були зібрані, дозволена, якщо вона є легітимною, необхідною та пропорційною відповідно до національного права або права ЄС[745]. Для інших цілей застосовується Загальний регламент захисту персональних даних. Реєстрування та документування передачі даних є одним із спеціальних обов'язків компетентних органів для допомоги у визначенні відповідальності за поданими скаргами.

Компетентні органи у сфері діяльності поліції або кримінальної юстиції є державними установами або установами, які уповноважені законом або органами влади виконувати функції державних органів[746], наприклад приватні в'язниці[747]. Директива застосовується як до обробки даних на національному рівні, так і до транскордонної обробки між поліцейськими та судовими органами держав-членів, а також до міжнародної передачі даних компетентними органами до третіх країн та міжнародних організацій[748]. Вона не охоплює сферу національної безпеки або обробки персональних даних інституціями, органами, бюро та агенціями ЄС[749].

Здебільшого Директива посилається на принципи та визначення, які містяться в Загальному регламенті захисту персональних даних, враховуючи при цьому особливий характер сфери діяльності поліції та органів кримінальної юстиції. Контроль може здійснюватися тими самими органами, які здійснюють

744 Директива про захист персональних даних для поліції та органів кримінальної юстиції, стаття 2 (1).

745 Там само, стаття 4 (2).

746 Там само, стаття 3 (7).

747 Європейська Комісія (2016), Комюніке Комісії до Європейського Парламенту відповідно до статті 294 (6) Договору про функціонування Європейського Союзу щодо позиції Ради про прийняття Директиви Європейського Парламенту та Ради про захист фізичних осіб у зв'язку з обробкою персональних даних компетентними органами влади в цілях попередження, розслідування, виявлення кримінальних правопорушень та притягнення до відповідальності за їх вчинення або виконання кримінальних покарань та про вільне переміщення таких даних та скасування Рамкового рішення Ради 2008/977/JHA, COM(2016) 213 остаточна, Брюссель, від 11 квітня 2016 р.

748 Директива про захист персональних даних для поліції та органів кримінальної юстиції, розділ V.

749 Там само, стаття 2 (3).

нагляд відповідно до Загального регламенту захисту персональних даних. Призначення спеціаліста із захисту персональних даних та здійснення оцінки впливу на захист персональних даних було передбачено в Директиві як нові обов'язки поліцейських органів та органів кримінальної юстиції[750]. Хоча ця концепція походить із Загального регламенту захисту персональних даних, Директива враховує спеціальний характер сфери діяльності поліцейських органів та органів кримінальної юстиції. У порівнянні із обробкою даних в комерційних цілях, що регулюється регламентом, пов'язана з безпекою обробка може вимагати більшого рівня гнучкості. Наприклад, надання суб'єктам даних такого ж рівня захисту щодо права на інформацію, права на доступ або на вилучення їхніх персональних даних, як передбачено Загальним регламентом захисту персональних даних, може означати, що будь-яка операція зі стеження, здійснена в правоохоронних цілях, стала б неефективною в контексті правоохоронної діяльності. Таким чином, Директива не містить принципу прозорості. Подібним чином принципи мінімізації даних та обмеження цілі, які вимагають, щоб персональні дані були зведені винятково до того, що є необхідним відносно цілей обробки, та оброблялися для спеціальних та чітких цілей, також повинні застосовуватися гнучко у сфері обробки, пов'язаної із безпекою. Інформація, зібрана та збережена компетентними органами в конкретній справі, може бути визнана дуже корисною для вирішення майбутніх справ.

Принципи обробки

Директива про захист персональних даних для поліції та органів кримінальної юстиції встановлює певні базові запобіжники щодо використання персональних даних. Вона також детально пояснює принципи обробки цих даних. Держави-учасниці зобов'язані забезпечити, щоб персональні дані:

- оброблялися законно та чесно;
- збиралися для визначених, чітких та легітимних цілей та не оброблялись у спосіб, який несумісний з цими цілями;
- були адекватними, відповідними та ненадмірними відносно цілей, для яких вони обробляються;
- були точними та за потреби оновлювалися; мають вживатися достатні дії для забезпечення того, щоб персональні дані, які є неточними, враховуючи мету обробки, видалялися або виправлялися без затримки;

750 Там само, в статті 32 та статті 27, відповідно.

- зберігались у формі, яка дозволяє ідентифікацію суб'єкта даних не довше, ніж це необхідно для для цілей обробки;
- оброблялись у спосіб, який забезпечує належну безпеку персональних даних, включаючи захист від недозволеної або неправомірної обробки та від випадкової втрати, знищення або пошкодження, з використанням належних технічних та організаційних заходів[751].

Відповідно до Директиви обробка є правомірною лише тоді, коли вона здійснюється в обсязі, необхідному для виконання відповідних завдань. Більше того, вона має здійснюватися компетентним органом для досягнення цілей, визначених у Директиві, а також має ґрунтуватися на законодавстві ЄС та національному законодавстві[752]. Дані не повинні зберігатися довше, ніж необхідно, та мають бути видалені або періодично переглядатись у певні строки. Дані повинні використовуватися виключно компетентним органом та з метою, з якою вони були зібрані, передані або оприлюднені.

Права суб'єкта даних

Директива також встановлює права суб'єкта даних. Вони включають:

- Право на отримання інформації. Держави-члени повинні зобов'язати контролерів даних надавати суб'єкту даних: 1) доступ до ідентифікаційної та контактної інформації про контролера; 2) доступ до контактної інформації спеціаліста із захисту персональних даних; 3) доступ до інформації про цілі запланованої обробки; 4) право подати скаргу до наглядового органу та інформацію про його контакти; 5) право на доступ до персональних даних, на їх зміну та видалення, а також на обмеження обробки даних[753]. Крім цих загальних інформаційних вимог, Директива передбачає, що в певних справах та для уможливлення реалізації прав суб'єктів даних контролери повинні надавати їм інформацію про юридичні підстави обробки та про те, як довго дані будуть збережені. Якщо персональні дані мають бути передані іншим одержувачам, включаючи треті країни або міжнародні організації, суб'єкти даних повинні бути поінформованими про категорії таких одержувачів. Нарешті, контролери повинні надавати будь-яку додаткову інформацію з урахуванням особливостей обставин, за яких здійснюється обробка даних, наприклад, коли персональні дані були

751 Там само, стаття 4 (1).

752 Там само, стаття 8.

753 Там само, стаття 13 (1).

зібрані під час негласного стеження, тобто без відома суб'єкта даних. Це гарантує справедливу обробку по відношенню до суб'єкта даних[754].

- Право на доступ до персональних даних. Держави-члени повинні забезпечити, щоб суб'єкт даних мав право знати, чи здійснюється обробка його або її персональних даних. Якщо вони обробляються, суб'єкт даних повинен мати доступ до певної інформації, такої як категорії даних, які обробляються[755]. Однак це право може бути обмежене, наприклад, щоб запобігти перешкоджанню слідству або переслідуванню за злочин, або для захисту громадської безпеки та прав і свобод інших[756].
- Право на виправлення персональних даних. Держави-учасниці зобов'язані забезпечити, щоб суб'єкт даних міг без будь-якої затримки домогтися виправлення некоректних персональних даних. Більше того, суб'єкт даних також має право на те, щоб неповні дані були доповнені[757].
- Право на видалення персональних даних та обмеження обробки. У певних випадках контролер має стерти персональні дані. Крім того, суб'єкти даних можуть забезпечити видалення своїх персональних даних, однак тільки у випадках, коли вони обробляються незаконно[758]. У певних ситуаціях обробка даних може бути обмежене без видалення даних. Така ситуація може виникнути у випадках, якщо: 1) була оскаржена точність персональних даних, але це не може бути підтверджено, 2) персональні дані необхідні для доказів[759].

Якщо контролер відмовляється обмежити чи видалити персональні дані або обмежити обробку даних, суб'єкт даних має бути поінформований про це письмово. Держави-члени можуть обмежити це право на інформацію, серед іншого, для захисту громадської безпеки або прав та свобод інших, тобто на тих самих підставах, що й обмеження права на доступ[760].

Суб'єкт даних за загальним правилом має право на інформацію про обробку своїх персональних даних і має право на доступ, виправлення або видалення даних, обмеження їх обробки. Ці права суб'єкт даних може реалізувати

754 Там само, стаття 13 (2).

755 Там само, стаття 14.

756 Там само, стаття 15.

757 Там само, стаття 16 (1).

758 Там само, стаття 16 (2).

759 Там само, стаття 16 (3).

760 Там само, стаття 16 (4).

безпосередньо через контролера. Як варіант, опосередкована реалізація прав суб'єкта даних через наглядовий орган також можлива відповідно до Директиви про захист персональних даних для поліції та органів кримінальної юстиції, і виникає це право, коли контролер обмежує право суб'єкта даних[761]. Стаття 17 Директиви вимагає, щоб держави-члени вжили заходів для забезпечення можливості суб'єкта даних реалізувати свої права через наглядовий орган. Тому контролер даних повинен поінформувати суб'єкта даних про можливість непрямого доступу.

Обов'язки контролера та оператора

У контексті Директиви про захист персональних даних для поліції та органів кримінальної юстиції контролери даних є компетентними державними органами або іншими установами з відповідними публічними повноваженнями та публічною владою, які визначають цілі та засоби обробки персональних прав. Директива встановлює низку обов'язків контролерів даних для забезпечення високого рівня захисту персональних даних, які обробляються в правоохоронних цілях.

Компетентні органи влади повинні вести реєстри операцій з обробки даних, які вони здійснюють у системах автоматичної обробки. Реєстри мають вестися щонайменше для збору, зміни, ознайомлення, відкриття, включаючи передачу, поєднання та видалення персональних даних[762]. Директива передбачає, що реєстри ознайомлення та відкриття повинні уможливити визначення дати та часу таких дій, їх обґрунтування та, наскільки це можливо, ідентифікацію осіб, які ознайомлювалися з системою або відкривали персональні дані, а також отримувачів персональних даних. Реєстри повинні використовуватися виняткова з метою перевірки правомірності обробки, для самоперевірки, для забезпечення цілісності та безпеки персональних даних, а також для кримінальних проваджень[763]. На вимогу наглядового органу контролер та оператор має надати органу доступ до реєстрів.

Зокрема, контролери мають загальний обов'язок запроваджувати технічні та організаційні заходи для здійснення обробки відповідно до Директиви, а також щоб бути здатними продемонструвати правомірність такої обробки[764]. При плануванні таких заходів вони мають брати до уваги характер, обсяг та

761 Там само, стаття 17.

762 Там само, стаття 25 (1).

763 Там само, стаття 25 (2).

764 Там само, стаття 19.

контекст обробки, а також важливо брати до уваги будь-які потенційні ризики для прав та свобод індивіда. Контролери мають розробити внутрішні правила та вжити заходів для дотримання принципів захисту даних, зокрема принципу захисту даних за призначенням та за замовчуванням[765]. Якщо обробка, вірогідно, призведе до ризику високого рівня щодо прав осіб, наприклад, у зв'язку з використанням нових технологій, контролери повинні здійснювати оцінку впливу на захист персональних даних до початку обробки[766]. Директива також передбачає список заходів, які повинні бути виконані контролерами для убезпечення обробки. Він включає заходи для попередження недозволеному доступу до персональних даних, що ними обробляються, для забезпечення того, що уповноважені особи матимуть доступ лише до тих персональних даних, на які розповсюджується їхній дозвіл на доступ, що функції системи обробки виконуються належним чином, а також що збережені персональні дані не можуть бути викривлені внаслідок несправної роботи системи[767]. Якщо дійсно виникають порушення правил захисту персональних даних, контролери повинні повідомити про це наглядовий орган протягом трьох днів з описанням характеру порушення, ймовірних наслідків, категорій залучених персональних даних та приблизної кількості відповідних суб'єктів даних, які можуть зазнати впливу. Факт порушення правил захисту персональних даних також повинен повідомлятись суб'єкту даних «без неналежної затримки», якщо порушення, ймовірно, призведе до ризику високого рівня для його або її прав та свобод[768].

Директива містить принцип підзвітності та покладає на контролерів обов'язок вжити заходів для забезпечення дотримання цього принципу. Контролери повинні вести записи всіх категорій дій з обробки, за яку вони несуть відповідальність: деталізований зміст таких записів передбачено в статті 24 Директиви. На вимогу контролюючого органу йому повинен надаватися доступ до цих записів так, щоб він міг здійснити моніторинг дій контролера з обробки даних. Іншим важливим заходом для посилення підзвітності є призначення спеціаліста із захисту персональних даних (СЗПД). Контролери зобов'язані призначити спеціаліста із захисту персональних даних, водночас Директива дозволяє державам-учасницям робити винятки з цього обов'язку для судів та інших незалежних судових органів[769]. Завдання СЗПД є аналогічними тим, що

765 Там само, стаття 20.

766 Там само, стаття 27.

767 Там само, стаття 29.

768 Там само, статті 30 та 31.

769 Там само, стаття 32.

передбачає Загальний регламент захисту персональних даних. Він або вона моніторить дотримання положень Директиви, надає інформацію та рекомендації працівникам, які здійснюють обробку даних, щодо їхніх обов'язків відповідно до законодавства із захисту персональних даних. СЗПД також надає поради щодо необхідності проведення оцінки впливу захисту персональних даних та діє як контактна особа для контролюючих органів.

Передача третім країнам або міжнародним організаціям

Як і Загальний регламент захисту персональних даних, Директива встановлює умови передачі персональних даних третім країнам або міжнародним організаціям. Якщо персональні дані можна було вільно передавати за межі юрисдикції ЄС, захисні гарантії та потужний захист, передбачений правом ЄС, могли б бути зруйновані. Та й умови досить відрізняються від тих, які передбачені Загальним регламентом захисту персональних даних. Передача персональних даних третім країнам або міжнародним організаціям дозволяється, якщо[770]:

- Передача даних необхідна для цілей цієї Директиви.
- Персональні дані передаються до компетентного органу (в розумінні Директиви) третьої країни або міжнародної організації, водночас існує відступ від цього правила в окремих та конкретних справах[771].
- Передача персональних даних до третіх країн або міжнародних організацій, які були отримані в ході транскордонного співробітництва, вимагає дозволу держави-члена, з якої ці дані походили, водночас з цього правила є винятки в термінових справах.
- Європейською комісією було прийнято рішення про відповідність, встановлені належні захисні гарантії або застосовується відступ для передачі в конкретних ситуаціях.
- Подальша передача персональних даних до іншої третьої країни або міжнародної організації вимагає попереднього дозволу компетентного органу влади місця походження, який візьме до уваги, серед іншого, серйозність правопорушення та рівень захисту персональних даних у країні, до якої передаються дані в ході другої міжнародної передачі[772].

770 Там само, стаття 35.

771 Там само, стаття 39.

772 Там само, стаття 35 (1).

Відповідно до Директиви передача персональних даних може відбутись, якщо дотримано одну з трьох умов. Першою умовою є надання Європейською комісією рішення про відповідність згідно з Директивою. Рішення може застосовуватися до всієї території третьої країни або до конкретних секторів третьої країни або міжнародної організації. Однак це можливо лише у разі, якщо забезпечено належний рівень захисту та дотримано умов Директиви[773]. У таких справах передача персональних даних не вимагає дозволу держави-учасниці[774]. Європейська Комісія повинна відстежувати події, які можуть вплинути на дію рішень про відповідність. Крім того, рішення повинне включати механізм періодичного перегляду. Комісія також може скасувати, змінити або зупинити рішення, якщо наявна інформація свідчить, що умови третьої країни або міжнародної організації більше не забезпечують належний рівень захисту. Якщо це так, Комісія має провести консультації з третьою країною або міжнародною організацією, щоб виправити ситуацію.

За відсутності рішення про відповідність передача може ґрунтуватися на належних гарантіях. Вони можуть бути викладені в юридично обов'язкових інструментах, або контролер може провести самостійний аналіз обставин передачі персональних даних та дійти висновку про існування належних гарантій. Самостійний аналіз повинен включати можливі угоди про співробітництво, укладені між Європолом і Євроюстом та третьою країною або міжнародною організацією, існування обов'язку збереження конфіденційності та дотримання принципу обмеження цілі, а також надані запевнення, що дані не будуть використовуватися для будь-яких форм жорстокого та нелюдського поводження, включаючи покарання у вигляді смертної кари[775]. В останньому випадку контролер повинен повідомити компетентний контролюючий орган про типи передач за цією категорією[776].

Якщо жодного рішення про відповідність не прийнято або не встановлено належних гарантій, передача все ж можлива в окремих ситуаціях, вказаних в Директиві. Такі ситуації включають, серед іншого, захист життєво важливих інтересів суб'єкта даних або інших осіб та попередження негайної та серйозної загрози безпеці громадського порядку держави-учасниці або третьої країни[777].

773 Там само, стаття 36.

774 Там само, стаття 36 (1).

775 Там само, п. 71 преамбули.

776 Там само, стаття 37 (1).

777 Там само, стаття 38 (1).

В індивідуальних та окремих випадках передача даних компетентними органами отримувачам, які зареєстровані в третіх країнах та які не є компетентними органами, може мати місце, якщо крім дотримання однієї з трьох вищевказаних умов також дотримано додаткових умов, передбачених статтею 39 Директиви. А саме, передача повинна бути вкрай необхідною для виконання завдань компетентного органу, що здійснює передачу, який також є відповідальним за визначення того, що жодні засадничі права або свободи осіб не переважають над публічним інтересом, яким обґрунтовується передача. Така передача повинна документуватись, а компетентний орган, який здійснює передачу, повідомляє компетентний контролюючий орган[778].

Нарешті, щодо третіх країн та міжнародних організацій Директива також вимагає створення механізму міжнародного співробітництва для сприяння ефективному виконанню законодавства і, таким чином, допомагає контролюючим органам із захисту персональних даних взаємодіяти з їхніми іноземними партнерами[779].

Незалежний контроль та засоби для суб'єктів даних

Кожна держава-член зобов'язана забезпечити, щоб один або більше незалежних національних контролюючих органів були відповідальними за надання консультацій та моніторинг застосування положень, прийнятих відповідно до Директиви[780]. Контролюючий орган, який створено для цілей Директиви, може бути тим самим органом, який створено відповідно до Загального регламенту захисту персональних даних. Водночас, держави-члени вільні у створенні іншого органу за умови, що він відповідає критеріям незалежності.

Контролюючі органи повинні також розглядати скарги, подані будь-якою особою щодо захисту своїх прав і свобод у контексті обробки персональних даних компетентними органами.

У разі відмови суб'єкту даних у реалізації своїх прав з обґрунтованих причин суб'єкт даних повинен мати право на оскарження до компетентного національного контролюючого органу та/або до суду. Якщо особа зазнала шкоди у зв'язку з порушенням національного закону, ухваленого для виконання Директиви, він або вона має право на компенсацію, яка повинна виплачуватися контролером або будь-яким іншим компетентним органом відповідно

778 Там само, стаття 37 (3).

779 Там само, стаття 40.

780 Там само, стаття 41.

до законодавства держави-члена[781]. За загальним правилом, суб'єкти даних повинні мати доступ до засобу судового захисту в разі будь-якого порушення їхніх прав, гарантованих національним законом, ухваленим для виконання Директиви[782].

8.3 Інші спеціальні правові інструменти із захисту даних у контексті правоохоронних питань

На додаток до Директиви про захист персональних даних для поліції та органів кримінальної юстиції обмін інформацією, якою володіють держави-члени в певних сферах, регулюється низкою правових документів, таких як Рамкове рішення Ради №2009/315/ЈНА про організацію та зміст обміну між державами-членами інформацією, отриманою з відомостей про судимості, Рішення Ради 2000/642/ЈНА стосовно домовленостей про співпрацю між підрозділами фінансової розвідки держав-членів щодо обміну інформацією, Рамкове рішення Ради №2006/960/ЈНА від 18 грудня 2006 року про спрощення обміну інформацією та розвідувальними даними між правоохоронними органами держав-членів Європейського Союзу[783].

Важливо, що транскордонне співробітництво[784] між компетентними органами все більше охоплює обмін імміграційними даними. Ця сфера права не вважається частиною питань поліції або кримінальної юстиції, але в багатьох аспектах вона стосується роботи поліції та органів правосуддя. Те саме стосується даних про товари, які імпортуються до ЄС та експортуються з нього. Припинення контролю за внутрішніми кордонами в межах Шенгенської зони посилило ризик шахрайства та викликало необхідність для держав-членів

781 Там само, стаття 56.

782 Там само, стаття 54.

783 Рада Європейського Союзу (2009), Рамкове рішення Ради 2009/315/ЈНА від 26 лютого 2009 р. про організацію та зміст обміну між державами-членами інформацією, отриманою з відомостей про судимості, OJ 2009 L 93; Рада Європейського Союзу (2000), Рішення Ради 2000/642/ЈНА від 17 жовтня 2000 р. стосовно домовленостей про співпрацю між підрозділами фінансової розвідки держав-членів щодо обміну інформацією, OJ 2000 L 271; Рамкове рішення Ради 2006/960/ЈНА від 18 грудня 2006 р. про спрощення обміну інформацією та розвідувальними даними між правоохоронними органами держав-членів Європейського Союзу, OJ L 386.

784 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.

активізувати співробітництво, зокрема шляхом посилення транскордонного обміну інформацією для більш ефективного виявлення порушень національного митного права та митного права ЄС і переслідування за такі порушення. Крім того, останніми роками в світі підвищується рівень серйозної та організованої злочинності і тероризму, які можуть бути пов'язані з пересуванням між країнами, викликаючи потребу в збільшенні транскордонної співпраці поліції та правоохоронних органів у багатьох справах[785].

Прюмське рішення

Важливим прикладом інституалізованого транскордонного співробітництва з обміну національними даними є Рішення Ради 2008/615/JHA (разом з положеннями щодо його виконання в Рішенні 2008/615/JHA) про посилення транскордонного співробітництва у зв'язку з боротьбою з тероризмом і транскордонною злочинністю (Прюмське рішення), яким Прюмська угода була включена до законодавства у 2008 році[786]. Прюмська угода є договором з міжнародного поліцейського співробітництва, підписаного у 2005 році Австрією, Бельгією, Францією, Німеччиною, Люксембургом, Нідерландами та Іспанією[787].

Прюмське рішення має на меті допомогти державам-учасницям покращити поширення інформації з метою попередження та боротьби із злочинністю у трьох сферах: тероризм, транскордонна злочинність та нелегальна міграція. З цією метою рішення передбачає положення щодо:

- автоматизованого доступу до ДНК-профілів, даних відбитків пальців і певних національних реєстраційних даних транспортних засобів;
- надання даних щодо основних подій, які мають транскордонний вимір;
- надання інформації для запобігання терористичній діяльності;
- інших заходів для посилення транскордонного поліцейського співробітництва.

785 Див. Європейська Комісія (2011), Пропозиція до Директиви Європейського Парламенту та Ради про використання РДП для попередження, виявлення, розслідування та переслідування за тероризм та серйозні злочини, COM(2011) 32 остаточний, Брюссель, від 2 лютого 2011 р., с. 1.

786 Рада Європейського Союзу (2008), Рішення Ради 2008/615/JHA від 23 червня 2008 р. про посилення транскордонного співробітництва у зв'язку з боротьбою з тероризмом і транскордонною злочинністю, OJ 2008 L 210.

787 *Конвенція* між Королівством Бельгією, Федеративною Республікою Німеччини, Королівством Іспанією, Французькою Республікою, Великим Герцогством Люксембургом, Королівством Нідерландами та Республікою Австрією щодо посилення транскордонного співробітництва, зокрема, у боротьбі з тероризмом, транскордонною злочинністю та нелегальною міграцією.

Бази даних, до яких надає доступ Прюмське рішення, регулюються винятково національним законодавством, але обмін даними додатково регулює це рішення, відповідність якого Директиві про захист персональних даних для поліції та органів кримінальної юстиції ще потребує оцінки. Компетентними органами, які здійснюють нагляд за такими потоками даних, є національні наглядові органи з питань захисту персональних даних.

Рамкове рішення 2006/960/JHA – Шведська ініціатива

Рамкове рішення 2006/960/JHA (Шведська ініціатива)[788] є іншим прикладом транскордонного співробітництва щодо обміну даними, якими володіють правоохоронні органи на національному рівні. Шведська ініціатива особливо зосереджується на обміні розвідувальними даними та інформацією, а також передбачає спеціальні правила захисту даних у статті 8.

Відповідно до цього інструменту, використання інформації та обмін розвідувальними даними повинні охоплюватися національними положеннями щодо захисту персональних даних держави-члена, яка отримує інформацію, а саме тими положеннями, які б регулювали діяльність із збору цієї інформації в самій державі. Стаття 8 йде навіть далі, передбачаючи, що надаючи інформацію та розвідувальні дані, компетентні правоохоронні органи повинні встановити умови, які відповідають їхньому національному законодавству, щодо використання переданої інформації компетентним правоохоронним органом, що її приймає. Такі умови також можуть застосовуватися до надання інформації про результат кримінального розслідування або кримінальних розвідувальних операцій, для яких вимагався обмін інформацією та розвідувальними даними. Однак, якщо національне законодавство передбачає винятки з обмежень на використання (наприклад, для судових органів, законодавчих установ тощо), інформація та розвідувальні дані можуть використовуватися винятково після попередньої консультації з державою-членом, яка передала інформацію.

Надані інформація та розвідувальні дані можуть використовуватися:

- для цілей, для яких вони були надані;
- для попередження негайного або серйозного ризику для громадської безпеки.

Обробка для інших цілей може бути дозволена, але виключно за попереднім дозволом держави-члена, яка передавала цю інформацію.

788 Рада Європейського Союзу (2006), Рамкове рішення Ради 2006/960/JHA від 18 грудня 2006 р. про спрощення обміну інформацією та розвідувальними даними між правоохоронними органами держав-членів Європейського Союзу, OJ L 386/89, від 29 грудня 2006 р.

Шведська ініціатива додатково встановлює, що персональні дані, які обробляються, повинні бути захищеними у відповідності до міжнародних правових інструментів, таких як:

- Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних[789];
- Додатковий протокол від 8 листопада 2001 р. до цієї Конвенції щодо контролюючих органів та транскордонних потоків даних[790];
- Рекомендація Ради Європи № R(87)15 щодо використання персональних даних поліцією[791].

Директива ЄС про використання реєстраційних даних пасажирів

Реєстраційні дані пасажирів (РДП; англ. PNR) стосуються інформації про авіапасажирів, що збирається та зберігається в системах резервування та контролю відправки перевізниками для їхніх комерційних цілей. Ці дані містять декілька різних видів інформації, як-от дати подорожей, маршрут подорожі, інформація про квитки, контактні дані, інформація про агента подорожі, якщо політ був зарезервований, використані способи оплати, номер посадкового місця та інформація про багаж[792]. Обробка РДП може допомогти правоохоронним органам ідентифікувати відомих або потенційних підозрюваних та на підставі інформації про маршрут здійснити аналіз пересування та інших індикаторів, які зазвичай пов'язані з кримінальною діяльністю. Аналіз РДП також дозволяє ретроспективне відстеження маршрутів подорожей та контактів осіб, які підозрюються в участі в кримінальній діяльності, що надає правоохоронним органам можливість виявити злочинну мережу[793]. ЄС уклав певні угоди з третіми краї-

789 Рада Європи (1981), Конвенція Ради Європи про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних, ETS № 108.

790 Рада Європи (2001), Додатковий протокол до Конвенції про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних щодо контролюючих органів та транскордонних потоків, ETS № 108.

791 Рада Європи, Комітет міністрів (1987), Рекомендація Rec(87)15 державам-членам щодо регулювання використання персональних даних у роботі поліції, (Прийнята Комітетом міністрів від 17 вересня 1987 р. на 410 засіданні Заступників міністрів).

792 Пропозиція до Директиви Європейського Парламенту і Ради (ЄС) щодо використання даних РДП для запобігання, виявлення, розслідування та судового переслідування терористичної діяльності й тяжких злочинів, COM(2011) 32 остаточна версія, Брюссель, 2 лютого 2011 р., с. 1.

793 Європейська Комісія (2015), Інформаційний бюлетень про боротьбу з тероризмом на рівні ЄС, огляд дій, заходів та ініціатив Комісії, Брюссель, від 11 січня 2015 р.

нами щодо обміну РДП, про які йдеться в розділі 7. Крім того, ЄС запровадив обробку РДП у рамках Директиви 2016/681/ЕС про використання даних РДП для попередження, виявлення, розслідування та переслідування за тероризм та серйозні злочини (Директива ЄС про РДП)[794]. Ця Директива передбачає обов'язки авіаперевізників передавати РДП компетентним органам та встановлює жорсткі гарантії захисту даних для обробки та збору таких даних. Директива ЄС про РДП застосовується до міжнародних перельотів до та з ЄС, а також до внутрішніх перелетів в ЄС, якщо держава-член прийняла відповідне рішення[795].

Зібрані дані РДП повинні містити лише ту інформацію, яка дозволяється Директивою ЄС про РДП. Вони мають зберігатись у єдиному інформаційному відділі і в захищеному місцезнаходженні в кожній державі-члені. РДП мають бути знеособленні через шість місяців після їх передачі авіаперевізником та зберігатися не більше ніж п'ять років[796]. Обмін РДП відбувається між державами-членами, державами-членами та Європолом, та з третіми країнами, однак лише на основі індивідуального підходу в кожній справі.

Передача та обробка РДП та права на захист для суб'єктів даних повинні відповідати Директиві про захист персональних даних для поліції та органів кримінальної юстиції та повинні забезпечувати високий рівень захисту приватності та персональних даних, який вимагається Хартією, Оновленою Конвенцією 108 та ЄСПЛ.

Незалежні контролюючі органи, які мають компетенцію контролю на підставі Директиви про захист персональних даних для поліції та органів кримінальної юстиції, також відповідальні за проведення консультацій та моніторинг застосування положень, прийнятих державами-членами відповідно до Директиви ЄС про РДП.

Збереження телекомунікаційних даних

Директива про зберігання даних[797] – визнана нечинною 8 квітня 2014 року у справі *«Digital Rights Ireland»* – зобов'язувала надавачів телекомунікаційних послуг зберігати доступними метадані для спеціальних цілей боротьби

794 *Директива 2016/681* Європейського Парламенту та Ради (ЄС) про використання даних записів реєстрації пасажирів (РДП) для запобігання, виявлення, розслідування та переслідування за вчинення терористичних злочинів та серйозних злочинів, від 27 квітня 2016OJ 2016 L 119, p. 132.

795 РДП Директива, L 119, p. 132, стаття 1 (1) та стаття 2 (1).

796 Там само, стаття 12 (1) та стаття 12 (2).

797 Директива 2002/58/ ЄС Європейського Парламенту та Ради про обробку персональних даних та захист таємниці в секторі електронних комунікацій, OJ 2006 L 105.

з серйозними злочинами щонайменше шість, але не більше 24 місяців незалежно від того, чи необхідні ці дані надавачу послуг для виставлення рахунків або технічних аспектів надання послуг.

Зберігання телекомунікаційних даних очевидно становить втручання у право на захист персональних даних[798]. Виправданість такого втручання була оскаржена в декількох судових провадженнях у державах-членах ЄС[799].

Приклад: у справі «*"Digital Rights Ireland" та Земельний уряд Каринтії та інші*»[800] група «Digital Rights» та пан Зайтлінгер звернулися з позовом до Високого Суду Ірландії та Конституційного Суду Австрії, відповідно, оскаржуючи правомірність національних заходів, які дозволяли зберігання даних електронних телекомунікацій. Група «Digital Rights» вимагала, щоб ірландський суд визнав Директиву 2006/24 та частину національного кримінального закону щодо терористичних правопорушень нечинними. Аналогічно, пан Зайтлінгер та більш ніж 11000 інших заявників оскаржили положення австрійського законодавства щодо телекомунікацій, які імплементували Директиву 2006/24, та вимагали визнати їх нечинними.

Розглядаючи ці вимоги в контексті надання преюдиціального рішення, СЄС визнав Директиву про зберігання даних нечинною. Відповідно до позиції Суду ЄС, сукупність даних, які могли зберігатися відповідно до Директиви, надавали точну інформацію про осіб. Крім того, СЄС розглянув серйозність втручання в основоположні права на повагу до приватного життя та на захист персональних даних. Він визнав, що зберігання даних відповідає цілі суспільного інтересу, який полягає в боротьбі з серйозними злочинами та, отже, у забезпеченні громадської безпеки. Однак СЄС вирішив, що законодавець ЄС порушив принцип пропорційності, прийнявши цю Директиву. Хоча Директива може бути належним інструментом для досягнення цілі,

798 ЄІЗПД (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/ЄС), 31 травня 2011 р.

799 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.

800 Див. рішення Суду ЄС, об'єднані справи C-293/12 ти C-594/12, «"Digital Rights Ireland Ltd." проти Міністра зв'язку, морських та природних ресурсів та інших та Земельний уряд Каринтії та інші» (*Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*) [ВП], від 08 квітня 2014 р., п. 65.

що була поставлена, «широкомасштабне та особливо серйозне втручання Директиви в основоположні права на повагу до приватного життя та захист персональних даних не є обмеженим тією мірою, щоб забезпечити зведення втручання до того, що є винятково необхідним».

За відсутності спеціального законодавства щодо зберігання даних таке зберігання дозволяється як виняток з правила конфіденційності телекомунікаційних даних відповідно до Директиви 2002/58/ЕС (Директива про конфіденційність та електронні комунікації)[801] якості превентивного заходу, який, одначе, може застосовуватися винятково для боротьби із серйозною злочинністю. Таке зберігання має зводитися до того, що є вкрай необхідним з урахуванням категорій збережених даних, засобів комунікації, на які здійснювався вплив, зацікавлених осіб та обраним періодом зберігання. Національні органи повинні мати доступ до збережених даних з суворим дотриманням умов, включаючи попередню перевірку незалежним органом. Дані повинні бути збережені в межах ЄС.

Приклад: після рішення у справі *«"Digital Rights Ireland" та Земельний уряд Каринтії та інші»*[802] до Суду ЄС надійшло ще дві справи, які стосувалися загального обов'язку зберігати телекомунікаційні дані, покладеного на надавачів послуг з електронного спілкування, у Швеції та Сполученому Королівстві, як цього вимагала визнана нечинною Директива про зберігання даних. У справі *«"Tele2 Sverige" та Секретар внутрішніх справ проти Тома Вотсонса та інших»*[803] Суд ЄС вирішив, що національне законодавство, яке передбачало загальне та нерозбірливе зберігання даних, що не вимагало встановлення будь-якого зв'язку між даними, які мають бути збережені, та загрозою громадській безпеці, та без встановлення будь-яких умов – наприклад, часу зберігання, географічної зони, груп осіб, які,

801 Директива 2002/58/ ЄС Європейського Парламенту та Ради про обробку персональних даних та захист таємниці в секторі електронних комунікацій (Директива про конфіденційність та електронні комунікації), OJ 2002 L 201.

802 Рішення Суду ЄС, об'єднані справи C-293/12 ти C-594/12, «"Digital Rights Ireland Ltd." проти Міністра зв'язку, морських та природних ресурсів та інших та Земельний уряд Каринтії та інші» (*Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*) [ВП], від 08 квітня 2014р.

803 Рішення Суду ЄС, об'єднані справи C-203/15 та C-698/15 «"Tele2 Sverige AB" проти Державного управління зв'язку та телекомунікації» та «Секретар внутрішніх справ проти Тома Вотсона та інших» (*Tele2 Sverige AB v. Post- och telestryrelsen and Secretary of State for the Home Department v. Tom Watson and Others*) [ВП], від 21 грудня 2016 р., пп. 105–106.

ймовірно, залучені до вчинення серйозних злочинів – вийшло за межі того, що є винятково необхідним, та не може вважатися виправданим в демократичному суспільстві, як це вимагається Директивою 2002/58/ЕС, витлумаченою в світлі Хартії основних прав ЄС.

Огляд

У січні 2017 року Європейська комісія опублікувала проєкт Регламенту щодо поваги до приватного життя та захисту персональних даних в електронному спілкуванні, який має скасувати та замінити Директиву 2002/58/ЄС[804]. Проєкт не включає спеціальних положень про зберігання даних. Однак він передбачає, що держави-члени можуть обмежити певні обов'язки та права законодавчим шляхом, якщо таке обмеження є необхідним та пропорційним заходом для захисту конкретних суспільних інтересів, включаючи національну безпеку, оборону, громадську безпеку, а також для попередження, розслідування, виявлення кримінальних правопорушень або переслідування за їх вчинення, або для виконання кримінальних покарань[805]. Таким чином, держави-члени матимуть можливість зберегти або створити національні системи збереження даних, які передбачають цілеспрямовані заходи із збереження за умови, що такі системи регулювання відповідають праву ЄС з урахуванням рішень СЄС стосовно тлумачення Директиви про конфіденційність та електронні комунікації та Хартії основних прав ЄС[806]. Станом на час написання цього посібника дискусії щодо прийняття цього регламенту тривали.

Рамковий договір ЄС–США про захист персональних даних, якими обмінюються для правоохоронних цілей

1 лютого 2017 року набув чинності Рамковий договір ЄС–США про обробку персональних даних для попередження, розслідування, виявлення кримінальних злочинів та переслідування за їх вчинення[807]. Рамковий договір ЄС–США має

804 Європейська Комісія (2017), Проєкт Регламенту Європейського Парламенту та Ради про повагу до приватного життя та захист персональних даних в електронному спілкуванні та скасування *Директиви 2002/58/ЄС* (Директиви про конфіденційність та електронні комунікації), COM(2017) 10 остаточна версія, Брюссель, від 10 січня 2017 р.

805 Там само, п. 26 преамбули.

806 Див. пояснювальний меморандум до проєкту Директиви про конфіденційність та електронні комунікації COM(2017) 10 остаточна версія, п. 1.3.

807 Див. Рада ЄС (2016), *«Посилений захист прав громадян ЄС у правоохоронному співробітництві: підписання ЄС та США «Рамкового договору»*, пресреліз 305/16, від 2 червня 2016 р.

забезпечити високий рівень захисту даних для громадян ЄС і в той же час посилити співробітництво правоохоронних органів ЄС та США. Він є додатковим договором до наявних угод, що укладені між правоохоронними органами ЄС і США та держав-членів і США, і допомагає встановити чіткі та гармонізовані правила із захисту персональних даних для майбутніх угод у цій сфері. Договір спрямований на створення довготривалої правової основи для сприяння обміну інформацією.

Власне договір не є належною правовою підставою для обміну персональними даними, натомість він пропонує зацікавленим особам належні гарантії захисту персональних даних. Він охоплює всю обробку персональних даних, необхідну для попередження, розслідування та виявлення злочинів, включаючи тероризм, а також переслідування за їх вчинення[808].

Договір встановлює різноманітні захисні гарантії для забезпечення використання персональних даних лише у зазначених в договорі цілях. Зокрема, він передбачає:

- обмеження використання даних: персональні дані можуть використовуватися лише для цілей попередження, розслідування, виявлення кримінальних правопорушень або переслідування за їх вчинення;
- захист від свавільної та невиправданої дискримінації;
- подальшу передачу: будь-яка подальша передача до країни, яка не входить до США чи Союзу, або міжнародній організації повинна підлягати попередній згоді компетентного органу країни, яка першою передала дані;
- якість даних: персональні дані повинні зберігатися з урахуванням їхньої точності, відповідності, своєчасності та повноти;
- безпеку обробки, включаючи повідомлення про порушення захисту даних;
- обробку чуттєвих даних, яку дозволено винятково за наявності належних захисних гарантій у відповідності до закону;
- періоди зберігання: персональні дані не можуть зберігатися довше, ніж це необхідно або доцільно;

808 Договір ЄС–США про обробку персональних даних для попередження, розслідування, виявлення злочинів та переслідування за їх вчинення від 18 травня 2016 р., (OR.en) 8557/16, стаття 3(1). Див. також повідомлення Комісії про переговори ЄС та США щодо договору про захист персональних даних від 26 травня 2010 р., MEMO/10/216 та пресреліз Комісії ЄС (2010) про високі стандарти захисту приватності в Договорі ЄС–США від 26 травня 2010 р., IP/10/609.

- права на доступ та виправлення: будь-яка особа має право на доступ до своїх персональних даних за певних умов, а також повинна мати можливість вимагати їх виправлення у разі неточності;
- прийняття автоматизованих рішень за наявності належних захисних гарантій, включаючи можливість домогтись участі людини;
- ефективний контроль, включаючи співпрацю між контролюючими органами ЄС та США;
- судовий захист та виконання судових рішень: громадяни ЄС мають право[809] вимагати захисту в судах США у справах, у яких органи влади США відмовляють у доступі до даних чи їх виправленні, або неправомірно відкривають їхні персональні дані.

Відповідно до Рамкового договору, також створюється система повідомлення про будь-які порушення захисту персональних даних компетентному контролюючому органу в державі-члені, у якій проживають особи, що зазнали впливу. Юридичні гарантії, передбачені договором, забезпечують рівне ставлення до громадян ЄС у США в разі порушення конфіденційності[810].

8.3.1 Захист даних в судових та правоохоронних агенціях ЄС

Європол

Європол – це правоохоронний орган ЄС зі штаб-квартирою в місті Гаазі та національними підрозділами Європолу (НПЄ) в кожній з держав-членів. Європол був створений у 1998 році; його теперішній правовий статус інституції ЄС ґрунтується на Регламенті про Агенцію ЄС із правоохоронного співробітництва (Регламент Європолу)[811]. Метою Європолу є надання допомоги в запо-

809 *Закон США про судовий захист* було підписано Президентом США Обамою 24 лютого 2016 р.

810 Європейський інспектор із захисту персональних даних видав Висновок стосовно Договору ЄС–США, рекомендуючи, зокрема, такі зміни: 1) додати до статті стосовно збереження даних не довшу ніж необхідно та належно «для визначених цілей, з якими вони були передані» та 2) за винятком масової передачі чутливих даних, яка може мати місце. Див. Європейський інспектор із захисту персональних даних, *Висновок 1/2016*, *Попередній висновок про договір між Сполученими Штатами Америки та Європейським Союзом про захист особистої інформації щодо попередження, розслідування, виявлення злочинів та переслідування за їх вчинення*, п. 35.

811 *Регламент (ЄС) 2016/794* Європейського Парламенту та Ради від 11 травня 2016 р. про Агенцію ЄС із правоохоронного співробітництва (Європол) та заміну і скасування Рішень Ради 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA та 2009/968/JHA, OJ 2016 L 135, с. 53.

біганні та розслідуванні організованої злочинності, тероризму та інших форм серйозних злочинів, перерахованих у додатку I до Регламенту Європолу, що впливають на дві або більше держав-членів. Він робить це шляхом обміну інформацією та виконання ролі інформаційного центру ЄС, аналіз розвідувальної інформації та оцінку загроз.

Для досягнення своїх цілей Європол створив Інформаційну систему Європолу (Europol Information System – EIS), яка надає державам-членам базу даних для обміну розвідувальними даними та інформацією через свої НПЄ. Інформаційна система Європолу може використовуватися для 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 НЄУ можуть як вносити дані безпосередньо до Інформаційної системи Європолу, так і вилучати дані з неї. Лише та сторона, яка внесла дані в систему, може змінити, виправити або видалити їх. Органи ЄС, треті країни та міжнародні організації також можуть надати інформацію Європолу.

Інформація, включно з персональними даними, також може бути отримана Європолом з публічно доступних джерел, як, наприклад, інтернет. Передачі персональних даних органам ЄС дозволяються, лише якщо це необхідно для виконання завдань Європолу або органу ЄС, що отримує інформацію. Передачі персональних даних третім країнам або міжнародним організаціям дозволяються, лише якщо Європейська Комісія вирішить, що відповідна держава або міжнародна організація забезпечує відповідний рівень захисту даних (рішення про відповідність) або якщо існує міжнародна угода чи угода про співробітництво. Європол може отримувати та обробляти персональні дані від приватних сторін та приватних осіб лише за умови, що ці дані передає НПЄ відповідно до його законодавства країни, контактна особа в третій країні, або міжнародна організація, з якою встановлено співробітництво на підставі угоди, або установа третьої країни чи міжнародної організації, щодо яких прийнято рішення про відповідність або з яким ЄС уклав міжнародну угоду. Весь обмін інформацією здійснюється через Мережу забезпечення обміну інформацією (SIENA).

У відповідь на події останнього часу в межах Європолу було створено спеціалізовані центри. У 2013 році було створено Європейський центр боротьби з кіберзлочинністю[812]. Центр є інформаційним порталом ЄС з питань кі-

812 Див. також, ЄІЗД (2012), Висновок Інспектора із 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.

берзлочинності, який сприяє більш швидкому реагуванню у разі вчинення онлайн-злочинів, розробляє і використовує цифрові судово-експертні засоби та надає інформацію про найкращий досвід розслідування кіберзлочинів. Центр спеціалізується на кіберзлочинах, які:

- скоюються організованими групами для отримання злочинним шляхом великих доходів, наприклад, через онлайн-шахрайство;
- заподіюють серйозну шкоду потерпілому, наприклад, через сексуальну експлуатацію дітей в інтернеті;
- зашкоджують критичній інфраструктурі та інформаційним системам у ЄС.

У січні 2016 року було створено Європейський центр боротьби з тероризмом (ЕСТС) для надання оперативної підтримки державам-членам у розслідуванні правопорушень, пов'язаних з тероризмом. Він здійснює в живому часі перехресну перевірку оперативних даних з тими даними, які вже має Європол, і швидко виявляє фінансові операції, що ведуть до злочинців, а також аналізує всі наявні слідчі дані для допомоги у формуванні структурованої картини терористичної мережі[813].

У лютому 2016 року, після зустрічі Ради в листопаді 2015 для підтримки держав-членів у виявленні та ліквідації злочинних мереж з незаконного транспортування мігрантів було відкрито Центр з протидії незаконному перевезенню мігрантів. Він діє як інформаційний хаб для підтримки регіональних офісів оперативних груп ЄС у містах Катанії (Італія) та Пірею (Греція), який допомагає національним органам у декількох сферах, включаючи обмін розвідувальними даними, кримінальні розслідування та переслідування злочинних мереж незаконного перевезення людей[814].

Регулювання захисту персональних даних у діяльності Європолу посилюється завдяки принципам Регламенту інститутів ЄС про захист персональних даних[815], а також відповідає Директиві про захист персональних даних для поліції та органів кримінальної юстиції, Оновленій Конвенції 108 та Рекомендації щодо використання персональних даних поліцією.

813 Див. *вебсайт Європолу щодо ЕСТС*.

814 Див. *вебсайт Європолу щодо EMSC*.

815 Регламент (ЕС) № 45/2001 Європейського Парламенту і Ради від 18 грудня 2000 р. про захист фізичних осіб у зв'язку з обробкою персональних даних інституціями та органами ЄС і про вільне переміщення таких даних, OJ 2001 L 8.

Обробка персональних даних стосовно жертв кримінальних правопорушень, свідків або інших осіб, які можуть надати інформацію щодо кримінальних порушень, або стосовно осіб віком до 18 років дозволяється, якщо це вкрай необхідно та пропорційно для запобігання або боротьби із злочинністю, що охоплюється цілями Європолу[816]. Обробка чутливих персональних даних заборонена, крім випадків, коли вона винятково необхідна та пропорційна щодо попередження або боротьби зі злочинами, на які націлений Європол, та якщо такі дані доповнюють інші персональні дані, що обробляються Європолом[817]. В обох випадках лише Європол може мати доступ до відповідних даних[818].

Зберігання даних дозволяється лише протягом необхідного та пропорційного періоду, а його продовження підлягає перевірці кожні три роки, без якої дані мають бути видалені автоматично[819].

За певних умов Європолу дозволяється прямо передавати персональні дані органу ЄС або органу влади третьої країни, або міжнародній організації[820]. Суб'єкти даних мають бути повідомлені без неналежної затримки про порушення захисту даних, якщо їхні права та свободи, ймовірно, зазнають серйозного негативного впливу[821]. На рівні держави-члена буде створено національний контролюючий орган для моніторингу обробки даних Європолом[822].

ЄІЗПД є відповідальним за моніторинг та забезпечення захисту основоположних прав і свобод фізичної особи в контексті обробки персональних даних Європолом, а також за консультування Європолу та суб'єктів даних щодо всіх питань з обробки персональних даних. З цією метою ЄІЗПД діє як орган, що здійснює розслідування та розглядає скарги, діючи в тісній співпраці з національними наглядовими органами[823]. ЄІЗПД та національні наглядові органи зустрічаються щонайменше двічі на рік у Раді співробітництва, яка має дорадчі функції[824]. Держави-члени зобов'язані законодавчо створити контролюючий орган, який має повноваження моніторити допустимість передачі персональних даних з державного рівня до Європолу та їхнє повернення,

816 Регламент Європолу, стаття 30 (1).

817 Там само, стаття 30 (2).

818 Там само, стаття 30 (3).

819 Там само, стаття 31.

820 Там само, стаття 24 та стаття 25, відповідно.

821 Там само, стаття 35.

822 Регламент Європолу, стаття 42.

823 Там само, стаття 43 та стаття 44.

824 Там само, стаття 45.

а також будь-яку комунікацію з Європолом щодо персональних даних[825]. Держави-члени також зобов'язані забезпечити, щоб національний орган міг діяти повністю незалежно, виконуючи свої завдання та обов'язки відповідно до Регламенту Європолу[826]. Для перевірки правомірності обробки даних, самостійного моніторингу своєї діяльності та забезпечення цілісності та безпеки даних Європол веде записи або документування діяльності з обробки даних. Ці записи містять інформацію про операції з обробки даних у системах автоматичної обробки щодо збору, зміни, ознайомлення, відкриття, комбінації або видалення[827].

Рішення ЄІЗПД може бути оскаржене до СЄС[828]. Будь-яка особа, яка зазнала шкоди внаслідок неправомірної операції з обробки даних, має право на отримання відшкодування або від Європолу, або від відповідальної держави-члена шляхом оскарження до СЄС у першому випадку, або до компетентного національного суду – у другому[829]. Крім того, спеціальна Спільна парламентська група з контролю (JPSG) національних парламентів та Європейського Парламенту може детально розглянути діяльність Європолу[830]. Будь-яка особа має право на доступ до будь-яких персональних даних, якими може володіти Європол про нього або неї, на додаток до права вимагати перевірки цих даних, виправлення або видалення. Ці права можуть підлягати виняткам та обмеженням.

Євроюст

Створений у 2002 році Євроюст є органом ЄС зі штаб-квартирою в Гаазі, який сприяє судовому співробітництву в розслідуванні та переслідуванні тяжких злочинів, що стосуються щонайменше двох держав-членів[831]. Євроюст має повноваження:

825 Там само, стаття 42 (1).

826 Там само, стаття 42 (1).

827 Там само, стаття 40.

828 Там само, стаття 48.

829 Там само, стаття 50.

830 Там само, стаття 51.

831 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).

- стимулювати і покращувати координацію розслідувань та судових переслідувань між компетентними органами різних держав-членів;
- допомагати у виконанні запитів і рішень, що стосуються судової співпраці.

Функції Євроюсту здійснюються національними членами. Кожна держава-член делегує до Євроюсту 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 вчиненні чи участі в кримінальному правопорушенні, або яких було засуджено за правопорушення, що належить до компетенції Євроюсту. Євроюст також може обробляти певну інформацію про свідків або жертв кримінальних правопорушень, що охоплюються його компетенцією[832]. 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. У 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 Оновленої Конвенції Ради Європи № 108 і наступним поправкам до неї. Під час обміну даними повинні дотримуватися 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[833].

У межах Євроюсту було створено незалежний Спільний контролюючий орган (СНО), завдання якого – 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,

832 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).

833 Правила процедури з обробки та захисту персональних даних в Євроюсті, OJ 2005 C 68/01, 19 березня 2005 р., п. 1.

блокування або видалення персональних даних. Якщо Євроюст обробляє персональні дані неправомірно, він несе відповідальність за шкоду, заподіяну суб'єкту персональних даних, згідно з національним законодавством держави-члена, де розташована його штаб-квартира, а саме Нідерландів.

Огляд

У липні 2013 року Європейська Комісія представила проєкт реформи Євроюсту. Цей проєкт супроводжувався пропозицією утворити Європейську прокуратуру (див. нижче). Ця ініціатива має на меті привести функції та структуру у відповідність до Лісабонського договору. Крім того, метою реформи є встановлення чіткого розподілу оперативних завдань Євроюсту, які здійснюються Колегією Євроюсту, та його адміністративних завдань. Це також надасть можливість державам-членам більше зосередитися на оперативних завданнях. Буде утворена нова Виконавча рада для допомоги колегії у виконанні адміністративних завдань[834].

Європейська прокуратура

Держави-члени мають виняткові повноваження переслідування за кримінальні злочини з шахрайства та неналежного використання бюджету ЄС, які потенційно можуть мати транскордонні наслідки. Важливість розслідування, переслідування та притягнення до відповідальності виконавців таких злочинів помітно зросла, особливо враховуючи економічну кризу, що триває[835]. Європейська Комісія запропонувала Регламент про утворення незалежної Європейської прокуратури (ЄП)[836] з метою боротьби із злочинністю, яка зачіпає фінансові інтереси ЄС. ЄП буде утворено з використанням процедури посиленого співробітництва, яка дозволяє мінімум дев'яти державам-членам встановлювати плідні стосунки співпраці в певній царині, дотичній до структур ЄС, без залучення інших країн ЄС[837]. Бельгія, Болгарія, Хорватія, Кіпр, Чеська Республіка, Естонія, Фінляндія, Франція, Німеччина, Греція, Латвія, Литва, Люксембург, Португалія, Румунія, Словенія, Словаччина та Іспанія

834 Див., *вебсторінку Євроюсту* на сайті Комісії.

835 Див. Європейська Комісія (2013), Проєкт Регламенту Ради про створення Європейського офісу прокуратури, COM(2013) 534 остаточний, Брюссель, від 17 липня 2013р., с. 1 та *вебсторінку ЄП* на сайті Комісії.

836 Європейська Комісія (2013), Проєкт Регламенту Ради про створення Європейського офісу прокуратури, COM(2013) 534 остаточний, Брюссель, від 17 липня 2013р.

837 Договір про функціонування Європейського Союзу, стаття 86 (1) та стаття 329 (1).

приєдналися до системи посиленого співробітництва; Австрія та Італія висловили намір приєднатись[838].

ЄП буде мати повноваження розслідувати шахрайство в ЄС та інші злочини, які зачіпають фінансові інтереси ЄС, а також притягати за них до відповідальності з метою ефективної координації розслідувань та притягнення до відповідальності в різних національних правових системах і покращення використання ресурсів і обміну інформацією на європейському рівні[839].

ЄП буде очолювати Європейський прокурор, а принаймні один делегований Європейський прокурор буде знаходитися в кожній державі-члені, відповідаючи за проведення розслідувань та підтримування обвинувачень у цій державі.

Пропозиція встановлює низку потужних захисних гарантій для прав осіб, залучених до розслідувань ЄП, передбачених національним законодавством, законодавством ЄС та Хартією основних прав ЄС. Розслідувальні заходи, які серйозно стосуються переважно основоположних прав, потребуватимуть попереднього дозволу національного суду[840]. Розслідування, що здійснюється ЄП, підлягатимуть контролю національних судів[841].

Регламент інститутів ЄС про захист персональних даних[842] буде застосовуватися до обробки адміністративних персональних даних ЄП. Для обробки персональних даних, пов'язаних з оперативними питаннями, ЄП, як і Європол, матиме окремий режим захисту персональних даних, подібний до того, що регулює діяльність Європолу та Євроюсту, враховуючи, що виконання функцій ЄП буде охоплювати обробку персональних даних з правоохоронними та прокурорськими органами на рівні держави-члена. Отже, правила захисту персональних даних ЄП практично ідентичні з правилами Директиви про захист персональних даних для поліції та органів кримінальної юстиції. Відповідно до пропозиції щодо утворення ЄП, обробка персональних даних повинна відповідати принципам законності та чесності, принципу обмеження

838 Див. Рада Європейського Союзу (2017), «*20 держав-членів погодилися щодо положень про створення Європейського офісу прокуратури (ЄП)*", пресреліз, від 8 червня 2017р.

839 Європейська Комісія (2013), Проєкт Регламенту Ради про створення Європейського офісу прокуратури, COM(2013) 534 остаточний, Брюссель, від 17 липня 2013р., с. 1 та с. 51-51. Див. також *вебсторінку ЄП* на сайті Комісії.

840 Європейська Комісія (2013), Проєкт Регламенту Ради про створення Європейського офісу прокуратури, COM(2013) 534 остаточний, Брюссель, від 17 липня 2013р., стаття 26 (4).

841 Там само, стаття 36.

842 Регламент (ЕС) № 45/2001 Європейського Парламенту і Ради від 18 грудня 2000 р. про захист фізичних осіб у зв'язку з обробкою персональних даних інституціями та органами ЄС і про вільне переміщення таких даних, OJ 2001 L 8.

цілі, мінімізації даних, точності, цілісності та конфіденційності. За можливості, ЄП повинна здійснювати чітке розмежування персональних даних різних категорій суб'єктів даних, таких як дані осіб, засуджених за злочин, осіб, які лише підозрюються, потерпілих та свідків. ЄП також повинна намагатися перевіряти якість персональних даних, що обробляються, та за можливості, розрізняти персональні дані, що ґрунтуються на фактах, та персональні дані, які ґрунтуються на особистій оцінці.

Пропозиція містить положення щодо прав суб'єктів даних, а саме права на інформацію, на доступ до своїх персональних даних, виправлення, видалення та обмеження обробки, а також передбачає, що такі права можуть реалізуватись опосередковано через ЄІЗПД. Вона також містить принципи безпеки обробки та підзвітності, вимагаючи, щоб ЄП впровадила належні технічні та організаційні заходи для забезпечення належного рівня безпеки щодо ризиків, які несе обробка, для ведення записів усієї діяльності з обробки та здійснення оцінки впливу на захист персональних даних до початку обробки, якщо даний вид обробки (наприклад, обробка з використанням нових технологій), ймовірно, може призвести до ризику високого рівня для прав осіб. Нарешті, пропозиція передбачає призначення колегією спеціаліста із захисту персональних даних, який має бути залучений до всіх питань, пов'язаних із захистом персональних даних, та забезпечити дотримання ЄП застосовного законодавства із захисту персональних даних.

8.3.2 Захист даних на рівні спільних інформаційних систем ЄС

На додаток до обміну інформацією між державами-членами та створення спеціалізованих органів ЄС для боротьби з транскордонною злочинністю, таких як Європол, Євроюст та ЄП, було утворено декілька спільних інформаційних систем на рівні ЄС для уможливлення і сприяння співробітництву та обміну даними між компетентними національними органами та органами ЄС для визначених цілей у сферах захисту кордонів, імміграції та притулку, а також митниці. Оскільки Шенгенська зона була вперше створена міжнародним договором, що діє незалежно від законодавства ЄС, Шенгенська інформаційна система (SIS) була заснована на багатосторонніх угодах та в подальшому закріплена в законодавстві ЄС. Візова інформаційна система (VIS), Євродак (Eurodac), Євросюр (Eurosur) або Митна інформаційна система (CIS) були утворені як інструменти, врегульовані правом ЄС.

Нагляд за цими системами розділений між національними контролюючими органами та ЄІЗПД. Для забезпечення високого рівня захисту ці органи взаємодіють з Наглядово-координаційними групами (SCGs), які пов'язані з наступними великомасштабними інформаційно-технологічними системами: 1) Євродак; 2) Візова інформаційна система; 3) Шенгенська інформаційна система; 4) Митна інформаційна система та 5) Інформаційна система внутрішнього ринку[843]. Наглядово-координаційні групи зазвичай зустрічаються двічі на рік під керівництвом обраного Голови та ухвалюють керівні настанови, обговорюють транскордонні справи або приймають спільні положення для перевірок.

Європейська агенція з питань широкомасштабних інформаційно-технологічних систем (eu-LISA)[844], створена в 2012 році, відповідає за довгострокове оперативне управління Шенгенською інформаційною системою другого покоління (SIS II), Візовою інформаційною системою (VIS) і системою Євродак. Основним завданням агенції eu-LISA є забезпечення ефективного, надійного і безперебійного функціонування інформаційно-технологічних систем. Вона також відповідає за здійснення необхідних заходів для гарантування безпеки систем і даних.

Шенгенська інформаційна система (SIS)

В 1985 році декілька держав-членів колишнього Європейського Співтовариства 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[845]. 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 тісну співпрацю між національними поліцейськими та судовими органами.

843 Див. вебсторінку про координацію нагляду *на сайті Європейського інспектора із захисту персональних даних.*

844 Регламент (ЄС) № 1077/2011 Європейського Парламенту та Ради від 25 жовтня 2011 р. про утворення Європейської агенції з питань широкомасштабних інформаційно-технологічних систем у сфері свободи, безпеки та юстиції, OJ 2011 L 286.

845 Угода між Урядами держав Економічного Союзу Бенілюкс, Федеративної Республіки Німеччини та Французької Республіки про поступове скасування перевірок на спільних кордонах, OJ 2000 L 239.

Внаслідок приєднання до Шенгенської угоди інших держав, Амстердамською угодою було остаточно інтегровано Шенгенську систему в правове поле ЄС[846]. 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 всі держави-члени ЄС[847], а також Ісландію, Ліхтенштейн, Норвегію та Швейцарію[848]. 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 використовує національну копію C-SIS, відому як Національна Шенгенська інформаційна система (N-SIS), яка постійно оновлюється і тим самим оновлює C-SIS. Система SIS видає попередження, якщо:

- особа не має права на в'їзд і перебування на території Шенгенської зони;
- особа чи об'єкт розшукуються судовими або правоохоронними органами (наприклад, європейський ордер на арешт, вимога проведення прихованих перевірок);
- особу визнано зниклою;
- про такі речі, як банкноти, автомобілі, фургони, вогнепальна зброя і документи, що засвідчують особу, було повідомлено як про викрадене або втрачене майно.

При отриманні попередження подальші кроки вчиняються із використанням обчислювального центру SIRENE. У SIS II є такі нові функції, як можливість внесення біометричних даних, таких як відбитки пальців і фотографії; або

846 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.

847 Хорватія, Кіпр та Ірландія здійснюють підготовчу роботу для інтеграції SIS II, але досі не є сторонами. Див. інформацію стосовно Шенгенської інформаційної системи, доступну *на вебсайті Генерального директорату Європейської Комісії щодо міграції та внутрішніх справ*.

848 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.

нові типи сигналів тривоги, наприклад, викрадені човни, літаки, контейнери чи платіжні засоби; посилені сигнали попередження про осіб та об'єкти; копії європейських ордерів на арешт (EAWs; ЄОА) осіб, які розшукуються з метою арешту, приведення до суду або екстрадиції.

SIS II ґрунтується на двох актах, що доповнюють один одного: Рішенні SIS II[849] та Регламенті SIS II[850]. Законодавець ЄС використав різні правові підходи для прийняття рішення та регламенту. Рішення регулює використання SIS II для цілей діяльності поліції та судового співробітництва в кримінальних питаннях (колишня третя підвалина діяльності ЄС). Регламент застосовується до процедури оповіщення щодо візової та імміграційної політики, політики надання притулку та інших питань, пов'язаних з вільним рухом осіб (колишня перша підвалина). Процедура оповіщення для кожної підвалини мала регулюватись окремим актом, оскільки ці два правові акти були ухвалені до Лісабонського договору та скасування структури підвалин.

Обидва правові акти містять правила захисту персональних даних. Рішення SIS II забороняє обробку чутливих даних[851]. Обробка персональних даних повинна регулюватись Оновленою Конвенцією 108[852]. Крім того, особи мають право на доступ до персональних даних, які їх стосуються, та які внесені до SIS II[853].

Регламент SIS II регулює умови та процедури для внесення та обробки сигнальних попереджень щодо відмов у в'їзді та перебуванні осіб, які не є громадянами ЄС. Він також передбачає правила обміну допоміжною та додатковою інформацією для цілей в'їзду або перебування в державі-члені[854]. Цей регламент також містить правила захисту персональних даних. Забороняється обробка чутливих даних, які передбачені статтею 9 (1) Загального регламенту захисту персональних даних[855]. Регламент SIS II також містить такі права суб'єкта даних:

849 Рішення Ради 2007/533/JHA від 12 червня 2007 р. про заснування, функціонування та використання Шенгенської інформаційної системи другого покоління (SIS II), OJ L, 7 серпня 2007р.

850 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, від 28 грудня 2006 р.

851 Рішення SIS II, стаття 56; Регламент SIS II, стаття 40.

852 Рішення SIS II, стаття 57.

853 Рішення SIS II, стаття 58; Регламент SIS II, стаття 41.

854 Регламент SIS II, стаття 2.

855 Там само, стаття 40.

- право на доступ до персональних даних, які належать суб'єкту даних[856];
- право на виправлення фактично неточних даних[857];
- право на видалення неправомірно збережених даних[858];
- право бути повідомленим, якщо проти суб'єкта даних було введено сигнал попередження. Інформація повинна бути надана в письмовій формі та супроводжуватися копією або посиланням на національне рішення щодо введення сигналу[859].

Право бути поінформованим не задовольняється, якщо: 1) персональні дані не були отримані від суб'єкта даних і надання такої інформації є неможливим або вимагає непропорційних зусиль; 2) суб'єкт даних вже володіє інформацією; 3) якщо національний закон дозволяє обмеження, що ґрунтуються, серед іншого, на міркуваннях національної безпеки або попередження кримінальних правопорушень[860].

Як відповідно до Рішення SIS II, так і відповідно до Регламенту SIS II, права доступу осіб щодо SIS II можуть бути реалізовані у будь-якій державі-члені, і відповідний запит має розглядатися згідно з законодавством держави-члена[861].

Приклад: у справі «*Даля проти Франції*»[862] заявнику було відмовлено у видачі візи для в'їзду до Франції, оскільки органи Франції повідомили Шенгенську інформаційну систему про те, що йому слід відмовити у в'їзді. Заявник безуспішно вимагав 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 надійшло відповідно до закону і переслідувало легітимну мету захисту національної безпеки. Оскільки заявник не довів, що він фактично постраждав в 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.

856 Там само, стаття 41 (1).

857 Там само, стаття 41 (5).

858 Там само, стаття 41 (5).

859 Там само, стаття 42 (1).

860 Там само, стаття 42 (2).

861 Регламент SIS II, стаття 41 (1) та рішення SIS II, стаття 58.

862 Рішення ЄСПЛ у справі «Даля проти Франції», (*Dalea v. France*), № 964/07, від 2 лютого 2010 р.

Компетентний національний контролюючий орган у кожній державі-члені здійснює нагляд за національною системою N-SIS. Національний контролюючий орган повинен забезпечити, щоб аудит операцій з обробки даних у національній N-SIS відбувався щонайменше кожні чотири роки[863]. Національний контролюючий орган та ЄІЗПД співпрацюють та забезпечують скоординований нагляд N-SIS, водночас ЄІЗПД відповідальний за нагляд над системою C-SIS. Заради прозорості кожні два роки до Європейського Парламенту, Ради та eu-LISA надсилається спільна доповідь про діяльність. Наглядово-координаційна група (SCG) системи SIS II була утворена для забезпечення координаційного нагляду за SIS та збирається двічі на рік. Ця група складається з ЄІЗПД та представників контролюючих органів тих держав-учасників, які імплементували SIS II, а також Ісландії, Ліхтенштейну, Норвегії та Швейцарії, оскільки до них також застосовується SIS II як до членів Шенгену[864]. Кіпр, Хорватія та Ірландія досі не є частиною SIS II та, відповідно, лише беруть участь як спостерігачі SCG. У контексті діяльності SCG ЄІЗПД та національні наглядові органи активно співпрацюють шляхом обміну інформацією, надання взаємної допомоги у проведенні аудитів та перевірок, проєктування узгоджених пропозицій для спільного вирішення потенційних проблем та забезпечення кращої поінформованості щодо прав захисту персональних даних[865]. SCG SIS II також надає методичні рекомендації для допомоги суб'єктам даних. Одним із прикладів є посібник для допомоги суб'єктам даних у реалізації їхніх прав на доступ[866].

Огляд

У 2016 році Європейська Комісія провела оцінку SIS[867], демонструючи, що були створені національні механізми для надання суб'єктам даних можливості доступу, виправлення та видалення своїх персональних даних у системі SIS II або можливості отримати компенсацію через неточність даних. Для вдосконалення дієздатності та ефективності SIS II Європейська Комісія запропонувала три позиції для регулювання:

863 Регламент SIS II, стаття 60 (2).

864 Див. *вебсторінку Шенгенської інформаційної системи* на сайті ЄІЗПД.

865 Регламент SIS II, стаття 46 та Рішення SIS II, стаття 62.

866 Див. SIS II SCG, *Шенгенська інформаційна система. Посібник реалізації права на доступ*, доступний на вебсайті ЄІЗПД.

867 Європейська Комісія (2016), Доповідь Комісії до Європейського Парламенту та Ради стосовно оцінки другого покоління Шенгенської інформаційної системи (SIS II) у відповідності до статтей 24 (5), 43 (3) та 50 (5) Регламенту (ЄС) № 1987/2006 та статті 59 (3) та 66 (5) Рішення 2007/533/ЈНА, COM(2016) 880 остаточне, Брюссель, від 21 грудня 2016 р.

- регламент щодо утворення, дії та використання SIS у сфері прикордонних перевірок, який замінить Регламент SIS II;
- регламент щодо утворення, дії та використання SIS у сфері поліцейського та судового співробітництва у кримінальних питаннях, який замінить, серед іншого, Рішення SIS II;
- регламент щодо використання SIS для повернення громадян третіх країн, які незаконно перебувають на території ЄС.

Важливо, що пропозиції на додаток до фотографій та відбитків пальців, які вже наразі є частиною системи SIS II, дозволяють обробку інших категорій біометричних даних. Розпізнавання обличчя, відбитки долоні та профілі ДНК також будуть зберігатись у базі даних SIS II. Крім того, Регламент SIS II та Рішення SIS II передбачали можливість здійснювати пошук за відбитками пальців для ідентифікації особи, а пропозиції передбачають цей пошук як обов'язковий у разі, якщо ідентифікувати особу в будь-який інший спосіб неможливо. Зображення обличчя, фото та відбитки долоні будуть використовуватися для пошукових систем та ідентифікації людей, коли це буде технічно можливим. Нові правила щодо біометричних даних становлять особливі ризики для прав осіб. У своєму висновку щодо пропозицій Комісії[868] ЄІЗПД зазначив, що біометричні дані є високо чутливими даними, і їх вміщення до такої масштабної бази даних має ґрунтуватися на науково підтвердженому фактами аналізі необхідності включення їх до системи SIS. Іншими словами, має бути продемонстрована необхідність обробки нових елементів. ЄІЗПД також вказав, що існує необхідність подальшого визначення типу інформації, яка може бути включена до профілю ДНК. Оскільки профіль ДНК може включати чутливу інформацію (яскравим прикладом такої інформації може бути інформація про стан здоров'я), профіль ДНК, який зберігається у системі SIS, повинен містити: «мінімальну інформацію, яка є виключно необхідною для ідентифікації зниклих осіб та недвозначно виключати інформацію про стан здоров'я, расову належність та іншу чутливу інформацію»[869]. Водночас пропозиції передбачають додаткові захисні гарантії для обмеження збору та подальшої обробки даних, які є вкрай необхідними та вимагаються для виконання завдань, а також доступ до таких даних дозволяється лише тим особам, які мають службову необхідність в обробці цих персональних

868 ЄІЗПД (2017), ЄІЗПД Висновок стосовно нової правової основи Шенгенської інформаційної системи, Висновок 7/2017, від 2 травня 2017 р.

869 Там само, п. 22.

даних[870]. Пропозиції також уповноважують Агенцію eu-LISA надавати висновки щодо якості даних для держав-членів з регулярною періодичністю для того, щоб регулярно перевіряти сигнали попередження для забезпечення якості даних[871].

Візова інформаційна система (VIS)

Візова інформаційна система (VIS), якою також управляє Агенція eu-LISA, була розроблена для забезпечення реалізації спільної візової політики ЄС[872]. VIS дозволяє державам-учасницям Шенгенської угоди обмінюватися візовими даними через систему, що 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.

Регламент № 767/2008 Європейського Парламенту і Ради (ЄС) щодо Візової інформаційної системи (VIS) та обміну даними між державами-членами щодо короткотермінових віз (Регламент VIS) передбачає умови та процедури передачі персональних даних стосовно заявок на короткотермінові візи. Вона також здійснює нагляд за прийнятими за цими заявками рішеннями, включаючи рішення про скасування, відкликання та продовження візи[873]. У VIS здебільшого містяться дані про заявника, його візи, фотографії, відбитки пальців, посилання на попередні заявки, а також інформація про осіб, які

870 Європейська Комісія (2016), Проєкт Регламенту Європейського Парламенту та Ради щодо створення функціонування та використання Шенгенської інформаційної системи (SIS) у сфері діяльності поліції та судового співробітництва у кримінальних питаннях, який змінює Регламент (ЄС) № 515/2014 та скасовує Регламент (ЄР) № 1986/2006, Рішення Ради 2007/533/JHA та Рішення Комісії 2010/261/EU, COM(2016) 883 остаточний, Брюссель, від 21 грудня 2016 р.

871 Там само, с. 15.

872 Рада Європейського Союзу (2004), Рішення Ради 2004/512/ЕС від 8 червня 2004 р. про створення інформаційної системи Visa (VIS), OJ 2004 L 213; Регламент (ЄР) № 767/2008 Європейського Парламенту та Ради від 9 липня 2008 р. про інформаційну систему Visa (VIS) та обмін даними між державами-членами про короткострокові візи, OJ 2008 L 218 (Регламент VIS); Рада Європейського Созу (2008), Рішення Ради 2008/633/JHA від 23 червня 2008 про доступ для ознайомлення з інформаційною системою (VIS) призначеними органами влади держав-членів та Європолом з метою попередження, виявлення та розслідування правопорушень, пов'язаних з тероризмом, та інших серйозних злочинів, OJ 2008 L 218.

873 Регламент VIS, стаття 1.

його супроводжують або запрошують[874]. Доступ до VIS для внесення, зміни або видалення даних надається виняткова візовим органам держав-членів, тоді як доступ для ознайомлення з даними надається візовим органам та установам, до компетенції яких входить перевірка зовнішніх пунктів перетину кордону, імміграційний контроль і надання притулку.

За певних обставин національні компетентні поліцейські органи і Європол можуть попросити доступу до даних, внесених у VIS з метою запобігання, виявлення і розслідування тероризму і кримінальних правопорушень[875]. Оскільки VIS була створена як інструмент для підтримки виконання спільної візової політики, у разі, якби вона перетворилася на правоохоронний інструмент, було б порушено принцип обмеження цілі, що, як пояснюється в розділі 3.2, вимагає, щоб обробка персональних даних здійснювалася виняткова для конкретних, чітких і законних цілей, а дані були адекватними, відповідними та ненадмірними щодо цілей, для яких вони обробляються. З цієї причини національні правоохоронні органи та Європол не мають доступу до VIS на загальній основі. Доступ може бути надано на основі індивідуального підходу та жорстких гарантій. Умови та гарантії доступу та ознайомлення цих органів з даними VIS врегульовано Рішенням Ради 2008/633/ЈНА[876].

Крім того, Регламент VIS передбачає права суб'єктів даних. До них належать:

- Право бути поінформованим відповідальною державою про ідентифікаційні та контактні дані контролера даних, уповноваженого здійснювати обробку даних у цій державі, про цілі майбутньої обробки в системі VIS, категорії осіб, яким можуть бути передані дані (отримувачі), а також період зберігання даних. Крім того, особи, що подають на візу, повинні бути поінформовані про факт того, що збір їхніх персональних даних за системою VIS є обов'язковим для розгляду їхньої заяви, водночас держава-член повинна також поінформувати суб'єктів щодо права на доступ до їхніх даних, право вимагати зміни або видалення та ознайомити з процедурами, які надають їм можливість реалізувати свої права[877].

874 Регламент (ЄР) № 767/2008 Європейського Парламенту та Ради від 9 липня 2008 р. про інформаційну систему Visa (VIS) та обмін даними між державами-членами про короткострокові візи, OJ 2008 L 218, (Регламент VIS).

875 Рада Європейського Союзу (2008), Рішення Ради 2008/633/ЈНА від 23 червня 2008 про доступ для ознайомлення з інформаційною системою (VIS) призначеними органами влади держав-членів та Європолом з метою попередження, виявлення та розслідування правопорушень, пов'язаних з тероризмом, та інших серйозних злочинів, OJ 2008 L 218.

876 Там само.

877 Регламент VIS, стаття 37.

- Право на доступ до персональних даних, які їх стосуються та які були внесені до системи VIS[878].
- Право на виправлення неточних даних[879].
- Право на видалення неправомірно збережених даних[880].

Для забезпечення нагляду за системою VIS, була утворена Наглядово-координаційна група (SCG). Вона складається з представників ЄІЗПД та національних контролюючих органів і збирається двічі на рік. Ця група включає представників 28 держав-членів ЄС та Ісландії, Ліхтенштейну, Норвегії та Швейцарії.

Євродак

Євродак означає європейська дактилоскопія[881]. Це централізована система, що містить дані про відбитки пальців громадян третіх країн та осіб без громадянства, які просять притулку в одній з держав-членів ЄС[882]. Система функціонує від січня 2003 року з прийняттям Регламенту Ради № 2725/2000, її оновлена версія функціонує з 2015 року. 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) № 604/2013, який встановлює критерії та механізми визначення держави-члена, відповідальної за розгляд заяви про надання притулку, поданої в одній із держав-членів громадянином третьої країни або особою без громадянства (Регламент

878 Там само, стаття 38 (1).

879 Там само, стаття 38 (2).

880 Там само, стаття 38 (2).

881 Див. *вебсторінку Євродак* на сайті ЄІЗПД.

882 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). Регламент (ЄС) № 603/2013 Європейського Парламенту та Ради від 26 червня 2013 року про заснування системи Євродак для порівняння відбитків пальців з метою ефективного застосування Регламенту (ЄС) 604/2013 щодо встановлення критеріїв та механізму визначення держави-члена, відповідальної за розгляд заяви про надання міжнародного захисту, поданої одній із держав-членів громадянином третьої країни або особою без громадянства, а також щодо вимоги про порівняння з даними системи Євродак, поданої правоохоронними органами держави-члена та Європолу для правоохоронних цілей, та про зміну Регламенту (ЄС) № 1077/2011 про утворення Європейської агенції з питань широкомасштабних інформаційно-технологічних систем у сфері свободи, безпеки та юстиції, OJ 2013 L 180, p. 1 (Регламент Євродак у новій редакції).

«Дублін III»)[883]. Основна мета персональних даних у системі Євродак – сприяти застосуванню Регламенту «Дублін III»[884].

Національним правоохоронним органам та Європолу дозволяється порівнювати відбитки пальців, пов'язані з кримінальними розслідуваннями, з тими, які містяться в системі Євродак, однак лише з метою попередження, виявлення або розслідування тероризму або інших серйозних кримінальних правопорушень. Оскільки Євродак було створено як інструмент для підтримки виконання політики ЄС з надання притулку, а не як правоохоронний інструмент, правоохоронні органи мають доступ до бази даних лише в особливих справах за особливих обставин та за жорстких умов[885]. Для подальшого використання даних в правоохоронних цілях застосовується Директива про захист персональних даних для поліції та органів кримінальної юстиції, тоді як використання даних для основної мети сприяння застосуванню Регламенту «Дублін III» захищене Загальним регламентом захисту персональних даних. Забороняється подальша передача персональних даних, отриманих державою-членом або Європолом відповідно до переглянутого Регламенту системи Євродак, будь-якій третій державі, міжнародній організації або приватній установі, зареєстрованій у ЄС або поза її межами[886].

Євродак 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 отримують і передають відбитки пальців кожної особи, яка досягла принаймні 14-річного віку та просить притулку на їхній території, а також кожної особи, яка не є громадянином ЄС або є особою без громадянства віком принаймні 14 років та яка затримана за несанкціонований перетин їхнього зовнішнього кордону. Держави-члени можуть також отримувати і передавати відбитки пальців осіб, що не є громадянами ЄС або не мають громадянства, якщо виявлено, що вони перебувають на їхній території без дозволу.

Хоча будь-які держави-члени можуть звертатися до системи Євродак та подавати запит на порівняння відбитків пальців, лише та держава-член, яка

883 Регламент (ЄС) № 603/2013 Європейського Парламенту та Ради від 26 червня 2013 року про заснування системи Євродак для порівняння відбитків пальців з метою ефективного застосування Регламенту (ЄС) 604/2013 щодо встановлення критеріїв та механізму визначення держави-члена, відповідальної за розгляд заяви про надання міжнародного захисту, поданої одній із держав-членів громадянином третьої країни або особою без громадянства, OJ 2013 L 180 (Регламент «Дублін III»).

884 Регламент щодо системи Євродак у новій редакції, OJ 2013 L 180, p. 1, стаття 1 (1).

885 Там само, стаття 1 (2).

886 Там само, стаття 35.

зібрала відбитки пальців та передала їх до центрального підрозділу, має право змінювати дані шляхом їх виправлення, доповнення або видалення[887]. Агенція eu-LISA веде записи всіх видів обробки даних для моніторингу захисту персональних даних та забезпечення безпеки даних[888]. Національні контролюючі органи допомагають та надають поради суб'єктам даних щодо реалізації їхніх прав[889]. Збір та передача відбитків пальців підлягають нагляду національних судів[890]. Регламент інститутів ЄС із захисту персональних даних[891] та нагляд ЄІЗПД застосовується до діяльності з обробки даних центральної системи, яка керується Агенцією eu-LISA щодо Євродак[892]. Якщо особа зазнає шкоди в результаті неправомірної операції з обробки даних або від будь-якої дії, яка несумісна з Регламентом Євродак, ця особа має право на відшкодування від держави-члена, відповідальної за шкоду[893]. Однак має бути наголошено, що особливо вразливою групою людей є шукачі притулку, яким нерідко доводиться здійснювати тривалу та небезпечну подорож. Тому з огляду на їхню вразливу та складну ситуацію реалізація їхніх прав, включаючи право на компенсацію, протягом часу розгляду заяв про надання притулку може виявитися складною.

Для використання системи Євродак в правоохоронних цілях держави-члени повинні призначити органи, які будуть мати право просити доступу, а також органи, які будуть перевіряти законність вимог про порівняння[894]. Доступ національних органів та Європолу до бази відбитків пальців Євродак підпорядкований жорстким умовам. Орган, який звертається, повинен надіслати обґрунтований електронний запит лише після порівняння даних з тими даними, які зберігаються в інших наявних інформаційних системах, наприклад національних базах відбитків пальців та VIS. Повинен існувати переважний інтерес громадської безпеки для того, щоб порівняння було визнане пропорційним. Порівняння повинно бути дійсно необхідним, стосуватися конкретної справи, а також мають бути обґрунтовані підстави вважати, що порівняння

887 Там само, стаття 27.

888 Там само, стаття 28.

889 Там само, стаття 29.

890 Там само, стаття 29.

891 Регламент (ЕС) № 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.

892 Регламент щодо системи Євродак у новій редакції, OJ 2013 L 180, p. 1, стаття 31.

893 Там само, стаття 37.

894 Рутс, Л. (2015), Новий Регламент щодо системи Євродак: відбитки пальців як джерело неформальної дискримінації, *Baltic Journal of European Studies Tallinn University of Technology*, Vol. 5, № 2, сс. 108–129.

суттєво сприятиме попередженню, виявленню або розслідуванню будь-якого кримінального правопорушення, яке розглядається, а саме якщо існує обґрунтована підозра, що підозрюваний, виконавець або жертва терористичного злочину або іншого серйозного злочину належать до категорії, на яку поширюється система збору відбитків пальців Євродак. Порівнюватися мають винятково відбитки пальців. Європол також має отримати дозвіл держави-члена, яка зібрала відповідні відбитки пальців.

Персональні дані в системі Євродак, які стосуються шукачів притулку, зберігаються протягом 10 років з дати відібрання відбитків пальців, якщо суб'єкт даних не набув громадянства держави-члена ЄС. У такому разі дані повинні бути негайно видалені. Дані, які стосуються іноземних громадян, затриманих за недозволений перетин зовнішнього кордону, зберігаються протягом 18 місяців. Ці дані мають бути видалені негайно після отримання суб'єктом даних дозволу на проживання, залишення території ЄС або отримання громадянства держави-члена. Дані осіб, які отримали притулок, залишаються наявними для порівняння протягом трьох років у контексті попередження, виявлення та розслідування тероризму та інших серйозних кримінальних злочинів.

Крім держав-членів, Ісландія, Норвегія, Ліхтенштейн та Швейцарія також застосовують Євродак на підставі міжнародних угод.

Було також утворено наглядово-координаційну групу для забезпечення нагляду за системою Євродак. Вона складається з представників ЄІЗПД та національних контролюючих органів, які зустрічаються двічі на рік. Ця група складається з 28 держав-членів ЄС та Ісландії, Ліхтенштейну, Норвегії та Швейцарії[895].

Огляд

У травні 2016 Комісія запропонувала проєкт для нового перегляду Регламенту Євродак як частини реформи, що має вдосконалити функціонування Спільної європейської системи шукачів притулку (СЄСШП; CEAS)[896]. Запропонований пе-

895 Див. *вебсторінку Євродак* на сайті ЄІЗПД.

896 Європейська Комісія, проєкт Регламенту Європейського Парламенту та Ради про утворення системи Євродак для порівняння відбитків пальців з метою ефективної імплементації [Регламенту (ЄС) 604/2013 щодо встановлення критеріїв та механізму визначення держави-члена, відповідальної за розгляд заяви про надання міжнародного захисту, поданої одній із держав-членів громадянином третьої країни або особою без громадянства, а також щодо вимоги про порівняння з даними системи Євродак, поданої правоохоронними органами держави-члена та Європолу для правоохоронних цілей], для ідентифікації громадянина третьої країни або особи без громадянства, яка незаконно перебуває на території та за вимогою про порівняння даних від правоохоронних органів держав-членів та Європолу для правоохоронних цілей COM(2016) 272 остаточний, від 4 травня 2016 р.

регляд важливий, оскільки він буде значно розширювати сферу дії початкової системи Євродак. Він був створений для забезпечення виконання СЄСШП шляхом надання доказів у вигляді відбитків пальців для визначення, яка саме держава-член є відповідальною за розгляд заяви про надання притулку, поданої до ЄС. Запропонований перегляд розширить обсяг бази даних для сприяння у поверненні незаконних мігрантів[897]. Національні органи матимуть можливість ознайомлюватися з даними для цілей ідентифікації громадян третіх країн, які нелегально перебувають на території ЄС, або тих, хто незаконно в'їхав на територію, для того щоб отримати докази та допомогти державам-членам повернути цих осіб. Крім того, якщо чинне регулювання вимагає лише збирання та зберігання відбитків пальців, дана пропозиція також уможливлює збір зображення обличчя осіб, що є іншим видом біометричних даних[898]. Пропозиція також знижує мінімальний вік дітей, біометричні дані яких можуть бути відібрані, з чинних відповідно до Регламенту (2013) 14 років до шести років[899]. Розширення обсягу пропозиції означає, що більша кількість осіб, які можуть бути включені до бази даних, зазнають втручання у свої права на приватне життя та на захист персональних даних. Для врівноваження цього втручання, пропозиція та зміни, запропоновані Комітетом Європейського арламенту з громадянських свобод, юстиції та внутрішніх справ (LIBE Committee)[900], посилюють інструменти захисту персональних даних. Станом на час написання цього посібника обговорення пропозиції Парламенту та Ради тривали.

---

897 Див. Пояснювальний меморандум до проєкту, с. 3.

898 Європейська Комісія, проєкт Регламенту Європейського Парламенту та Ради про утворення системи Євродак для порівняння відбитків пальців з метою ефективної імплементації [Регламенту (ЄС) 604/2013 щодо встановлення критеріїв та механізму визначення держави-члена, відповідальної за розгляд заяви про надання міжнародного захисту, поданої одній із держав-членів громадянином третьої країни або особою без громадянства, а також щодо вимоги про порівняння з даними системи Євродак, поданої правоохоронними органами держави-члена та Європолу для правоохоронних цілей], для ідентифікації громадянина третьої країни або особи без громадянства, яка незаконно перебуває на території та за вимогою про порівняння даних від правоохоронних органів держав-членів та Європолу для правоохоронних цілей COM(2016) 272 остаточний, від 4 травня 2016 р.(оновлена редакція) , стаття 2 (1).

899 Там само, стаття 2 (2).

900 Європейський Парламент, *Доповідь щодо проєкту регламенту Європейського Парламенту та Ради про утворення системи Євродак для порівняння відбитків пальців з метою ефективної імплементації [Регламенту (ЄС) 604/2013 щодо встановлення критеріїв та мехіназму визначення держави-члена, відповідальної за розгляд заяви про надання міжнародного захисту, поданої одній із держав-членів громадянином третьої країни або особою без громадянства, а також щодо вимоги про порівняння з даними системи Євродак, поданої правоохоронними органами держави-члена та Європолу для правоохоронних цілей], для ідентифікації громадянина третьої країни або особи без громадянства, яка незаконно перебуває на території та за вимогою про порівняння даних від правоохоронних органів держав-членів та Європолу для правоохоронних цілей* (оновлена редакція), PE 597.620v03-00, від 9 червня 2017 р.

Система спостереження за кордонами

Європейська система спостереження за кордонами (Eurosur)[901] 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 та Фронтексом, агенцією ЄС, що відповідає за розробку і застосування нової концепції інтегрованого управління кордонами[902]. 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, сприяючи запобіганню транскордонної злочинності[903].

Система Eurosur почала функціонувати 2 грудня 2013 року в усіх державах-членах, які мають зовнішні кордони, а з 1 грудня 2014 року – в інших державах-членах. Система застосовується для спостереження за зовнішніми кордонами на землі та морі, а також контролю за повітряними кордонами держав-членів. Система обмінюється персональними даними та здійснює їх обробку в дуже обмеженому обсязі, оскільки держави-члени та Frontex мають повноваження обмінюватися лише ідентифікаційними номерами суден. Eurosur обмінюється оперативною інформацією, такою як місцезнаходження патрулів та інцидентів, і за загальним правилом інформація, якою обмінюються, не може включати персональні дані[904]. У виняткових випадках, коли здійснюється обмін персональних даних у рамках Eurosur, правила

901 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.

902 Регламент (ЄС) № 2916/1624 Європейського Парламенту та Ради від 14 вересня 2016 р. про Європейську охорону земельних і морських кордонів та про зміну Регламенту (ЄС) 2016/399 Європейського Парламенту та Ради і відміну Регламенту (ЄС) № 863.2007 Європейського Парламенту та Ради, Регламенту Ради (ЄС) № 2007/2004 та Рішення Ради 2005/267/ЕС, OJ L 251.

903 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.

904 Європейська Комісія, *EUROSUR: Захист зовнішніх кордонів Шенгену – захист життя мігрантів. Коротко про EUROSUR,* від 29 листопада 2013 р.

передбачають застосування в повному обсязі загального правопорядку ЄС із захисту персональних даних[905].

Таким чином, Eurosur забезпечує право на захист персональних даних, підтверджуючи, що обмін персональними даними повинен відповідати критеріям та захисним гарантіям, передбаченим Директивою про захист персональних даних для поліції та органів кримінальної юстиції, та Загальним регламентом захисту персональних даних[906].

Митна інформаційна система

Іншою важливою спільною інформаційною системою, створеною на рівні ЄС, є Митна інформаційна система (CIS)[907]. У процесі формування внутрішнього ринку всі перевірки і формальності щодо товарів, які переміщуються територією ЄС, було скасовано, що призвело до підвищеного ризику шахрайства. Цьому ризику було протиставлено посилене співробітництво між органами керування митницями держав-членів. Метою CIS є надання державам-членам допомоги в запобіганні, розслідуванні та судовому переслідуванні серйозних порушень митних і сільськогосподарських нормативних актів держав-членів та ЄС. CIS було утворено двома правовими актами, прийнятими щодо різних юридичних сфер: Регламент Ради (ЄС) № 515/97, який стосується співробітництва між різними національними адміністративними органами для боротьби з шахрайством у контексті митного союзу та спільної сільськогосподарської політики, та Рішення Ради 2009/917/JHA, яке стосується допомоги у попередженні та розслідуванні серйозних порушень митного законодавства і переслідування за їх вчинення. Це означає, що CIS стосується не лише правоохоронної сфери.

Інформація, що міститься ув CIS, охоплює персональні дані стосовно сировинних матеріалів, транспортних засобів, підприємств, осіб, затриманих або заарештованих, конфіскованих товарів та готівкових коштів. Категорії даних, які можуть оброблятися, чітко визначені та включають прізвища,

905 Регламент 1052/2013, п. 13 преамбули та стаття 13.

906 Там само, п. 13 преамбули та стаття 13.

907 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).

національність, стать, місце та дату народження зацікавлених осіб, підстави їх внесення до системи та реєстраційний номер транспортних засобів[908]. Ця інформація може використовуватися винятково для цілей спостереження, звітування чи проведення конкретних перевірок або для здійснення стратегічного чи оперативного аналізу осіб, яких підозрюють у порушенні митних положень.

Доступ до CIS мають національні митні, податкові, сільськогосподарські органи, органи охорони здоров'я та поліції, а також Європол та Євроюст.

Обробка персональних даних повинна здійснюватись з дотриманням спеціальних правил, встановлених Регламентом №515/97 та Рішенням Ради 2009/917/JHA, а також з дотриманням положень Загального регламенту захисту персональних даних, Регламенту захисту персональних даних інститутами ЄС, Оновленої Конвенції 108 та Рекомендації щодо використання персональних даних поліцією. ЄІЗД несе відповідальність за нагляд над дотриманням CIS Регламенту (ЄС) № 45/2001 і щонайменше один раз на рік проводить зустріч усіх національних наглядових органів з питань захисту персональних даних, які є компетентними у питаннях, пов'язаних з CIS.

Взаємосумісність інформаційних систем ЄС

Управління міграцією, інтегроване управління зовнішніми кордонами ЄС та боротьба з тероризмом і транскордонною злочинністю породжують значні виклики та стають все більш складними в глобалізованому світі. Останні роки ЄС працює над розробкою нового комплексного підходу до захисних гарантій та підтримки безпеки без послаблення цінностей ЄС та основоположних прав. Ключовим у цих зусиллях є ефективний обмін інформацією між національними правоохоронними органами, а також між державами-членами та відповідними агенціями ЄС[909]. Інформаційні системи ЄС в царинах управління кордоном та внутрішньою безпекою мають свої завдання, інституційні засади,

908 Див. Рішення CIS, статті 24, 25 та 28.

909 Європейська Комісія (2016), Комюніке Комісії до Європейського Парламенту та Ради: Сильніша та розумніша інформаційна система для кордонів та безпеки COM(2016) 205 остаточне, Брюссель, від 6 квітня 2016 р., Європейська Комісія (2016), Комюніке Комісії Європейському Парламенту, Європейській Раді та Раді: посилення безпеки у світі мобільності: вдосконалений обмін інформацією у боротьбі з тероризмом та посилення зовнішніх кордонів, COM(2016) 602 остаточне, Брюссель, від 14 вересня 2016 р., Європейська Комісія (2016), Проєкт Регламенту Європейського Парламенту та ради про використання Шенгенської інформаційної системи для повернення громадян третіх країн, які незаконно перебувають на території. Див. також Комюніке Комісії до Європейського Парламенту, Європейської Ради та Ради: Сьома доповідь щодо досягнення справжнього та ефективного Союзу безпеки, COM(2017) 261 остаточне, Брюссель, від 16 травня 2017 р.

суб'єктів даних і користувачів. ЄС працює над подоланням недоліків у функціонуванні управління даними ЄС, розпорошеного між різними інформаційними системами, як-от SIS II, VIS та Євродак, досліджуючи потенційну взаємосумісність[910]. Головною метою є систематичне забезпечення компетентних органів поліції, митниці та суду необхідною інформацією для виконання їхніх обов'язків з дотриманням балансу між правом на приватність, правом на захист персональних даних та іншими основоположними правами.

Взаємосумісність – це «здатність інформаційних систем здійснювати обмін даними та можливість ділитись інформацією»[911]. Цей обмін не повинен ставити під сумнів необхідність жорстких правил щодо доступу та використання, передбачених Загальним регламентом захисту персональних даних, Директивою про захист персональних даних для поліції та органів кримінальної юстиції, Хартією основних прав ЄС та іншими дотичними документами. Будь-яке інтегроване рішення щодо управління даними не повинне впливати на принципи обмеження мети, захисту даних за призначенням або захисту даних за замовчуванням[912].

Для вдосконалення функціональних можливостей трьох головних інформаційних систем – SIS II, VIS та Євродак – Комісія запропонувала також створити четверту централізовану систему управління кордоном, спрямовану на громадян третіх країн: Система В'їзд-Виїзд (EES)[913], впровадження якої очікується у 2020 році[914]. Комісія також запропонувала утворити Європейську

910 Рада Європейського Союзу (2005), Гаазька програма: Посилення свободи, безпеки та справедливості в Європейському Союзі, OJ 2005 C 53, Європейська Комісія (2010), Комюніке Комісії до Європейського Парламенту та Ради: Огляд інформаційного управління у сфері свободи, безпеки та правосуддя, COM(2010) 385 остаточне, Європейська Комісія (2016), Комюніке Комісії до Європейського Парламенту та Ради: Сильніша та розумніша інформаційна система для кордонів та безпеки COM(2016) 205 остаточне, Брюссель, від 6 квітня 2016 р., Європейська Комісія (2016), Рішення Комісії від 17 червня 2016 р. про заснування Експертної групи високого рівня щодо інформаційних систем та взаємосумісності, OJ 2016 C 257.

911 Європейська Комісія (2016), Комюніке Комісії до Європейського Парламенту та Ради: Сильніша та розумніша інформаційна система для кордонів та безпеки COM(2016) 205 остаточне, Брюссель, від 6 квітня 2016 р., стор. 14.

912 Там само, сс. 4–5.

913 Європейська Комісія (2016), Проєкт Регламенту Європейського Парламенту та Ради про утворення Системи В'їзд-Виїзд (Entry/Exit System (EES) для реєстрації даних в'їзду і виїзду та даних щодо відмов громадянам третіх країн, які перетинають зовнішні корони держав-членів Європейського Союзу, у в'їзді та визначення умов доступу до EES для правоохоронних цілей, а також стосовно зміни Регламенту (ЄС) № 767/2008 та Регламенту (ЄU) № 1077/2011, COM(2016) 194 остаточний, Брюссель, від 6 квітня 2016 р.

914 Європейська Комісія (2016), Комюніке Комісії до Європейського Парламенту та Ради: Сильніша та розумніша інформаційна система для кордонів та безпеки COM(2016) 205 остаточне, Брюссель, від 6 квітня 2016 р., с. 5.

інформаційну систему з питань подорожей та дозволів (ETIAS)[915]. Ця система буде збирати інформацію про осіб, які подорожують безвізово до ЄС, для проведення завчасних перевірок щодо нелегальної міграції та безпеки.

915 Європейська Комісія (2016), Проєкт Регламенту Європейського Парламенту та Ради про утворення Європейської інформаційної системи подорожей та дозволів (ETIAS) та зміну регламентів (EU) № 515/2014, (EU) 2016/399, (EU) 2016/794 та (EU) 2016/1624, COM(2016) 731 остаточний, від 16 листопада 2016 р.

9 Окремі види персональних даних та їх відповідні правила захисту

ЄС	Питання, що висвітлюються	РЄ
Загальний регламент захисту персональних даних *Директива про конфіденційність та електронні комунікації*	**Електронні комунікації**	Оновлена Конвенція 108 Рекомендація щодо телекомунікаційних послуг
Загальний регламент захисту персональних даних, стаття 89	**Трудові відносини**	Оновлена Конвенція 108 Рекомендація щодо даних про працевлаштування
		ЄСПЛ, «Копланд проти Сполученого Королівства», (*Copland v. the United Kingdom*), № 62617/00, 2007 р.
Загальний регламент захисту персональних даних, стаття 9 (2) (h) та (i)	**Медичні дані**	Оновлена Конвенція 108 Рекомендація щодо медичних даних
		ЄСПЛ, «З. проти Фінляндії», (*Z v. Finland*), № 22009/93, 1997 р.
Регламент клінічних випробувань	**Клінічні випробування**	
Загальний регламент захисту персональних даних, стаття 6 (4), стаття 89	**Статистичні дані**	Оновлена Конвенція 108 Рекомендація щодо статистичних даних

ЄС	Питання, що висвітлюються	РЄ
Регламент (ЄС) № 223/2009 щодо європейської статистики Суд ЄС, C-524/06, «Гайнц Губер проти Федеративної Республіки Німеччини», (*Huber v. Bundesrepublik Deutschland*), 16 грудня 2008 р	**Офіційні статистичні дані**	Оновлена Конвенція 108 Рекомендація щодо статистичних даних
Директива 2014/65/ЄС про ринки фінансових інструментів *Регламент (ЄС) № 648/2012 щодо позабіржових деривативів, центральних контрагентів і торгових репозиторіїв* Регламент (ЄС) № 1060/2009 щодо кредитно-рейтингових агенцій Директива 2007/64/ЄС про платіжні послуги на внутрішньому ринку	**Фінансові дані**	Оновлена Конвенція 108 Рекомендація 90(19) щодо платежів та інших суміжних операцій ЄСПЛ, «Мішо проти Франції», (*Michaud v. France*), № 12323/11, 2012 р.

У декількох випадках на європейському рівні були прийняті спеціальні правові документи, у яких до конкретних ситуацій застосовуються загальні норми Оновленої Конвенції 108 або Загального регламенту захисту персональних даних більш деталізовано.

9.1 Електронні комунікації

Ключові моменти

- Спеціальні норми захисту персональних даних у сфері телекомунікацій з особливою увагою до телефонних послуг містяться в Рекомендації РЄ від 1995 року.
- Обробка персональних даних, що стосується надання комунікаційних послуг, на рівні ЄС регулюється Директивою про конфіденційність та електронні комунікації.
- Конфіденційність електронних комунікацій стосується не лише змісту спілкування, але й таких метаданих, як інформація про те, хто з ким, коли і як довго спілкувався, а також даних про місцезнаходження, наприклад, звідки надходили дані.

Комунікаційні мережі потенційно більше наражаються на небезпеку необґрунтованого втручання в особисту сферу користувачів, оскільки вони надають додаткові технічні можливості для прослуховування і спостереження за комунікаціями, що здійснюються в таких мережах. Внаслідок цього було визнано необхідним розробити спеціальні положення щодо захисту персональних даних для подолання специфічних 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[916]. 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 відправлення повідомлень прямого маркетингу. Як правило повідомлення прямого маркетингу не можуть надсилатися будь-якому абоненту, який явно відмовився від їх отримання. Автоматизовані пристрої здійснення дзвінків можуть використовуватися для передачі попередньо записаних повідомлень

916 Рада Європи, Комітет міністрів (1995), Рекомендація Rec(95)4 державам-учасницям щодо захисту персональних даних у сфері телекомунікаційних послуг, з особливими рекомендаціями для телефонних послуг, від 07 лютого 1995 р.

рекламного характеру лише за умови надання абонентом явно висловленої згоди. Національне законодавство повинно містити детальні правила в цій сфері.

У **законодавстві ЄС** перша спроба була здійснена в 1997 році, Директива про конфіденційність та електронні комунікації була прийнята у 2002 році, а в 2009 році до неї було внесено зміни. Це було зроблено з метою доповнення та конкретизації положень попередньої Директиви про захист даних у галузі телекомунікацій[917].

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, створених у процесі комунікації:

- дані, що становлять зміст повідомлень, відправлених у процесі комунікації; ці дані є суворо конфіденційними;
- дані, необхідні для встановлення і здійснення комунікації, так звані метадані (в Директиві вказуються як «дані трафіку»), такі як інформація про учасників комунікації, час і тривалість комунікації;
- серед метаданих 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 трафіку можуть використовуватися постачальником послуг лише для виставлення рахунків і технічного надання послуги. Втім, за наявності згоди суб'єкта персональних даних, ці дані можуть бути надані іншим контролерам, які пропонують такі додаткові послуги, як надання інформації, прив'язаної до місцезнаходження користувача, щодо найближчої станції метро чи аптеки, чи прогнозу погоди для цього місця.

Відповідно до статті 15 Директиви про конфіденційність та електронні комунікації, інші випадки доступу до інформації про комунікацію в електронних

917 Директива 2002/58/ЕС Європейського Парламенту та Ради від 12 липня 2002 стосовно обробки персональних даних і захисту приватності у сфері електронних комунікацій, OJ 2002 L 201 (Директива про конфіденційність та електронні комунікації) із змінами, внесеними Директивою 2009/136/ЕС Європейського Парламенту та Ради від 25 листопада 2009 про внесення змін до Директиви 2002/22/ЕС про універсальну послугу та права користувачів, що стосуються електронних комунікаційних мереж і послуг, Директиви 2002/58/ЕС стосовно обробки персональних даних і захисту приватності у сфері електронних комунікацій та Регламенту (ЕС) № 2006/2004 про співробітництво між національними органами влади, відповідальними за виконання законів про захист прав споживачів, OJ 2009 L 337.

мережах повинні задовольняти вимоги щодо виправданого втручання у право на захист даних, як передбачено статтею 8 (2) ЄКПЛ та підтверджено в статтях 8 і 52 Хартії основних прав ЄС. Такий доступ може включати доступ в цілях розслідування злочинів.

Поправки 2009 року до Директиви про конфіденційність та електронні комунікації[918] внесли такі зміни:

- Обмеження на відправку електронних листів з метою прямого маркетингу було поширено на сервіси коротких повідомлень, сервіси передачі мультимедійних повідомлень та інші сфери подібного застосування; надсилання електронних листів з метою маркетингу забороняється, якщо лише для цього не було отримано попередню згоду. Без такої згоди електронні листи з метою маркетингу можуть надсилатися лише попереднім клієнтам, якщо вони надали свою поштову адресу і не заперечують проти цього.
- На держави-члени було покладено зобов'язання забезпечувати засоби судового захисту від порушень заборони на розсилку незапитуваних повідомлень[919].
- 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 регулювати форми висловлення та отримання згоди для забезпечення достатнього захисту[920].

Якщо внаслідок несанкціонованого доступу, втрати або знищення даних відбувається витік даних, про це повинен бути негайно поінформований компетентний контролюючий орган. Абоненти мають бути поінформовані, якщо шкода, яка їм могла бути завдана, є наслідком витоку даних[921].

---

918 Директива 2009/136/ЕС Європейського Парламенту і Ради від 25 листопада 2009 р. про внесення змін до Директиви 2002/22/ЕС про універсальну послугу та права користувачів, що стосуються електронних комунікаційних мереж і послуг, Директиви 2002/58/ЕС стосовно обробки персональних даних і захисту приватності у сфері електронних комунікацій та Регламенту (ЕС) № 2006/2004 про співробітництво між національними органами влади, відповідальними за виконання законів про захист прав споживачів, OJ 2009 L 337.

919 Див. змінену Директиву, стаття 13.

920 Див. там само, стаття 5; див. також Робоча група «Стаття 29» (2012), *Висновок 04/2012 про звільнення від вимоги отримання згоди для застосування файлів cookie*, РГ 194, Брюссель, від 07 червня 2012 р.

921 Див. також Робоча група «Стаття 29» (2011), *Робочий документ 01/2011 про чинну нормативну базу ЄС з питань витоку персональних даних та рекомендації щодо подальшого розвитку політики*, РГ 184, Брюссель, від 05 квітня 2011 р.

Директива про зберігання даних[922] зобов'язувала постачальників комунікаційних послуг зберігати метадані. Однак цю Директиву було визнано нечинною СЄС (щодо більш детальної інформації див. *розділ 8.3*).

Огляд

У січні 2017 року Європейська Комісія прийняла новий проєкт регламенту про конфіденційність та електронні комунікації на заміну попередньої Директиви. Метою залишатиметься захист «основних прав та свобод фізичних і юридичних осіб під час надання та використання електронних комунікаційних послуг та, зокрема, права на повагу до приватного життя і кореспонденції та захист фізичних осіб щодо обробки персональних даних». Водночас новий проєкт має забезпечувати вільне переміщення даних електронних комунікацій та послуг електронного зв'язку в межах ЄС[923]. Хоча Загальний регламент захисту персональних даних головним чином стосується статті 8 Хартії основних прав ЄС, запропонований регламент має на меті зробити статтю 7 Хартії частиною вторинного законодавства ЄС.

Регламент адаптуватиме положення попередньої Директиви до нових технологій і ринкової реальності та створить комплексну структуру, узгоджену з Загальним регламентом захисту персональних даних. У цьому сенсі регламент про конфіденційність та електронні комунікації буде *lex specialis* по відношенню до Загального регламенту захисту персональних даних, адаптуючи його до даних електронного зв'язку, які є персональними даними. Новий Регламент поширюється на обробку «даних електронного зв'язку», що включають зміст електронних комунікацій та метадані, які необов'язково є персональними даними. Територіальна сфера дії обмежується ЄС, зокрема якщо отримані в ЄС дані обробляються поза його межами, та поширюється на постачальників зв'язку через інтернет. Це постачальники, що надають контент, послуги чи програми через мережу інтернет без прямого залучення оператора чи провайдера послуг інтернету (ППІ; ISP). Прикладами таких провайдерів є «Skype» (голосові та відеодзвінки), «WhatsApp» (обмін повідомленнями), «Google» (пошук), «Spotify» (музика) чи «Netflix» (відеоконтент). Механізми забезпечення

922 Директива 2006/24/ЕС Європейського Парламенту і Ради від 15 березня 2006 р. про збереження даних, які створюються чи обробляються при наданні загальнодоступних послуг електронних комунікацій чи публічних мереж зв'язку, яка вносить зміни до Директиви 2002/58/ЕС, OJ 2006 L 105.

923 Проєкт Регламенту Європейського Парламенту і Ради стосовно поваги до приватного життя та захисту персональних даних в електронних комунікаціях та скасування Директиви 2002/58/ЕС (Регламент про конфіденційність та електронні комунікації) (COM(2017) 10 остаточний), стаття 1.

дотримання Загального регламенту захисту персональних даних будуть застосовуватися до нового регламенту.

Регламент про конфіденційність та електронні комунікації прийнято 2018 року, до того часу Загальний регламент захисту персональних даних застосовувався в усіх 28 державах-членах. Втім це залежало від згоди як Європейського Парламенту, так і Ради[924].

9.2 Дані про працевлаштування

Ключові моменти

- Спеціальні правила захисту персональних даних у трудових відносинах окреслені в Рекомендації РЄ щодо даних працевлаштування.
- У Загальному регламенті захисту персональних даних трудові відносини конкретно згадуються лише в контексті обробки чутливих даних.
- Дійсність згоди, яка мала бути вільно наданою, як правова підстава для обробки даних щодо працівників може бути сумнівною, враховуючи відсутність економічної рівноваги між роботодавцем та працівниками. Обставини надання згоди потрібно ретельно оцінювати.

Обробка даних у контексті працевлаштування підпадає під загальне законодавче регулювання ЄС питань захисту персональних даних. Однак один Регламент[925] конкретно стосується захисту обробки персональних даних Європейськими інституціями в контексті працевлаштування (серед інших питань). У Загальному регламенті захисту персональних даних трудові відносини згадуються у статті 9 (2), де зазначено, що персональні дані можуть оброблятися під час виконання обов'язків чи реалізації окремих прав контролера чи суб'єкта даних у сфері зайнятості.

Відповідно до Загального регламенту захисту персональних даних, працівник повинен мати можливість чітко виокремлювати дані, на обробку/зберігання

924 Для отримання більше інформації див. Європейська Комісія (2017), «*Комісія пропонує високий рівень правил приватності для всіх електронних комунікацій та оновлює правила захисту персональних даних для установ ЄС*», пресреліз, від 10 січня 2017.

925 Регламент (ЕС) № 45/2001 Європейського Парламенту і Ради від 18 грудня 2000 про захист фізичних осіб у зв'язку з обробкою персональних даних інституціями та органами Співдружності і про вільне переміщення таких даних, OJ 2001 L 8.

яких він чи вона погоджується, та цілі, задля яких його чи її дані зберігаються. Працівники також до моменту надання згоди мають бути поінформовані про свої права та тривалість зберігання їхніх даних. У разі витоку персональних даних, що може призвести до високого ризику для прав і свобод фізичних осіб, роботодавець має повідомити про цей витік працівника. Стаття 88 Регламенту дозволяє державам-членам запроваджувати конкретніші правила для забезпечення захисту прав і свобод працівників щодо їхніх персональних даних у контексті працевлаштування.

Приклад: у справі «*Вортен*»[926] дані включали записи робочого часу, що містили інформацію про щоденні періоди роботи та періоди відпочинку, які є персональними даними. Національним законодавством може вимагатися надання роботодавцем доступу до записів робочого часу державним органам, що здійснюють моніторинг умов праці. Це дозволяє отримати негайний доступ до відповідних персональних даних. Однак доступ до персональних даних є необхідним для надання можливості національним органам здійснювати контроль за дотриманням законодавства щодо умов праці[927].

Що стосується **РЄ,** то 1989 року була видана, а 2015 року переглянута Рекомендація щодо даних працевлаштування[928]. Рекомендація охоплює обробку персональних даних в цілях працевлаштування, як у державному, так і приватному секторі. Обробка має відповідати певним принципам та обмеженням, таким як принцип прозорості та консультації з представниками працівників перед встановленням системи нагляду на робочому місці. У Рекомендації також зазначено, що роботодавці повинні застосовувати превентивні заходи, наприклад замість відстеження, як їхні працівники користуються інтернетом, застосовувати фільтри.

Огляд найпоширеніших проблем захисту персональних даних, характерних для контексту працевлаштування, можна знайти в робочому документі Робочої групи «Стаття 29»[929]. Робоча група проаналізувала значення згоди

926 Суд ЄС, C-342/12, «"Worten – Home Equipment SA" проти Контролюючого органу з дотримання умов праці» (*Worten–Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT)*), від 30 травня 2013 р., п. 19.

927 Там само, п. 43.

928 Рада Європи, Комітет міністрів (2015), Рекомендація Rec(2015)5 державам-учасницям про обробку персональних даних у контексті зайнятості, квітень 2015 р.

929 Робоча група «Стаття 29» (2017), *Висновок 2/2017 про обробку персональних даних на роботі*, РГ 249, Брюссель, від 08 червня 2017р.

як правової підстави для обробки даних про зайнятість[930]. Вона виявила, 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. У зв'язку з цим, оцінюючи дійсність згоди в контексті працевлаштування, необхідно уважно розглянути умови, за яких згода використовується як юридична підстава обробки даних.

Загальною проблемою захисту персональних даних у сьогоднішньому типовому робочому середовищі є обсяг правомірного контролю за електронною комунікацією працівників 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. У цьому контексті особливо цікавими є рішення ЄСПЛ у справах *«Копланд проти Сполученого Королівства»* та *«Барбулеску проти Румунії»*.

Приклад: у справі *«Копланд проти Сполученого Королівства»*[931] за використанням працівницею коледжу телефону, електронної пошти та інтернету здійснювався прихований контроль з метою з'ясування, чи було з її боку надмірним використання обладнання коледжу в особистих цілях. ЄСПЛ постановив, що телефонні дзвінки, здійснені у службових приміщеннях, підпадають під поняття приватного життя і таємницю кореспонденції. Тому такі дзвінки та електронні листи, надіслані з роботи, а також інформація, отримана в результаті моніторингу персонального використання інтернету, захищені статтею 8 ЄКПЛ. У справі заявниці не існувало жодних положень, які б регламентували 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.

Приклад: у справі *«Барбулеску проти Румунії»*[932] заявника було звільнено за використання інтернету за місцем його роботи в робочий час з порушенням внутрішніх правил. Роботодавець відслідковував його

930 Робоча група «Стаття 29» (2005), *Робочий документ про загальне тлумачення статті 26(1) Директиви 95/46/ЕС від 24 жовтня 1995 р.*, РГ 114, Брюссель, від 25 листопада 2005 р.

931 Рішення ЄСПЛ у справі «Копланд проти Сполученого Королівства» (*Copland v. the United Kingdom*), № 62617/00, від 03 квітня 2007 р.

932 Рішення ЄСПЛ у справі «Барбулеску проти Румунії» (*Bărbulescu v. Romania* [GC]), № 61496/08, від 05 вересня 2017 р., п. 121.

комунікації. Під час провадження в суді країни були представлені записи, які відображали повідомлення суто приватного характеру. Встановлюючи застосовність статті 8, ЄСПЛ лишив відкритим питання, чи міг заявник достатньою мірою очікувати на конфіденційність з огляду на встановлені роботодавцем обмежувальні правила, однак Суд постановив, що правила роботодавця не можуть зводити нанівець приватне соціальне життя на робочому місці.

Щодо суті, Договірні Сторони повинні мати свободу розсуду у визначенні необхідності запровадження нормативних документів, які обумовлюватимуть умови, за яких роботодавець може регламентувати електронні чи інші комунікації непрофесійного характеру своїх працівників на робочому місці. Проте національні органи повинні були забезпечити, щоб запровадження роботодавцем заходів щодо моніторингу листування та інших комунікацій, незалежно від обсягу та тривалості таких заходів, супроводжувалося належними та достатніми гарантіями проти зловживань. Пропорційність та процедурні гарантії проти свавілля є дуже важливими, і ЄСПЛ визначив низку факторів, що були суттєвими в даних обставинах. До них належать, серед іншого, обсяг перевірки роботодавцем і ступінь втручання в приватне життя працівника, наслідки для працівника, та чи були забезпечені належні гарантії. Крім того, національні органи мали забезпечити, щоб працівник, спілкування якого відстежувалося, мав доступ до захисту в суді, що мав би повноваження визначати, щонайменше по суті, яким чином було дотримано зазначених критеріїв та чи були оскаржувані заходи правомірними.

У цій справі ЄСПЛ встановив порушення статті 8, оскільки національні органи не надали належного захисту праву заявника на повагу до приватного життя і кореспонденції, внаслідок чого не змогли досягти справедливого балансу між інтересами, що розглядалися.

Відповідно до Рекомендації РЄ щодо даних про працевлаштування, персональні дані, що збираються в цілях працевлаштування, повинні бути отримані безпосередньо від працівника.

Персональні дані, що збираються для найму, повинні обмежуватися інформацією, необхідною для оцінки придатності кандидатів та їхнього кар'єрного потенціалу.

У Рекомендації також окремо вказано на оціночні дані, які стосуються продуктивності або потенціалу окремих працівників. Оціночні дані повинні ґрунтуватися на справедливих та чесних висновках і не повинні бути образливими у своєму формулюванні. Цього вимагають принципи чесної обробки і точності даних.

Особливим аспектом законодавства щодо захисту персональних даних у відносинах між роботодавцем і працівниками є роль представників працівників. Такі представники можуть отримати персональні дані працівників лише в обсязі, необхідному для того, щоб мати можливість представляти інтереси працівників, або якщо такі дані необхідні для виконання чи контролю за зобов'язаннями, передбаченими колективними договорами.

Чутливі дані, зібрані в цілях працевлаштування, можуть оброблятися лише в окремих випадках і згідно з гарантіями, передбаченими в національному законодавстві. Роботодавці можуть запитувати працівників або кандидатів на посаду про стан їхнього здоров'я або організовувати їхній медичний огляд лише за необхідності. Це може бути зроблено для визначення придатності для працевлаштування, дотримання вимог профілактичної медицини, захисту життєво важливих інтересів суб'єкта даних чи інших працівників та фізичних осіб, надання дозволу на призначення соціальних пільг чи надання відповіді на судові запити. Дані про стан здоров'я не можуть збиратися з інших джерел, окрім як отримуватися від відповідного працівника, за винятком випадків, коли було отримано явно висловлену та поінформовану згоду, або якщо це передбачено національним законодавством.

Згідно з Рекомендацією щодо даних про працевлаштування, працівники повинні бути поінформовані про мету обробки їхніх персональних даних, тип персональних даних, що збираються, суб'єктів, яким регулярно повідомляються дані, мету та правову підставу такого розкриття. Доступ до електронних комунікацій на робочому місці може здійснюватися лише з міркувань безпеки чи з інших легітимних підстав, і дозволяється лише після інформування працівників про те, що роботодавець може мати доступ до такого способу спілкування.

Працівники повинні мати право на доступ до своїх даних щодо працевлаштування, а також право на їх виправлення чи видалення. Якщо обробляються оціночні дані, працівники також повинні мати право на оскарження цієї оцінки. Втім, ці права можуть тимчасово обмежуватися з метою проведення внутрішніх розслідувань. Якщо працівнику було відмовлено в наданні доступу, виправленні або видаленні персональних даних щодо працевлаштування, національне законодавство має передбачати належні процедури оскарження відмови.

9.3 Дані про стан здоров'я

Ключовий момент

- Медичні дані є чутливими даними, а відтак їм надається особливий захист.

Згідно зі статтею 9 (1) Загального регламенту захисту персональних даних та статті 6 Оновленої Конвенції 108, персональні дані стосовно стану здоров'я суб'єкта даних кваліфікуються як чутливі дані. Відповідно, дані стосовно стану здоров'я підлягають суворішому режиму обробки, ніж нечутливі дані. Загальним регламентом захисту персональних даних заборонено обробку «персональних даних стосовно стану здоров'я» (маються на увазі «всі дані, що пов'язані зі станом здоров'я суб'єкта даних і розкривають інформацію про минулий, поточний або майбутній стан фізичного чи психічного здоров'я суб'єкта даних)[933], а також генетичних даних і біометричних даних, крім випадків, коли це дозволено статтею 9 (2). Обидва типи даних були додані до списку «спеціальних категорій даних»[934].

Приклад: у справі *«З. проти Фінляндії»*[935] колишній чоловік заявниці, який жив з ВІЛ, скоїв низку статевих злочинів. Згодом його було засуджено за вбивство через необережність на тій підставі, що він свідомо піддавав своїх жертв ризику інфікування ВІЛ. Національний суд розпорядився, щоб повне рішення і документи справи залишалися конфіденційними протягом 10 років, незважаючи на вимоги заявниці щодо встановлення тривалішого періоду конфіденційності. Апеляційний суд відмовив у задоволенні цих вимог, а його рішення містило повні імена заявниці та її колишнього чоловіка. ЄСПЛ постановив, що втручання не вважалося необхідним у демократичному суспільстві, оскільки захист

933 Загальний регламент захисту персональних даних, п. 35 Преамбули.

934 Там само, стаття 2.

935 Рішення ЄСПЛ у справі «З. проти Фінляндії» (*Z v. Finland*), № 22009/93, від 25 лютого 1997 р., пп. 94 та 112; див. також рішення ЄСПЛ у справі «М. С. проти Швеції» (*M. S. v. Sweden*), № 20837/92, від 27 серпня 1997 р.; рішення ЄСПЛ у справі «Л.Л. проти Франції» (*L.L. v. France*), № 7508/02, від 10 жовтня 2006р.; рішення ЄСПЛ у справі «І. проти Фінляндії» (*I v. Finland*), № 20511/03, від 17 липня 2008 р.; рішення ЄСПЛ у справі «К. Г. та інші проти Словаччини» (*K. H. and Others v. Slovakia*), № 32881/04, від 28 квітня 2009 р.; рішення ЄСПЛ у справі «Жулук проти Сполученого Королівства» (*Szuluk v. the United Kingdom*), № 36936/05, від 2 червня 2009 р.

медичних даних має фундаментальне значення для здійснення права на повагу до приватного і сімейного життя, особливо коли йдеться про інформацію щодо ВІЛ-інфекції з огляду на стигматизацію, що супроводжує цю хворобу в багатьох суспільствах. Таким чином, Суд дійшов висновку, що надання доступу до інформації про особу заявника і стан його здоров'я, як це мало місце в рішенні апеляційного суду після завершення 10-річного періоду з часу прийняття рішення, порушувало статтю 8 ЄКПЛ.

Відповідно до **законодавства ЄС,** стаття 9 (2) (h) Загального регламенту захисту персональних даних дозволяє обробку медичних даних, якщо вона є необхідною в цілях профілактичної медицини, медичної діагностики, надання медичної допомоги чи лікування або для керування послугами у сфері охорони здоров'я. Проте обробка є допустимою лише тоді, коли вона здійснюється медичним працівником, який зобов'язаний дотримуватися професійної таємниці, або іншою особою, на яку поширюється подібне зобов'язання[936].

Відповідно до **права РЄ,** Рекомендація РЄ щодо медичних даних від 1997 року більш докладно застосовує принципи Конвенції 108 до обробки даних у сфері медицини[937]. Запропоновані норми відповідають нормам Загального регламенту захисту персональних даних щодо легітимних цілей обробки медичних даних, необхідності зберігати професійну таємницю особами, які використовують дані, обов'язку, а також прав суб'єктів даних на прозорість і доступ, виправлення та видалення даних. Більше того, медичні дані, які на законних підставах обробляють медичні працівники, не можуть передаватися правоохоронним органам, якщо не надано «належного захисту, що дозволяє запобігти передачі даних з порушенням принципу поваги до [...] приватного життя, гарантованого статтею 8 ЄКПЛ»[938]. Національне законодавство також має бути «сформульовано з достатньою чіткістю та надавати належний правовий захист від свавілля»[939].

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 для

936 Див. також ЄСПЛ, «Бірюк проти Литви» (*Biriuk v. Lithuania*), № 23373/03, від 25 листопада 2008 р.

937 Рада Європи, Комітет міністрів (1997), Рекомендація Rec(97)5 державам-учасницям щодо захисту медичних даних, від 13 лютого 1997. Зверніть увагу, що ця Рекомендація наразі переглядається.

938 Рішення ЄСПЛ у справі «Авілкіна проти Росії» (*Avilkina and Others v. Russia*), № 1585/09, від 06 червня 2013 р., п. 53. Див. також рішення ЄСПЛ у справі «Бірюк проти Литви» (*Biriuk v. Lithuania*), № 23373/03, від 25 листопада 2008 р.

939 Рішення ЄСПЛ у справі «Л. Г. проти Латвії» (*L. H. v. Latvia*), № 52019/07, від 29 квітня 2014 р., п. 59.

зберігання даних довше, ніж вони є необхідними, хоча це зазвичай вимагає знеособлення. Стаття 12 Рекомендації щодо медичних даних пропонує детальні інструкції для ситуацій, коли дослідникам потрібні персональні дані, а знеособлених даних недостатньо.

Псевдонімізація може бути належним засобом задоволення наукових потреб і водночас захисту інтересів відповідних пацієнтів. У контексті захисту даних поняття псевдонімізації більш докладно пояснюється в розділі 2.1.1.

Рекомендація РЄ 2016 року щодо даних, отриманих в результаті проведення генетичних тестів, також застосовується до обробки персональних даних у медичній сфері[940]. Ця Рекомендація має велике значення для системи «Електронне здоров'я» (eHealth), у якій інформаційно-телекомунікаційні технології використовуються для сприяння наданню медичної допомоги. Прикладом є пересилання результатів тесту на батьківство пацієнта від одного медичного працівника до іншого. Ця Рекомендація спрямована на захист прав осіб, персональні дані яких обробляються в цілях страхування, щоб застрахувати від ризиків, пов'язаних зі здоров'ям особи, її фізичною цілісністю, віком чи смертю. Обробка даних, пов'язаних зі станом здоров'я, повинна бути обґрунтованою страховиками та пропорційною характеру і важливості відповідного ризику. Обробка такого роду даних залежить від згоди суб'єкта даних. Страховики також повинні застосовувати заходи безпеки для зберігання даних, пов'язаних зі станом здоров'я.

Клінічні випробування, які передбачають оцінку впливу нових лікарських засобів на пацієнтів у документально зафіксованих дослідженнях, мають значні наслідки для захисту даних. Проведення клінічних випробувань лікарських засобів для вживання людьми регулюється Регламентом (ЄС) № 536/2014 Європейського Парламенту і Ради від 16 квітня 2014 року щодо клінічних випробувань лікарських засобів для вживання людьми, який скасував Директиву 2001/20/ЕС (Регламент клінічних випробувань)[941]. Головними елементами Регламенту клінічних випробувань є:

- спрощена процедура подання заяв через портал ЄС[942];

940 Рада Європи, Комітет міністрів (2016), Рекомендація Rec(2016)8 державам-учасницям щодо обробки персональних даних, які пов'язані зі станом здоров'я, в цілях страхування, в тому числі даних, отриманих в результаті проведення генетичних тестів, від 26 жовтня 2016 р.

941 Регламент (ЄС) № 536/2014 Європейського Парламенту і Ради від 16 квітня 2014 р. щодо клінічних випробувань лікарських засобів для вживання людьми та скасування Директиви 2001/20/ЕС (Регламент щодо клінічних випробувань), OJ 2014 L 158.

942 Регламент щодо клінічних випробувань, стаття 5 (1).

- строки оцінки заяв на клінічні випробування[943];
- комітет з питань етики, який є частиною процесу оцінювання, відповідно до законодавства держави-члена (та Європейського законодавства, що визначає відповідні періоди часу)[944]; та
- більша прозорість клінічних випробувань та їхніх результатів[945].

Загальний регламент захисту персональних даних вказує, що для надання згоди на участь у науково-дослідницькій діяльності в ході клінічних випробувань застосовується Регламент (ЄС) 536/2014[946].

На рівні ЄС на розгляді перебуває ще багато законодавчих та інших ініціатив щодо персональних даних у сфері охорони здоров'я[947].

Електронні медичні записи

Електронні медичні записи визначаються як «повна медична карта чи подібна документація в електронній формі про минулий та теперішній фізичний і психічний стан здоров'я фізичної особи, яка забезпечує безпосередній доступ до цих даних для медичного лікування та інших тісно пов'язаних цілей»[948]. Електронні медичні записи є електронною версією історії хвороби пацієнтів, яка може містити такі клінічні дані цих осіб, як минула історія хвороби, проблеми та умови, призначені медикаменти та лікування, а також результати та звіти обстежень і лабораторних досліджень. До таких електронних файлів, які можуть варіюватися від детальних записів до простих витягів або короткого викладу, можуть мати доступ терапевт, фармацевт та інші медичні працівники. Поняття 'eHealth' також зачіпає ці медичні записи.

Приклад: пан А отримав страховий поліс компанії В (страховик). Останній отримуватиме від пана А певну інформацію щодо його стану здоров'я, наприклад про поточні проблеми зі здоров'ям чи захворювання.

943 Там само, стаття 5 (2)–(5).

944 Там само, стаття 2 частина 2 (11).

945 Там само, стаття 9 (1) та п. 67 преамбули.

946 Загальний регламент захисту персональних даних, пп. 156 та 161 преамбули.

947 ЄІЗПД (2013), *Висновок Європейського інспектора із захисту даних щодо Комюніке Комісії стосовно Плану дій «eHealth на 2012–2020 роки – Інноваційна система охорони здоров'я в 21 столітті»*, Брюссель, від 27 березня 2013 р.

948 Рекомендація Комісії від 02 липня 2008 щодо транскордонної інтероперабельності електронних систем медичних записів, п. 3 (c).

Страховик має зберігати персональні дані, що пов'язані зі станом здоров'я, окремо від інших даних. Крім того, страховик має їх зберігати окремо від інших персональних даних. Це означає, що лише працівник, який веде справу пана А, матиме доступ до даних стосовно його здоров'я.

Однак виникають певні питання щодо захисту персональних даних у зв'язку з веденням електронних медичних файлів, наприклад про їхню доступність, належне зберігання та доступ суб'єктів даних до них.

Окрім електронних медичних записів, 10 квітня 2014 року Європейська Комісія опублікувала Зелену книгу про мобільне здоров'я (mHealth), вважаючи, що mHealth – це напрямок, який починає своє існування і швидко розвивається та може вдосконалити систему охорони здоров'я, підвищити її ефективність та якість. Цей термін охоплює медичну практику та систему охорони здоров'я населення, яка підтримується мобільними пристроями, наприклад мобільними телефонами, пристроями моніторингу пацієнтів, персональними цифровими помічниками та іншими бездротовими пристроями, а також комп'ютерними програмами (наприклад, для покращання самопочуття), які можуть підключатись до медичних пристроїв або датчиків[949]. У документі окреслено ризики, які може спричинити розвиток mHealth для права на захист персональних даних, та зазначено, що з огляду на чутливий характер медичних даних його розробка повинна містити конкретні та відповідні гарантії безпеки даних пацієнтів, наприклад шифрування, та належні механізми ідентифікації пацієнтів з метою зменшення ризиків для безпеки. Дотримання правил захисту персональних даних, зокрема обов'язку надання інформації суб'єкту даних, безпеки даних і принципу правомірної обробки персональних даних, є дуже важливим для формування довіри до технологій mHealth[950]. З цією метою було розроблено Кодекс поведінки в цій галузі на основі внесків широкого кола зацікавлених сторін, до якого входять експерти у сфері захисту персональних даних, само- та співрегулювання, інформаційно-комунікаційних технологій та охорони здоров'я[951]. На час підготовки цього посібника проєкт кодексу поведінки був поданий на розгляд Робочій групі «Стаття 29» до його офіційного затвердження.

949 Європейська Комісія (2014), *Зелена книга про мобільне здоров'я ("mHealth")*, COM(2014) 219 остаточний, Брюссель, від 10 квітня 2014 р..

950 Там само, п. 8.

951 *Проєкт Кодексу поведінки щодо приватності мобільних програм охорони здоров'я*, від 07 червня 2016 р.

9.4 Обробка персональних даних у дослідницьких та статистичних цілях

Ключові моменти

- Персональні дані, зібрані у статистичних цілях, цілях наукового чи історичного дослідження, не можуть використовуватися для інших цілей.
- Персональні дані, правомірно зібрані з будь-якою метою, можуть у подальшому використовуватися у статистичних цілях, цілях наукового чи історичного дослідження за умови наявності належних гарантій безпеки. Для забезпечення цих гарантій до передачі даних третім особам має бути передбачена їх анонімізація чи псевдонімізація.

Право ЄС дозволяє обробку даних у статистичних цілях та цілях наукового чи історичного дослідження за умови забезпечення відповідних гарантій для прав та свобод суб'єктів даних. Такі заходи можуть передбачати використання псевдонімів (псевдонімізації)[952]. Законодавство ЄС чи національне законодавство може передбачати певний відступ від прав суб'єктів даних, якщо ці права, ймовірно, можуть зробити неможливим чи серйозно зменшити досягнення легітимних цілей дослідження[953]. Відступи можуть бути введені щодо права суб'єктом даних на доступ, права на виправлення, права на обмеження обробки та права на заперечення.

Хоча персональні дані, які були правомірно зібрані контролером для будь-якої цілі, можуть бути повторно використані цим контролером для його власних статистичних цілей, цілей наукового чи історичного дослідження, залежно від контексту, перед передачею цих даних третій стороні у таких цілях вони повинні бути анонімізовані або псевдонімізовані, крім випадків, якщо суб'єкт персональних даних надав на це згоду чи це конкретно передбачено національним законодавством. Дані, що підлягають псевдонімізації, на відміну від анонімізованих, залишаються предметом захисту Загального регламенту захисту персональних даних[954].

952 Загальний регламент захисту персональних даних, стаття 89 (1).

953 Там само, стаття 89 (2).

954 Там само, п. 26 преамбули.

Таким чином, Регламент передбачає особливе ставлення до досліджень щодо загальних норм захисту персональних даних, щоб уникнути обмеження розвитку досліджень і дотримуватися мети Європейського дослідницького простору, яка закріплена у статті 179 ДФЄС. Він передбачає широке тлумачення обробки персональних даних у цілях наукових досліджень, в тому числі в аспекті технологічних розробок і демонстрацій, прикладних досліджень і досліджень за фінансової підтримки з боку приватного сектору. Він також визнає важливість компілювання даних з реєстрів для цілей досліджень і можливі труднощі з повноцінним визначенням подальшої мети обробки персональних даних у цілях наукового дослідження в той час, коли вони збираються[955]. У зв'язку з цим Регламент дозволяє обробку даних у цих цілях без згоди суб'єктів даних за умови наявності відповідних захисних гарантій.

Важливим прикладом використання даних у статистичних цілях є офіційна статистика, що отримується національними бюро статистики і бюро статистики ЄС на підставі національного законодавства і законодавства ЄС у сфері офіційної статистики. Відповідно до цього законодавства, громадяни і підприємства, як правило, зобов'язані розкривати персональні дані органам статистики. Посадовці, які працюють у бюро статистики, мають зобов'язання збереження професійної таємниці, яких повинні належним чином дотримуватися, оскільки вони є важливими для високого рівня довіри громадян, необхідної в разі потреби розкриття даних органам статистики[956].

Регламент (ЕС) № 223/2009 щодо європейської статистики містить основні норми захисту даних у контексті офіційної статистичної діяльності, а тому також може вважатися дотичним до положень щодо офіційної статистичної діяльності на національному рівні[957]. Регламент підтримує принцип, відповідно до якого офіційна статистична діяльність потребує достатньо чітких юридичних підстав[958].

955 Там само, п. 33, 157 та 159 преамбули.

956 Там само, стаття 90.

957 Регламент (ЕС) № 223/2009 Європейського Парламенту і Ради від 11 березня 2009 р. щодо європейської статистики та скасування Регламенту (ЕС, Євратом) № 1101/2008 Європейського Парламенту і Ради про передачу даних до Статистичної служби Європейського Співтовариства на які поширюється конфіденційність статистичної інформації, Регламенту Ради (ЕС) № 322/97 про статистику Співтовариства, та Рішення Ради 89/382/ЕЕС, Євратом про створення Комітету статистичних програм Європейського співтовариства, OJ 2009 L 87, із змінами, внесеними Регламентом (ЄС) 2015/759 Європейського Парламенту і Ради від 29 квітня 2015, яким було внесено зміни до Регламенту (ЕС) № 223/2009 про європейську статистику, OJ 2015 L 123.

958 Цей принцип має бути більш детально викладений у *Кодексі практики Євростату,* яким відповідно до статті 11 Регламенту про європейську статистику передбачено етичні правила здійснення офіційної статистичної діяльності, в тому числі дбайливе використання персональних даних.

Приклад: у справі «*Губер проти Федеративної Республіки Німеччини*»[959] австрійський бізнесмен, який переїхав до Німеччини, скаржився, що збирання та зберігання персональних даних іноземних громадян органами влади Німеччини в центральному реєстрі (AZR) також для статистичних цілей порушувало його права, передбачені Директивою про захист даних. З огляду на мету Директиви 95/46 забезпечити рівнозначний рівень захисту персональних даних у всіх державах-членах, СЄС постановив, що для гарантування високого рівня захисту в ЄС поняття необхідності у статті 7 (e) не може мати різного значення в різних державах-членах. Таким чином, це поняття має своє незалежне значення у праві ЄС і має тлумачитися у спосіб, що повністю відображає мету Директиви 95/46. Зазначивши, що для статистичних цілей вимагається лише знеособлена інформація, СЄС постановив, що німецький реєстр несумісний з вимогою необхідності відповідно до статті 7 (e).

У контексті **РЄ** подальша обробка даних може здійснюватись в інтересах суспільства для наукових, історичних чи статистичних цілей та повинна підлягати відповідним гарантіям[960]. Права суб'єктів даних можуть також бути обмежені у разі обробки даних у статистичних цілях за умови відсутності ризику порушення їхніх прав та свобод[961].

Рекомендація щодо статистичних даних, прийнята в 1997 році, охоплює статистичну діяльність у державному та приватному секторах[962].

Дані, зібрані контролером у статистичних цілях, не можуть використовуватися в будь-яких інших цілях. Дані, які було зібрано у нестатистичних цілях, повинні бути доступними для подальшого використання в статистичних цілях. Рекомендація щодо статистичних даних також дозволяє повідомлення даних третім особам, якщо це здійснюється лише у статистичних цілях. В таких випадках сторони повинні домовитися і зафіксувати межі подальшого правомірного використання даних для статистики. Оскільки це не може замінити згоду суб'єкта персональних даних, за потреби в національному законодавстві повинні бути передбачені належні гарантії для мінімізації ризиків

959 Суд ЄС, C-524/06, «Гайнц Губер проти Федеративної Республіки Німеччини» (*Heinz Huber v. Bundesrepublik Deutschland* [GC]), від 16 грудня 2008; особливо див. п. 68.

960 Оновлена Конвенція 108, стаття 5 (4) (b).

961 Там само, стаття 11 (2).

962 Рада Європи, Комітет міністрів (1997), Рекомендація Rec(97)18 державам-учасницям щодо захисту персональних даних, які збираються і обробляються для статистичних цілей, від 30 вересня 1997 р.

зловживання особистими даними, наприклад, зобов'язання анонімізувати або псевдонімізувати такі дані перед розкриттям.

На осіб, які професійно займаються статистичними дослідженнями, як це зазвичай відбувається в сфері офіційної статистики, повинні бути покладені спеціальні зобов'язання збереження професійної таємниці відповідно до національного законодавства. Ця вимога має поширюватися і на осіб, які проводять опитування, а також на інших збирачів, якщо вони залучені до отримання даних від 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 це було правомірним, або мати можливість висунути заперечення. Якщо персональні дані збираються у статистичних цілях шляхом опитування осіб, ці особи повинні бути чітко поінформовані про те, чи є надання даних обов'язковим за національним законодавством.

Якщо статистичне дослідження не може бути проведено з використанням анонімних даних і потрібні персональні дані, тоді зібрані з цією метою дані повинні бути якомога швидше знеособлені. Результати статистичного дослідження не повинні принаймні дозволяти ідентифікацію будь-якого з суб'єктів персональних даних, хіба що коли це не становитиме жодного ризику.

Після завершення статистичного аналізу використані персональні дані повинні бути або видалені, або знеособлені. У таких випадках Рекомендація щодо статистичних даних пропонує зберігати ідентифікаційні дані окремо від інших персональних даних. Це означає, наприклад, що ключ шифрування чи список з ідентифікаційними синонімами повинен зберігатися окремо від інших даних.

9.5 Фінансові дані

Ключові моменти

- Хоча фінансові дані не вважаються чутливими даними в розумінні Оновленої Конвенції 108 чи Загального регламенту захисту персональних даних, їх обробка вимагає особливих гарантій для забезпечення точності і безпеки даних.
- Електронні платіжні системи особливо потребують «вбудованого» захисту даних, тобто забезпечувати приватність чи захист даних за призначенням та за замовчуванням.
- Особливі проблеми захисту можуть виникнути в цій сфері через необхідність створення відповідних механізмів автентифікації.

Приклад: у справі «*Мішо проти Франції*»[963] заявник, французький адвокат, оскаржував своє зобов'язання за французьким законодавством повідомляти про підозри стосовно можливої діяльності з відмивання грошей його клієнтами. ЄСПЛ зауважив, що вимога до адвокатів повідомляти адміністративним органам інформацію стосовно іншої особи, яка стала їм відома в ході професійного спілкування з цією особою, становила втручання у право адвокатів на захист своєї кореспонденції і приватного життя, гарантованого статтею 8 ЄКПЛ, оскільки це поняття охоплює діяльність професійного і ділового характеру. Проте втручання здійснювалося відповідно до закону і переслідувало легітимну мету, а саме запобігання заворушенням та злочинності. Оскільки на адвокатів покладалося зобов'язання повідомляти про свої підозри лише за дуже обмежених обставин, ЄСПЛ постановив, що це зобов'язання було пропорційним. Він дійшов висновку, що порушення статті 8 не було.

Приклад: у справі «*М. Н. та інші проти Сан-Марино*»[964] заявник, італійський громадянин, уклав договір доручення з компанією, щодо якої здійснювалося слідство. Це означає, що в компанії проводились обшуки та вилучались копії (електронної) документації. Заявник подав скаргу до суду Сан-Марино, стверджуючи про відсутність зв'язку між ним та стверджуваними злочинами. Однак суд визнав його скаргу неприйнятною, оскільки він не був «зацікавленою стороною». ЄСПЛ постановив, що заявник був у вкрай невигідному становищі щодо судового захисту порівняно із «зацікавленою стороною», та його дані все ж підлягали обшуку та вилученню. Таким чином, Суд постановив, що мало місце порушення статті 8.

Приклад: у справі «*G. S. B. проти Швейцарії*»[965] реквізити банківського рахунку заявника були надіслані до податкових органів США на підставі угоди про адміністративну взаємодію між Швейцарією та США. ЄСПЛ постановив, що передача не є порушенням статті 8 ЄКПЛ, оскільки втручання в право заявника на приватне життя було передбачене законом, переслідувало легітимну мету та було пропорційним стосовно відповідного суспільного інтересу.

963 Рішення ЄСПЛ у справі «Мішо проти Франції» (*Michaud v. France*), № 12323/11, від 06 грудня 2012 р. Див. також рішення ЄСПЛ у справі «Нємєц проти Німеччини» (*Niemietz v. Germany*), № 13710/88, від 16 грудня 1992 р., п. 29, та рішення ЄСПЛ у справі, «Гелфорд проти Сполученого Королівства» (*Halford v. the United Kingdom*), № 20605/92, від 25 червня 1997 р., п. 42.

964 Рішення ЄСПЛ у справі «М. Н. та інші проти Сан-Марино» (*M. N. and Others v. San Marino*), № 28005/12, від 07 липня 2015 р.

965 Рішення ЄСПЛ у справі «G.S.B. проти Швейцарії» (*G.S.B. v. Switzerland*), № 28601/11 від 22 грудня 2015 р.

Застосування загальної правової системи у сфері захисту персональних даних (як визначено в Конвенції 108) у контексті платежів було розширено **РЄ** в Рекомендації Rec (90) 19 від 1990 року[966]. Ця Рекомендація роз'яснює питання щодо обсягу законного збирання і використання даних у контексті здійснення платежів, особливо за допомогою платіжних карт. Крім того, вона надає національним законодавцям докладні рекомендації щодо меж повідомлення платіжних даних третім особам, строків збереження даних, прозорості, безпеки даних і транскордонної передачі даних, а також щодо нагляду і засобів юридичного захисту. РЄ також розробила Висновок щодо передачі податкових даних[967], що містить рекомендації та питання, які необхідно враховувати при роботі з передачею податкових даних.

ЄСПЛ дозволяє передачу фінансових даних, зокрема реквізити банківського рахунку фізичної особи, відповідно до статті 8 ЄКПЛ, якщо це передбачено законом, переслідує легітимну мету та є пропорційним стосовно відповідного суспільного інтересу[968].

Щодо **законодавства ЄС**, електронні платіжні системи, які передбачають обробку персональних даних, мають відповідати Загальному регламенту захисту персональних даних. У зв'язку з цим такі системи мають забезпечити захист персональних даних за призначенням і за замовчуванням. Захист персональних даних за призначенням зобов'язує контролера вживати належних технічних та організаційних заходів для реалізації принципів захисту персональних даних. Захист персональних даних за замовчуванням означає, що контролер повинен забезпечити обробку за замовчуванням лише тих персональних даних, які необхідні для конкретної мети (див. *розділ 4.4*). Стосовно фінансових даних, Суд ЄС вважає, що передані податкові дані можуть становити персональні дані[969]. Робоча група з питань захисту персональних даних «Стаття 29» видала відповідні настанови державам-членам, зокрема критерії для забезпечення дотримання правил захисту персональних даних при автоматичному обміні персональними даними автоматизованими засобами у податкових

966 Рада Європи, Комітет міністрів (1990), Рекомендація No. R(90)19 щодо захисту персональних даних, що використовуються для розрахункових та інших суміжних операцій, від 13 вересня 1990 р.

967 Рада Європи, Консультативний Комітет Конвенції 108 (2014), Висновок щодо значення для захисту персональних даних механізмів автоматичного міждержавного обміну даними в адміністративних та податкових цілях, від 04 червня 2014 р.

968 Рішення ЄСПЛ у справі «G.S.B. проти Швейцарії» (*G.S.B. v. Switzerland*), № 28601/11, від 22 грудня 2015 р.

969 Рішення Суду ЄС, C-201/14, «Смаранда Бара та інші проти Національного фонду медичного страхування та інших» (*Smaranda Bara and Others v. Casa Naţională de Asigurări de Sănătate and Others*), від 01 жовтня 2015 р., п. 29.

цілях[970]. Крім того, прийнято низку нормативних актів для регулювання фінансових ринків і діяльності кредитних установ та інвестиційних фірм[971]. Інші правові документи допомагають у боротьбі з інсайдерською торгівлею та маніпуляціями на ринку[972]. Основними напрямками впливу на захист персональних даних є:

- збереження записів про фінансові транзакції;
- передача персональних даних до третіх країн;
- запис телефонних розмов чи електронних повідомлень, в тому числі повноваження компетентних органів вимагати записи телефонних розмов і дані трафіку;
- розкриття персональної інформації, в тому числі публікація санкцій;
- наглядові та слідчі повноваження компетентних органів, у тому числі перевірки на місцях і вхід до приватних приміщень для конфіскації документів;
- механізми повідомлень про порушення, тобто система захисту викривачів;
- співробітництво між компетентними органами держав-членів та Європейським органом з цінних паперів та ринків (ЄОЦПР; ESMA).

970 Робоча група із захисту персональних даних «Стаття 29» (2015), Заява щодо автоматичного міждержавного обміну персональними даними в податкових цілях, 14/EN РГ 230.

971 Директива 2014/65/EU Європейського Парламенту і Ради від 15 травня 2014 про ринки фінансових інструментів та внесення змін до Директиви 2002/92/ЕС та Директиви 2011/61/EU, OJ 2014 L 173; Регламент (ЄС) № 600/2014 Європейського Парламенту і Ради від 15 травня 2014 р. про ринки фінансових інструментів та внесення змін до Регламенту (ЄС) № 648/2012, OJ 2014 L 173; Директива 2013/36/EU Європейського Парламенту і Ради від 26 червня 2013 р. про доступ до діяльності кредитних установ та пруденційний нагляд за кредитними установами та інвестиційними фірмами, внесення змін до Директиви 2002/87/ЕС та скасування Директиви 2006/48/ЕС та 2006/49/ЕС, OJ 2013 L 176.

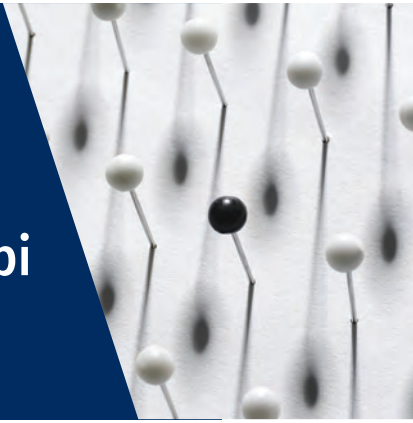
972 Регламент (ЄС) № 596/2014 Європейського Парламенту і Ради від 16 квітня 2014 р. про зловживання на ринку (Регламент щодо зловживання на ринку) та скасування Директиви 2003/6/ЕС Європейського Парламенту і Ради та Директив Комісії 2003/124/ЕС, 2003/125/ЕС та 2004/72/ЕС, OJ 2014 L 173.

У цих сферах особливу увагу приділено й іншим питанням, у тому числі питанню збирання даних про фінансовий стан суб'єктів персональних даних[973] або транскордонні платежі шляхом здійснення банківських переказів, які неминуче призводять до потоку персональних даних[974].

973 Регламент (ЕС) № 1060/2009 Європейського Парламенту і Ради від 16 вересня 2009 р. щодо кредитних рейтингових агенцій, OJ 2009 L 302, із нещодавніми змінами, внесеними Директивою 2014/51/EU Європейського Парламенту і Ради від 16 квітня 2014 р. про внесення змін до Директиви 2003/71/ЕС та 2009/138/ЕС та Регламентів (ЕС) № 1060/2009, (ЄС) № 1094/2010 та (ЄС) № 1095/2010 стосовно повноважень Європейського наглядового органу (Європейська організація зі страхування та пенсійного забезпечення) та Європейського наглядового органу (Європейська організація з цінних паперів та ринків), OJ 2014 L 153; Регламент (ЄС) № 462/2013 Європейського Парламенту і Ради від 21 травня 2013 р. про внесення змін до Регламенту (ЕС) № 1060/2009 щодо кредитних рейтингових агенцій, OJ 2013 L 146.

974 Директива 2007/64/ЕС Європейського Парламенту і Ради від 13 листопада 2007р. про платіжні послуги на внутрішньому ринку та про внесення змін до Директив 97/7/ЕС, 2002/65/ЕС, 2005/60/ЕС та 2006/48/ЕС та скасування Директиви 97/5/ЕС, OJ 2007 L 319, до яких було внесено зміни Директивою 2009/111/ЕС Європейського Парламенту і Ради від 16 вересня 2009 про внесення змін до Директив 2006/48/ЕС, 2006/49/ЕС та 2007/64/ЕС стосовно афілійованих банків центральних установ, окремих статей власного фонду, великих ризиків, механізмів захисту та антикризового управління, OJ 2009 L 302.

10
Сучасні виклики у сфері захисту персональних даних



Цифрова ера, або ера інформаційних технологій, характеризується широким використанням комп'ютерів, інтернету та цифрових технологій. Це передбачає збирання та обробку величезної кількості даних, в тому числі персональних даних. Збирання та обробка персональних даних у глобалізованій економіці означає зростання транскордонних потоків даних. Така обробка може принести значну та очевидну користь у повсякденному житті: пошукові системи полегшують доступ до великого обсягу інформації та знань, соціальні мережеві сервіси надають людям можливість спілкуватись по всьому світу, висловлювати думки та мобілізувати підтримку в соціальних, екологічних та політичних цілях, а компанії та споживачі отримують переваги від ефективних і дієвих ринкових технологій, що сприяють зростанню економіки. Технології та обробка персональних даних також є незамінними інструментами для державних органів у боротьбі зі злочинністю та тероризмом. Аналогічно, великі дані /«big data» (збирання, зберігання та аналіз великої кількості інформації для визначення закономірностей та прогнозування поведінки) «можуть бути джерелом значної цінності для суспільства, підвищуючи продуктивність праці, ефективність роботи публічного сектору та громадську участь»[975].

Незважаючи на вказані численні переваги, цифрова ера також створює виклики для приватності та захисту персональних даних, оскільки велика кількість персональної інформації збирається та обробляється все більш складними та непрозорими способами. Технологічний прогрес призвів до

975 Рада Європи, Консультативний Комітет Конвенції 108, *Рекомендації щодо захисту фізичних осіб стосовно обробки персональних даних у світі великих даних*, T-PD(2017)01, Страсбург, від 23 січня 2017 р.

формування масивних наборів даних, які можна легко звірити та в подальшому проаналізувати для виявлення закономірностей або для прийняття рішень на основі алгоритмів, які можуть надати безпрецедентне уявлення про поведінку та приватне життя людини[976].

Нові технології потужні та можуть бути небезпечними на практиці, якщо потраплять не туди, куди мають. Державні органи, що здійснюють масове спостереження та можуть використовувати такі технології, є прикладом того, який значний вплив технології мають на права фізичних осіб. У 2013 році викриття Едварда Сноудена щодо ведення розвідувальними агентствами в деяких країнах широкомасштабних програм інтернет- та телефонних спостережень викликали велике занепокоєння стосовно небезпеки, яку несе діяльність зі здійснення спостереження для приватного життя, демократичного управління та свободи вираження поглядів. Масове спостереження та технології, які дозволяють глобалізовано зберігати і обробляти особисту інформацію та надають доступ до даних, можуть зазіхати на саму сутність права на приватність[977]. Крім того, вони можуть мати негативний вплив на політичну культуру та стримувати розвиток демократії, творчості та інновацій[978]. Сам лише страх, що держава може постійно відстежувати та аналізувати поведінку і дії громадян, може позбавити цих громадян мужності висловлювати свої погляди з певних питань та призвести до надмірної обачливості й обережності[979]. Ці виклики спонукали низку державних органів, центрів досліджень та організацій громадянського суспільства проаналізувати потенційний вплив нових технологій на суспільство. У 2015 році Європейський інспектор із захисту персональних даних розпочав кілька ініціатив, спрямованих на оцінку впливу великих даних та «інтернету речей» на етику. Зокрема, було створено Консультативну групу з питань етики, яка має стимулювати «відкриту та предметну дискусію щодо цифрової етики, що надає змогу ЄС усвідомити переваги технологій для суспільства та економіки, і в той же час посилити права та

976 Європейський Парламент (2017), Резолюція про значення великих даних для основних прав: приватність, захист персональних даних, відсутність дискримінації, безпека та правозастосування закону (P8_TA-PROV(2017)0076, Страсбург, від 14 березня 2017 р.

977 Див. ООН, Генеральна Асамблея, *Доповідь спеціального доповідача про заохочення та захист прав людини та основних свобод при протидії тероризму*, Бен Емерсон, A/69/397, від 23 версня 2014 р., п. 59. Див. також ЄСПЛ, *Інформаційний бюлетень про масове спостереження*, липень 2017 р.

978 ЄІЗПД (2015), *Прийняття викликів великих даних*, Висновок 7/2015, Брюссель, від 19 листопада 2015 р.

979 Див. рішення Суду ЄС, об'єднані справи C-293/12 ти C-594/12, «"Digital Rights Ireland Ltd." проти Міністра зв'язку, морських та природних ресурсів та інших та Земельний уряд Каринтії та інші» (*Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*) [ВП], від 08 квітня 2014 р., п. 37.

свободи фізичних осіб, особливо права на приватність та захист персональних даних»[980].

Обробка персональних даних також є потужним інструментом у руках корпорацій. Сьогодні вона може розкрити детальну інформацію про стан здоров'я та фінансовий стан особи, інформацію, яка потім використовується корпораціями для прийняття важливих рішень щодо фізичних осіб, таких як розмір премій медичного страхування для працівників чи їх кредитоспроможність. Методи обробки даних також можуть позначитися на демократичних процесах, якщо вони використовуються політиками чи корпораціями, щоб вплинути на вибори, наприклад, через «мікроспрямовану» комунікацію з виборцями. Інакше кажучи, хоча приватність першочергово сприймалась як право на захист фізичних осіб від необґрунтованого втручання державних органів, у сучасну епоху їй можуть також загрожувати можливості приватних суб'єктів. Це викликає питання щодо використання технологій та прогнозного аналізу в процесі прийняття рішень, які мають вплив на повсякденне життя фізичних осіб, та посилює необхідність забезпечення, щоб будь-яка обробка персональних даних здійснювалася з дотриманням основоположних прав.

Захист персональних даних по суті пов'язаний з технологічними, соціальними та політичними змінами. З цієї причини неможливо було б розробити всебічний перелік майбутніх викликів. У цьому розділі розглядаються окремі сфери стосовно великих даних, інтернет-соціальних мереж та єдиного цифрового ринку ЄС. Оцінка цих сфер з точки зору захисту персональних даних не є вичерпною, натомість висвітлює безліч можливих варіантів взаємодії між новою чи зміненою людською діяльністю та захистом персональних даних.

980 ЄІЗПД, Рішення від 03 грудня 2015 р., яким створено зовнішню консультативну групу щодо етичних аспектів захисту персональних даних (Консультативна група з питань етики/'the Ethics Advisory Group'), від 03 грудня 2015 р., п. 5 загальної частини.

10.1 Великі дані, алгоритми та штучний інтелект

Ключові моменти

- Революційні інновації в інформаційно-комунікаційних технологіях (ІКТ) формують новий спосіб життя, у якому соціальні відносини, бізнес, приватні та публічні послуги взаємопов'язані цифровим шляхом, створюючи таким чином великий обсяг даних, значна частина яких є персональними даними.
- Держави, підприємства та громадяни все більше працюють в економіці, що спирається на дані, в якій самі ці дані стали цінними активами.
- Поняття «великі дані» (big data) стосується як самих даних, так і їх аналітики.
- Нормативно-правові документи ЄС та РЄ поширюється на персональні дані, які обробляються за допомогою аналітики великих даних.
- Відступи від прав на персональні дані та правил їх захисту обмежені і зводяться до певних прав та окремих ситуацій, у яких дотримання права виявиться неможливим або вимагатиме непропорційних зусиль контролерів даних.
- Повністю автоматизоване прийняття рішень загалом заборонене, крім окремих випадків.
- Поінформованість осіб та здійснення ними контролю є основоположним для забезпечення дотримання прав.

У нашому все більш оцифрованому світі кожна діяльність залишає цифрові сліди, які можна збирати, обробляти та оцінювати чи аналізувати. З появою нової інформації та комунікаційних технологій все більше і більше даних збирається та записується[981]. До недавнього часу жодна технологія не могла проаналізувати чи здійснити оцінку маси даних чи зробити з них корисні висновки. Дані були просто занадто численними для оцінки, занадто складними, погано структурованими та швидкозмінними для визначення тенденцій та звичок.

981 Європейська Комісія, Комюніке Комісії до Європейського Парламенту, Ради, Європейського соціально-економічного комітету та Регіонального комітету щодо процвітаючої економіки даних COM(2014) 442 остаточне, Брюссель, від 02 липня 2014 р.

10.1.1 Визначення великих даних, алгоритмів та штучного інтелекту

Великі дані (big data)

Термін «великі дані» (big data) це сучасний вислів, який може стосуватися декількох концепцій залежно від контексту. Він, як правило, охоплює «дедалі більшу технологічну можливість акумулювати процеси та отримувати нові та прогнозні знання з різноманітних даних великого обсягу і швидкості»[982]. У зв'язку з цим поняття великих даних (big data) включає як самі дані, так і їх аналітику.

Джерела даних є різноманітних типів, до яких в тому числі належать люди та їхні персональні дані, машини чи сенсори, кліматична інформація, супутникові знімки, цифрові зображення та відео чи GPS-сигнали. Однак великою частиною даних та інформації є персональні дані – будь-які дані, починаючи з прізвища, фотознімків, електронної адреси, банківських реквізитів, даних відстеження GPS, постів на вебсайтах соціальних мереж, медичної інформації чи IP-адреси комп'ютера[983].

Під великими даними також мається на увазі **обробка**, аналіз та оцінка великої кількості даних і наявної інформації, тобто отримання корисної інформації в цілях дослідження великих даних. Це означає, що зібрані дані та інформація можуть бути використані для інших цілей, ніж було визначено першочергово, наприклад для виявлення статистичних тенденцій чи для більш спеціальних послуг, таких як реклама.

Фактично, за наявності технологій для збору, обробки та оцінки великих даних, будь-яку інформацію можна комбінувати та переоцінювати: фінансові операції, кредитоспроможність, медичне лікування, приватне споживання, професійну діяльність, відстеження та проходження маршрутів, використання

982 Рада Європи, Консультативний Комітет Конвенції 108, Рекомендації щодо захисту фізичних осіб стосовно обробки персональних даних у світі Великих даних, від 23 січня 2017 р., на сторінці 2; Європейська Комісія, Комюніке Комісії до Європейського Парламенту, Ради, Європейського соціально-економічного комітету та Регіонального комітету щодо процвітаючої економіки даних COM(2014) 442 остаточне, Брюссель, від 02 липня 2014 р., на сторінці 4; Міжнародний союз електрозв'язку (2015), Рекомендація Y.3600. Великі дані – Вимоги та можливості хмарних обчислень.

983 Інформаційний бюлетень Комісії ЄС з питань реформи захисту персональних даних і великих даних; Рада Європи, Консультативний Комітет Конвенції 108, Рекомендації щодо захисту фізичних осіб стосовно обробки персональних даних у світі Великих даних, від 23 січня 2017 р., на сторінці 2.

інтернету, електронних карток та смартфонів, відеомоніторинг чи моніторинг комунікацій. Аналіз великих даних призводить до нового кількісного виміру даних, який можна оцінити та використати в реальному часі, наприклад, для надання споживачам послуг на замовлення.

Алгоритми та штучний інтелект

Штучний інтелект (ШІ) означає інтелект машин, які діють як «розумні агенти». Певні пристрої, як розумні агенти, за підтримки програмного забезпечення можуть сприймати своє навколишнє середовище та здійснювати дії за алгоритмами. Термін ШІ застосовується, коли машина імітує когнітивні функції (такі, як навчання та вирішення проблем), які зазвичай асоціюються з людьми[984]. Для відтворення процесу прийняття рішень у сучасних технологіях і програмному забезпеченні застосовуються алгоритми, які використовуються пристроями для прийняття «автоматизованих рішень». Алгоритм найкраще описується як покрокова процедура обчислення, обробки даних, оцінки і автоматизованого обґрунтування та прийняття рішень.

Аналогічно до аналітики великих даних, ШІ та здійснюване ним автоматизоване прийняття рішень вимагає зведення та обробки даних великого обсягу. Такі дані можуть надходити від самого пристрою (нагрівання гальм, паливо тощо) чи з навколишнього середовища. Наприклад, профайлінг – це процес, який може здійснюватися на основі автоматизованого прийняття рішень відповідно до заздалегідь встановлених шаблонів і факторів.

Приклад: Профайлінг та цільова реклама

Профайлінг на основі великих даних передбачає пошук шаблонів, які відображають «характеристики типу особистості», наприклад, коли компанії онлайн-продажів пропонують продукти із написом «Вам також можуть сподобатись» на основі інформації, зібраної щодо раніше сформованого кошика покупця продуктів. Що більше даних, то чіткіша мозаїка. Наприклад, смартфон є потужною анкетою, яку фізичні особи заповнюють при кожному використанні, свідомо та несвідомо.

984 Стюарт Рассел та Пітер Норвінг, *Штучний інтелект: Сучасний підхід (2-ге вид.)*, 2003, Аппер Садл Рівер, Нью Джерсі: Прентіс Хол, сторінка 27, 32–58, 968–972; Стюарт Рассел та Пітер Норвінг, *Штучний інтелект: Сучасний підхід (3-тє вид.)*, 2009, Аппер Садл Рівер, Нью Джерсі: Прентіс Хол, с. 2.

Сучасна психографія (наука вивчення особистості) використовує метод «OCEAN», на основі якого визначаються відповідні типи характеру. До рис характеру «Велика п'ятірка» відносяться відкритість (openness; наскільки людина відкрита до нового), сумлінність (conscientiousness; наскільки особа прагне довершеності), екстраверсія (extraversion; наскільки товариська людина), доброзичливість (agreeableness; наскільки людина доброзичлива) та невротизм (neuroticism; наскільки людина вразлива). Ця інформація описує відповідну людину, її потреби та побоювання, як вона буде поводитись тощо. Потім додається інша інформацією про особу, отримана з будь-яких доступних джерел: від брокерів даних, соціальних мереж (в тому числі відміток «подобається»/«likes» під постами та запощених фото) до музики, яка прослуховується онлайн, чи даних GPS та відстеження пересування.

Маса профілів, що створюються за допомогою технік аналізу великих даних, пізніше порівнюються для виявлення подібних моделей та складання груп особистостей. Внаслідок цього інформація про поведінку та ставлення певних особистостей перевертається: за допомогою доступу до великих даних та їх використання тест особистості стає зворотним, і тепер інформація про поведінку та погляди застосовується для опису особистості людини. Маючи об'єднану інформацію про вподобання («likes») в соціальних мережах, дані відстеження пересування, музику, яка прослуховується, чи фільми, які переглядаються, може скластися чітка картинка про особистість людини, що дозволяє підприємствам надсилати цільову рекламу та/чи інформацію відповідно до «особистості» такої людини. Крім того, така інформація може оброблятись у реальному часі[985].

10.1.2 Оцінка переваг та ризиків великих даних

Сучасні методи обробки можуть справлятися з великими масивами даних, швидко імпортувати нові дані, забезпечувати обробку інформації в реальному часі з коротким строком надання відповіді (навіть у випадку отримання складних запитів), надавати можливість опрацювання багаторазових та одночасних запитів, а також можуть аналізувати різні типи інформації (фотознімки, текст чи цифри). Ці технологічні інновації дозволяють структурувати,

985 Методи обробки та нове програмне забезпечення здійснюють оцінку інформації щодо вподобань людини, на що вона дивиться під час онлайн-покупок або додає до кошика в реальному часі та можуть пропонувати «товари», які можуть зацікавити, з огляду на отриману інформацію.

обробляти та оцінювати велику кількість даних та інформації в реальному часі[986]. Багаторазово збільшуючи кількість доступних та таких, що підлягають аналізу, даних, тепер можна досягти результатів, які були б неможливі при меншому масштабі. Великі дані допомогли заснувати нову сферу бізнесу, у якій можуть з'являтися нові послуги як для підприємств, так і споживачів. Вартість персональних даних громадян ЄС може потенційно зрости до майже 1 трильйона євро на рік до 2020 року[987]. Таким чином, великі дані можуть надати нові **можливості** в результаті оцінки великої кількості даних для нових соціальних, економічних чи наукових уявлень, які можуть принести користь фізичним особам, а також бізнесу та державним органам[988].

Аналітика великих даних може виявити закономірності між різними джерелами та наборами даних, що приводить до корисних відкриттів у таких сферах, як наука та медицина. Так відбувається, наприклад, у сфері охорони здоров'я, харчової безпеки, інтелектуальних транспортних систем, енергоефективності чи містобудування. Такий аналіз інформації в реальному часі може бути використаний для вдосконалення запроваджуваних систем. Можна отримати нові знання в дослідницькій роботі шляхом поєднання великої кількості даних і статистичних оцінок, особливо з дисциплін, у яких дотепер оцінка великої частини даних здійснювалася лише вручну. Можуть бути розроблені нові методи лікування, спеціально пристосовані до потреб окремих пацієнтів, на основі порівняння з великою кількістю доступної інформації. Компанії сподіваються, що аналіз великих даних дозволить їм отримати конкурентну перевагу, заощадити кошти та створити нові сфери бізнесу шляхом

986 Розробка програмного забезпечення для обробки Великих даних ще перебуває на ранньому етапі. Однак нещодавно було розроблено аналітичні програми, особливо для аналізу великої кількості даних та інформації в реальному часі стосовно активностей людей. Можливість аналізу та обробки великих даних (big data) структурованим шляхом надала нові засоби профайлінгу та цільової реклами. Європейська Комісія, Комюніке Комісії до Європейського Парламенту, Ради, Європейського соціально-економічного комітету та Регіонального комітету щодо процвітаючої економіки даних COM(2014) 442 остаточне, Брюссель, від 02 липня 2014 р.; Інформаційний бюлетень Комісії ЄС з питань реформи захисту персональних даних та великих даних; Рада Європи, Консультативний Комітет Конвенції 108, Рекомендації щодо захисту фізичних осіб стосовно обробки персональних даних у світі великих даних, від 23 січня 2017 р., на с. 2.

987 Інформаційний бюлетень Комісії ЄС щодо реформи захисту персональних даних і великих даних.

988 Міжнародна конференція Уповноважених із захисту персональних даних та приватності (2014), Резолюція щодо великих даних, та Європейська Комісія, Комюніке Комісії до Європейського Парламенту, Ради, Європейського соціально-економічного комітету та Регіонального комітету щодо процвітаючої економіки даних COM(2014) 442 остаточне, Брюссель, від 02 липня 2014 р., на сторінці 2; Інформаційний бюлетень Комісії ЄС щодо реформи захисту персональних даних та великих даних, та Рада Європи, Рекомендації щодо захисту фізичних осіб стосовно обробки персональних даних у світі великих даних, від 23 січня 2017 р., на сторінці 1.

прямого, індивідуалізованого обслуговування споживачів. Державні органи сподіваються досягти вдосконалення в кримінальному правосудді. Стратегія Комісії щодо Єдиного цифрового ринку Європи визнає потенціал заснованих на даних технологій, послуг і великих даних як каталізаторів економічного зростання, інновацій та цифровізації в ЄС[989].

Втім великі дані також несуть **ризики**, як правило, пов'язані з трьома характеристиками (три V): обсяг (volume), швидкість (velocity) та різноманітність (variety) оброблюваних даних. Обсяг означає суму оброблюваних даних, різноманітність – кількість та різновиди типів даних, а швидкість стосується швидкості темпів обробки даних. Конкретні питання щодо захисту персональних даних особливо актуальні, коли аналітика великих даних використовується стосовно великих наборів даних для виокремлення нових і прогнозних знань у цілях прийняття рішень стосовно фізичних осіб та/або груп[990]. Ризики великих даних для захисту персональних даних і приватності були висвітлені у висновках ЄІЗПД та Робочої групи «Стаття 29», резолюціях Європейського Парламенту та програмних документах Ради Європи[991].

Ризики можуть включати неправильне поводження з великими даними осіб, які мають доступ до великої кількості інформації, шляхом маніпуляцій, дискримінації або пригноблення фізичних осіб чи окремих груп суспільства[992]. Коли збираються, обробляються та оцінюються масиви персональних даних та інформації щодо поведінки фізичних осіб, їх використання може призвести до суттєвих порушень засадничих прав і свобод, що виходять за межі права на приватність. Неможливо виміряти точний ступінь впливу на приватність та персональні дані. Європейський Парламент виявив відсутність методики для проведення заснованої на фактичних даних оцінки загального впливу великих даних, але є підстави вважати, що аналітика великих

989 Резолюція Європейського Парламенту від 14 березня 2017 р. про значення великих даних для основних прав: приватності, захисту персональних даних, недискримінації, безпеки та правозастосування (2016/2225 (INI)).

990 Рада Європи, Консультативний Комітет Конвенції 108, Рекомендації щодо захисту фізичних осіб стосовно обробки персональних даних у світі Великих даних, від 23 січня 2017 р., на сторінці 2.

991 Див., наприклад, ЄІЗПД (2015), *Прийняття викликів великих даних*, Висновок 7/2015, від 19 листопада 2015 р.; ЄІЗПД (2016), *Когерентне забезпечення основних прав у еру Великих даних*, Висновок 8/2016, від 23 вересня 2016 р.; Європейський Парламент (2016), Резолюція про значення Великих даних для основних прав: приватності, захисту персональних даних, недискримінація, безпеки та правозастосування, P8_TA(2017)0076, Страсбург, від 14 березня 2017 р.; Рада Європи, Консультативний Комітет Конвенції 108, Рекомендації щодо захисту фізичних осіб стосовно обробки персональних даних у світі великих даних, T-PD(2017)01, Страсбург, від 23 січня 2017 р.

992 Міжнародна конференція Уповноважених із захисту даних та приватності (2014), Резолюція щодо Великих даних.

даних може мати значні горизонтальні наслідки як для публічного, так і приватного сектору[993].

Загальний регламент захисту персональних даних містить положення щодо права не бути суб'єктом автоматизованих рішень, включаючи профайлінг[994]. Питання приватності виникає, коли реалізація права на заперечення вимагає людського втручання, дозволяючи суб'єктам даних висловлювати свою думку та оскаржувати рішення[995]. Це може спричиняти проблеми в забезпеченні належного рівня захисту персональних даних якщо, наприклад, людське втручання неможливе, чи алгоритми є занадто складними, а кількість залучених даних занадто велика, щоб надати фізичним особам обґрунтування певних рішень та/або попередню інформацію з метою отримання їхньої згоди. Приклад використання ШІ та автоматизованого прийняття рішень можна знайти в останніх розробках іпотечних додатків або під час процесу підбору персоналу. Заявки не задовольняються або відхиляються на підставі того, що заявники не відповідають заздалегідь визначеним параметрам або факторам.

10.1.3 Питання, пов'язані із захистом персональних даних

Головними питаннями щодо захисту персональних даних, з одного боку, є обсяг та різноманітність оброблюваних персональних даних, з іншого – обробка та її результати. Впровадження складних алгоритмів і програмного забезпечення для перетворення масових даних на ресурс для прийняття рішень впливає на людей та групи, особливо у випадках профайлінгу чи позначення ярликами, і, зрештою, викликає багато питань щодо захисту персональних даних[996].

Ідентифікація контролерів і операторів та їхня відповідальність

Великі дані та ШІ викликають декілька питань щодо ідентифікації контролерів і операторів та їхньої відповідальності: коли така велика кількість даних

993 Резолюція Європейського Парламенту від 14 березня 2017 р. про значення Великих даних для основних прав: приватності, захисту персональних даних, недискримінації, безпеки та правозастосування (2016/2225(INI)).

994 Загальний регламент захисту персональних даних, стаття 22.

995 Там само, стаття 22 (3).

996 Рада Європи, Консультативний Комітет Конвенції 108, Рекомендації щодо захисту фізичних осіб стосовно обробки персональних даних у світі великих даних, від 23 січня 2017 р., на сторінці 2.

збирається і обробляється, хто є їхнім власником? Хто є контролером, коли дані обробляються інтелектуальними машинами та програмним забезпеченням? Які конкретно обов'язки кожного суб'єкта в обробці даних? Та для яких цілей можуть використовуватися великі дані?

Питання відповідальності в контексті ШІ стане ще більш складним, коли ШІ прийматиме рішення на основі обробки даних, яку він розробив самостійно. Загальний регламент захисту персональних даних забезпечує правову базу для відповідальності контролерів чи операторів даних. Неправомірна обробка персональних даних передбачає відповідальність контролера та оператора даних[997]. Штучний інтелект та автоматизоване прийняття рішень викликають питання про те, хто несе відповідальність за порушення, які зачіпають приватність суб'єктів даних, коли складність і кількість оброблюваних даних не можуть бути визначені з певністю. Якщо ШІ та алгоритми розглядаються як продукти, виникає дилема між персональною відповідальністю, яка регулюється Загальним регламентом захисту персональних даних, та відповідальністю за продукт, яка ним не врегульована[998]. Для цього необхідне створення норм щодо відповідальності з метою заповнення прогалини між персональною відповідальністю та відповідальністю за продукт, наприклад робототехніку та ШІ, в тому числі автоматизоване прийняття рішень[999].

Наслідки для принципів захисту даних

Вказані вище характер, аналіз та використання великих даних кинули виклик застосуванню деяких традиційних, засадничих принципів європейського права захисту персональних даних[1000]. Такі виклики здебільшого стосуються принципів законності, мінімізації даних, обмеження мети та прозорості.

Принцип мінімізації даних вимагає, щоб персональні дані були адекватними, відповідними та зводилися до того, що необхідно для цілей, з якими вони обробляються. Однак бізнес-модель великих даних може бути цілковитою

997 Загальний регламент захисту персональних даних, статті 77–79 та стаття 82.

998 Європейський Парламент, Європейські норми цивільного права з робототехніки, Генеральний директорат з питань внутрішньої політики (жовтень 2016), сторінка 14.

999 *Промова Роберто Віоли* на медіасемінарі з питань європейського права з робототехніки в Європейському Парламенті. (Промова 16/02/2017); *Повідомлення* Європейського Парламенту щодо запиту до Комісії про надання пропозицій стосовно Положення про цивільну відповідальність за робототехніку та ШІ.

1000 Рада Європи, *Рекомендації щодо захисту фізичних осіб стосовно обробки персональних даних у світі Великих даних*, T-PD (2017) 01, Страсбург, від 23 січня 2017 р.

протилежністю мінімізації даних, оскільки вимагає все більше і більше даних, часто для невизначених цілей.

Це стосується і принципу обмеження мети, відповідно до якого дані повинні оброблятись у визначених цілях і не можуть бути використані у цілях, несумісних з першочерговою метою збирання, крім випадку здійснення такої обробки на законній підставі, такій як згода суб'єкта даних, але не обмежуючись нею (див. *розділ 4.1.1*).

Нарешті, великі дані також кидають виклик принципу точності даних, оскільки програми великих даних збирають відомості з різних джерел без можливості перевірки та/чи підтримання достовірності зібраних даних[1001].

Спеціальні правила та права

Загальним правилом залишається те, що персональні дані, які обробляються через аналітику великих даних, підпадають під дію законодавства про захист персональних даних. Однак до нормативно-правових актів ЄС та РЄ були введені спеціальні правила або відступи щодо окремих випадків, коли дані обробляються за допомогою складних алгоритмів.

Що стосується правових документів РЄ, Оновлена Конвенція 108 наділяє суб'єктів даних новими правами для здійснення більш ефективного контролю за своїми персональними даними в епоху великих даних. Це стосується, наприклад, статті 9 (1)(a), (c) та (d) Оновленої Конвенції 108 щодо права не підлягати рішенням, що мають значний вплив на особу і прийняті виключно на основі автоматизованої обробки даних, без врахування його або її думки; права на вимогу отримувати відомості про причини обробки даних, якщо результати такої обробки застосовуються до нього або неї, а також права на заперечення. Інші положення Оновленої Конвенції 108, зокрема щодо прозорості та додаткових зобов'язань, є додатковими елементами механізму захисту, встановленого Оновленою Конвенцією 108 для подолання цифрових викликів.

У законодавстві ЄС, за винятком перерахованих у статті 23 ЗРЗПД випадків, прозорість має бути забезпечена щодо всієї обробки даних. Це особливо важливо по відношенню до інтернет-послуг та іншої складної автоматизованої обробки даних, наприклад використання алгоритмів для процесу прийняття рішень. Тут властивості систем обробки даних мають надавати можливість суб'єктам даних реально розуміти, що відбувається з їхніми даними.

1001 ЄІЗПД (2016), *Когерентне забезпечення основних прав в еру великих даних*, Висновок 8/2016, від 23 вересня 2016 р., с. 8.

Відповідно до Загального регламенту захисту персональних даних, для забезпечення чесної та прозорої обробки контролер зобов'язаний надати суб'єкту даних змістовну інформацію щодо логіки, яка застосовується в автоматизованому прийнятті рішень, включаючи профайлінг[1002]. У рекомендації про захист та підтримку права на свободу вираження поглядів та права на повагу до приватного життя Комітет міністрів Ради Європи порекомендував провайдерам інтернет-послуг стосовно мережевої нейтральності «надавати користувачам чітку, повну та загальнодоступну інформацію щодо будь-яких методів управління трафіком, які можуть впливати на доступ користувачів та розповсюдження контенту, застосунків та послуг»[1003]. Звіти про методи управління трафіком, які створюються компетентними органами в усіх державах-членах, мають готуватись у відкритий та прозорий спосіб та бути в безплатному доступі для громадськості[1004].

Контролери даних мають **повідомляти** суб'єктам даних (як у випадку отримання даних від них, так і від інших суб'єктів) не лише певні відомості про дані, що збираються, та передбачувану обробку (див. *розділ 6.1.1*), але також, за необхідності, про наявність процесів автоматизованого прийняття рішень, надаючи їм «змістовну інформацію про логіку, що застосовується»[1005], цілі та потенційні наслідки таких процесів. Загальний регламент захисту персональних даних також визначає (лише у випадках, якщо дані були отримані не від суб'єкта даних), що контролер не зобов'язаний надавати суб'єкту даних інформацію, якщо «надання такої інформації було б неможливим чи вимагало б непропорційних зусиль»[1006]. При цьому, як наголошує Робоча група «Стаття 29» у *Рекомендаціях щодо автоматизованого прийняття рішень та профайлінгу для цілей Регламенту 2016/679,* складність обробки не повинна сама собою бути перешкодою для контролера в наданні суб'єкту даних чітких пояснень щодо цілей та аналітики, яка використовується в обробці даних[1007].

Права суб'єктів даних на **доступ**, **виправлення** та **видалення** їхніх персональних даних, а також їхнє право на **обмеження** обробки не передбачають

1002 Загальний регламент захисту персональних даних, стаття 13 (2) (f).

1003 Рада Європи, Комітет міністрів (2016), Рекомендація CM/Rec(2016)1 Комітету Міністрів державам-учасницям про захист та підтримку права на свободу вираження поглядів та права на повагу до приватного життя стосовно мережевої нейтральності, від 13 січня 2016 р., п. 5.1.

1004 Там само, п. 5.2.

1005 Загальний регламент захисту персональних даних, стаття, стаття 13 (2) f та 14 (2) g.

1006 Там само, стаття 14 (5) b.

1007 Робоча група «Стаття 29», *Рекомендації щодо автоматизованого прийняття рішень та профайлінгу для цілей Регламенту 2016/679*, РГ251, від 03 жовтня 2017 р., с. 14.

подібних винятків. Однак, з контролера може бути знято обов'язок повідомляти суб'єкт даних про будь-яке виправлення чи видалення його персональних даних (див. *розділ 6.1.4*), якщо таке повідомлення «було б неможливим чи вимагало б непропорційних зусиль»[1008].

Суб'єкти даних також мають право **заперечувати** відповідно до статті 21 ЗРЗПД (див. *розділ 6.1.6*) проти будь-якої обробки їхніх персональних даних, зокрема у випадку аналітики великих даних. Хоча контролери можуть бути звільнені від такого обов'язку, якщо вони зможуть довести наявність переважних легітимних інтересів, вони не будуть звільнені від цього обов'язку, якщо дані обробляються у цілях прямого маркетингу.

Контролери можуть вдаватися до відступу від цих прав у разі обробки персональних даних у суспільних інтересах для цілей архівування, наукових чи історичних досліджень або статистичних цілей[1009].

Стосовно **профайлінгу та автоматизованого прийняття рішень,** ЗРЗПД встановлено спеціальні норми: стаття 22 (1) передбачає, що суб'єкт даних «повинен мати право не підлягати рішенню, що ґрунтується винятково на автоматизованій обробці, зокрема профайлінгу, що породжує правові наслідки для нього або неї». Як підкреслено в рекомендаціях Робочою групою «Стаття 29», ця стаття встановлює загальну заборону на повністю автоматизоване прийняття рішень[1010]. Контролери можуть бути звільнені від такої заборони лише в трьох окремих випадках: якщо рішення 1) необхідне для виконання контракту між суб'єктом даних і контролером, 2) дозволене національним законом або законодавством ЄС, 3) приймається на основі явно висловленої згоди[1011].

Особистий контроль

Складність і недостатність прозорості аналітики великих даних може вимагати переосмислення ідей особистого контролю персональних даних. Слід пристосовуватися до певного соціального та технологічного контексту з урахуванням недостатньої обізнаності з боку людей. Отже, захист даних стосовно великих даних повинен здійснюватися з урахуванням ширшого поняття контролю над використанням даних, згідно з яким індивідуальний контроль

1008 Загальний регламент захисту персональних даних, стаття 19.

1009 Там само, стаття 89 (2) та (3).

1010 Робоча група «Стаття 29», *Рекомендації щодо автоматизованого прийняття рішень та профайлінгу для цілей Регламенту 2016/679*, wp251, від 03 жовтня 2017 р, с. 9.

1011 Загальний регламент захисту персональних даних, стаття 22 (2).

перетворюється на більш складний процес множинних оцінок впливу ризиків, пов'язаних з використанням даних[1012].

Якість програми великих даних залежить від того, наскільки добре вона може передбачити бажання або поведінку випробовуваних осіб (або споживачів). Нинішні моделі прогнозування, засновані на аналітиці великих даних, постійно вдосконалюються. Останні розробки передбачають не лише використання даних для класифікації особистостей (тобто поведінки та поглядів), а й аналіз поведінки через дослідження голосу та інтенсивності, з якою друкуються повідомлення, чи температури тіла. Ця інформація може бути використана в режимі реального часу в порівнянні, наприклад, з відомостями, отриманими з аналізу великих даних для оцінки кредитоспроможності під час зустрічі з представником банку. Оцінка здійснюється не за даними особи, яка звертається по кредит, а швидше за характеристиками її поведінки, які були отримані в результаті аналізу та оцінки відомостей великих даних, тобто яким голосом говорить кандидат – сильним чи підлесливим, якою є його мова чи температура тіла.

Профайлінг та цільова реклама не обов'язково будуть проблемою, якщо особи **обізнані** з тим, що вони є об'єктами спрямованих рекламних оголошень. Профайлінг стає проблемою, коли використовується для маніпулювання людьми, тобто пошуку певних особистостей та груп людей для політичної агітації. Наприклад, до груп виборців, які не визначилися, можна звертатися з політичними закликами, пристосованими до їхньої «особистості» та поглядів. Іншою проблемою може бути використання такого профайлінгу для відмови певним особам у доступі до товарів та послуг. Гарантією, яка може забезпечити захист від неправильного використання великих даних та особистої інформації, є псевдонімізація (див. *розділ 2.1.1*)[1013]. Випадки, коли персональні дані дійсно анонімізовані, тобто відсутня інформація, яка дає можливість відтворити зв'язок із суб'єктом персональних даних, не підпадають під дію Загального регламенту захисту персональних даних. Проблемою для законодавства з захисту персональних даних також є згода суб'єктів даних і фізичних осіб в обробці великих даних. Це стосується згоди бути об'єктом цільової реклами та профайлінгу, що може обґрунтовуватися міркуваннями «споживацького досвіду», та згоди на використання великої кількості персональних даних для вдосконалення і розробки аналітичних інструментів на основі інформації. Обізнаність щодо обробки великих даних або її відсутність викликає кілька питань стосовно засобів,

1012 Рада Європи, Консультативний Комітет Конвенції 108, *Рекомендації щодо захисту фізичних осіб стосовно обробки персональних даних у світі Великих даних,* T-PD(2017)01, Страсбург, від 23 січня 2017 р.

1013 Там само, с. 2.

за допомогою яких суб'єкти даних можуть реалізувати свої права, враховуючи, що обробка великих даних може ґрунтуватися на застосуванні алгоритмів як псевдонімізованої, так і анонімізованої інформації. В той час як псевдонімізовані дані підпадають під дію Загального регламенту захисту персональних даних, до анонімізованих даних він не застосовний. Особистий контроль над обробкою своїх персональних даних та обізнаність щодо неї є вирішальними в аналітиці великих даних: без цього фізичні особи не матимуть чіткого уявлення про те, хто є контролером чи оператором, що перешкоджатиме їм у реальному користуванні своїми правами.

10.2 Webs 2.0 та 3.0: соціальні мережі та інтернет речей

Ключові моменти

- Служби соціальних мереж (ССМ) – це комунікаційні онлайн-платформи, які надають людям можливість приєднуватись і створювати мережі однодумців.
- Інтернет речей – це підключення об'єктів до інтернету та взаємодія таких об'єктів між собою.
- Згода суб'єктів даних є найпоширенішою правовою підставою законної обробки персональних даних контролером у соціальних мережах.
- Користувачі соціальних мереж, як правило, захищені «побутовим винятком»; однак цей відступ може бути скасовано за окремих обставин.
- Провайдери соціальних мереж не захищені «побутовим винятком».
- Приватність за призначенням та за замовчуванням є ключовими для гарантування безпеки даних у цій сфері.

10.2.1 Визначення Webs 2.0 та 3.0

Служби соціальних мереж

Спочатку інтернет був задуманий як мережа для взаємозв'язку комп'ютерів та передачі повідомлень з обмеженою здатністю для обміну даними та з вебсайтами, які надаватимуть людям можливість лише пасивно переглядати їхній

контент[1014]. В еру Web 2.0 інтернет був трансформований у форум, на якому користувачі взаємодіють, співпрацюють та генерують дані. Ця ера характеризується надзвичайним успіхом та широким використанням служб соціальних мереж, які зараз є важливою частиною повсякденного життя мільйонів людей.

Служби соціальних мереж (ССМ) або «соціальні медіа» в широкому розумінні визначаються як «онлайн-платформи комунікацій, які надають людям можливість приєднуватись або створювати мережі однодумців»[1015]. Щоб приєднатися до мережі або створити її, особам пропонується надати персональні дані та створити свій обліковий запис. ССМ дозволяють користувачам створювати цифровий «контент», від фотографій та відеозаписів до посилань на газети та особистих нотаток , щоб висловити свою думку. За допомогою таких онлайн-платформ комунікацій користувачі можуть взаємодіяти та спілкуватися з кількома іншими користувачами. Важливо, що більшість популярних ССМ не вимагають жодних реєстраційних внесків. Замість того, щоб вимагати від користувачів плату за приєднання до мережі, провайдери ССМ отримують більшу частину своїх доходів від цільової реклами. Рекламодавці можуть отримати значну користь від особистої інформації, яка щодня розкривається на цих сайтах. Володіння інформацією про вік, стать, місцезнаходження та інтереси користувача допомагає їм доводити свою рекламу до відома «потрібних» людей.

Комітетом міністрів Ради Європи було прийнято Рекомендацію *про захист прав людини в контексті служб соціальних мереж*[1016], в окремому розділі якої йдеться про захист персональних даних, а у 2018 році було доповнено ще однією Рекомендацією про роль та обов'язки інтернет-посередників[1017].

Приклад: Нора дуже щаслива, тому що її партнер зробив пропозицію одружитися. Вона хоче поділитися приємною новиною з друзями і родиною та вирішує написати емоційну розповідь у соціальній мережі, висловлюючи свою радість, а також змінити статус своїх стосунків на «заручена». Невдовзі, коли вона входить до свого облікового запису, Нора бачить рекламу весільних суконь і квіткових магазинів. Чому так?

1014 Європейська Комісія (2016), *Поширення інтернету речей в Європі*, SWD(2016) 110 остаточний.

1015 Робоча група «Стаття 29» (2009), *Висновок 5/2009 про онлайн-соціальні мережі*, РГ 163, від 12 червня 2009 р., с. 4.

1016 Рада Європи, Комітет міністрів, *Рекомендація CM/Rec(2012)4 Комітету міністрів державам-учасницям про захист прав людини відносно служб соціальних мереж*, від 04 квітня 2012 р.

1017 Рада Європи, Комітет міністрів, Рекомендація CM/Rec(2018)2 Комітету міністрів державам-учасницям про роль та обов'язки інтернет-посередників, від 07 березня 2018 р.

Створюючи рекламу на Facebook, компанії з продажу весільних суконь та квітів вибрали певні параметри, щоб охопити таких людей, як Нора. Як тільки у профілі Нори вказується, що вона жінка, заручена та проживає в Парижі неподалік району місцезнаходження магазинів суконь та квітів, які розмістили рекламу, вона відразу бачить цю рекламу.

Інтернет речей

Інтернет речей (IP) являє собою наступний крок у розвитку інтернету: ера Web 3.0. За допомогою IP пристрої можуть бути підключені та взаємодіяти з іншими пристроями через інтернет. Це дає об'єктам і людям можливість спілкуватися через комунікаційні мережі, повідомляти про свій стан та/або про стан навколишнього середовища[1018]. IP та підключені пристрої є вже реальністю, і очікується, що вони істотно посиляться в найближчі кілька років зі створенням та подальшим розвитком «розумних» пристроїв, що призведе до створення «розумних» міст, «розумних» будинків та «розумного» бізнесу.

Приклад: IP може бути особливо корисним для охорони здоров'я. Компаніями вже були створені пристрої, сенсори та додатки, які надають можливість перевіряти стан здоров'я пацієнта. За допомогою використання начіпних кнопок тривоги та інших бездротових сенсорів, розміщених по всьому будинку, можливо відстежувати повсякденну поведінку самотніх людей похилого віку та отримувати сповіщення у разі значних змін у такій поведінці розкладі. Наприклад, людьми похилого віку широко використовуються датчики падіння. Ці датчики можуть точно визначити падіння та повідомити про це лікаря цієї особи та/або родину.

Приклад: Барселона є одним із найвідоміших прикладів «розумного міста». З 2012 року місто впроваджує використання інноваційних технологій, покликаних створити розумну систему громадського транспорту, утилізації відходів, паркування та освітлення вулиць. Для покращення прибирання відходів, наприклад, місто використовує розумні контейнери. Вони дають змогу перевіряти рівень відходів для оптимізації маршрутів збирання. Якщо контейнери майже повністю заповнені, вони передають сигнали через мережу мобільного зв'язку до програмного додатку,

1018 Європейська Комісія, Робочий документ персоналу Комісії, *Поширення інтернету речей в Європі*, SWD(2016) 110, від 19 квітня 2016 р.

який використовує компанія з утилізації відходів. Таким чином, компанія може спланувати найкращий маршрут збирання відходів, визначаючи пріоритети та/чи лише організовуючи збирання контейнерів, які потребують очищення.

10.2.2 Збалансування переваг і ризиків

Величезне розширення та успіх соціальних мереж за останнє десятиліття свідчать про те, що вони приносять **значну користь**. Наприклад, цільова реклама (як описано в наведеному прикладі) є дуже інноваційним способом, завдяки якому компанії можуть охопити свою аудиторію, пропонуючи їй більш конкретні товари. Споживачі можуть бути також зацікавлені в тому, щоб презентована їм реклама була більш доцільною та цікавою. Ще важливіше, що служби соціальних мереж та соціальні медіа можуть мати позитивний вплив на суспільство та впровадження змін. Вони дають користувачам можливість спілкуватися, взаємодіяти, організовувати групи та заходи з питань, що їх стосуються.

Так само IP, як очікується, принесе значну користь економіці, будучи частиною стратегії розвитку Єдиного цифрового ринку ЄС. Згідно з підрахунками, у межах ЄС у 2020 році кількість підключень до IP збільшиться до 6 мільярдів. Очікується, що таке розширення принесе значну вигоду економіці завдяки розвитку інноваційних сервісів та додатків, покращенню сфери охорони здоров'я, кращому розумінню потреб споживачів та підвищенню ефективності.

Водночас, враховуючи величезний обсяг особистої інформації, що генерується користувачами соціальних медіа та в подальшому обробляється операторами, розширення ССМ викликає **все більше занепокоєння** щодо шляхів, якими можуть захищатися приватне життя і дані. ССМ може становити загрози праву на приватне життя та праву на свободу вираження поглядів. До таких загроз можуть належати: «відсутність юридичних і процедурних гарантій щодо процесів, які можуть призвести до вилучення користувачів; неналежний захист дітей та молоді від шкідливого контенту чи поведінки; відсутність поваги до прав інших осіб; відсутність налаштувань захисту приватності за замовчуванням; відсутність прозорості стосовно мети збирання та обробки персональних даних»[1019]. Європейське законодавство щодо захисту персо-

1019 Рада Європи, Рекомендація Rec(2012)4 державам-учасницям Рекомендація CM/Rec(2012)4 Комітету міністрів державам-учасницям про захист прав людини відносно служб соціальних мереж, від 04 квітня 2012 р.

нальних даних намагається відповісти на виклики соціальних медіа стосовно захисту приватності та персональних даних. Такі принципи, як згода, захист приватного життя та персональних даних за призначенням і замовчуванням, а також права фізичних осіб, є особливо важливими в контексті соціальних медіа та мережевих служб.

У контексті IP ризики для приватності та захисту персональних даних несе величезний обсяг персональних даних, які генеруються з різноманітних взаємопов'язаних пристроїв. Попри те, що прозорість є важливим принципом європейського законодавства щодо захисту персональних даних, через безліч підключених пристроїв не завжди зрозуміло, хто здатний збирати, мати доступ та використовувати дані, зібрані з пристроїв IP[1020]. Однак згідно з правовими документами ЄС та РЄ, принцип прозорості встановлює обов'язок контролерів інформувати суб'єктів даних про те, яким чином їхні дані використовуються, із застосуванням чітких і простих формулювань. Ризики, правила, гарантії та права стосовно обробки їхніх персональних даних мають бути зрозумілими для людей. Підключені до IP пристрої, множинні процеси обробки та залучені дані також можуть бути кидати виклик вимозі щодо явної та поінформованої згоди на обробку даних, якщо така обробка здійснюється на підставі згоди. Люди часто не розуміють технічного процесу такої обробки та, відповідно, наслідків своєї згоди.

Іншою важливою проблемою є безпека, оскільки під'єднані пристрої особливо вразливі до ризиків, пов'язаних з технікою безпеки. Під'єднані пристрої мають різний рівень безпеки. Вони працюють поза межами стандартної IT інфраструктури, тож їм може бракувати достатньої обчислювальної потужності та місткості сховища для розміщення програмного забезпечення безпеки даних чи використання методів, таких як шифрування, псевдонімізація чи анонімізація з метою захисту особистої інформації користувачів.

Приклад: у Німеччині регулятори вирішили заборонити іграшку, яка підключалася до інтернету, через серйозне занепокоєння щодо її впливу на захист приватного життя дітей. Регулятори вирішили, що лялька на ім'я Кайла з підключенням до інтернету фактично є прихованим шпигунським пристроєм. Лялька працювала, надсилаючи звукові запитання дитини, що грала з нею, у додаток на цифровому пристрої, який перекладав їх у текст і шукав відповідь в інтернеті. Потім додаток надсилав відповідь ляльці, яка озвучувала її дитині. За допомогою цієї ляльки спілкування дитини, а

1020 Європейський інспектор із захисту персональних даних (2017), *Розуміння інтернету речей*.

також спілкування з дорослими поблизу могли записуватись і передаватися до додатку. Якби виробник ляльки не вжив належних заходів безпеки, будь-хто міг би використовувати її для прослуховування розмов.

10.2.3 Проблемні питання стосовно захисту персональних даних

Згода

У Європі обробка персональних даних є правомірною, лише якщо вона дозволена європейським законодавством про захист персональних даних. Для провайдерів служб соціальних мереж згода суб'єктів даних, як правило, є законною підставою для обробки персональних даних. Згода має бути вільно наданою, явною, поінформованою та однозначною (див. *розділ 4.1.1*)[1021]. «Вільно надана» по суті означає, що суб'єкти даних повинні мати можливість зробити реальний та справжній вибір. Згода є «явною» та «поінформованою», якщо вона ясна, очевидно та точно стосується повного обсягу, цілей та наслідків обробки персональних даних. У контексті соціальних медіа є спірним питанням, чи є згода вільною, явною та поінформованою для всіх типів обробки, які здійснюються оператором служб соціальних мереж та третіми особами.

Приклад: для приєднання та доступу до соціальної мережі особам часто доводиться погоджуватися на різні види обробки своїх персональних даних, не отримуючи необхідних технічних характеристик чи альтернативних варіантів. Прикладом може бути необхідність згоди на отримання поведінкової реклами для реєстрації в соціальних мережах. Як зазначає Робоча група «Стаття 29» у висновку щодо визначення згоди, «враховуючи важливу роль, що її набули деякі соціальні мережі, декотрі категорії користувачів (наприклад, підлітки) погодяться на отримання поведінкової реклами, щоб уникнути ризику бути частково виключеними із соціальної взаємодії. Користувачу має бути надана можливість дати вільну та явну згоду на отримання поведінкової реклами, незалежно від доступу до соціальної мережі»[1022].

1021 Загальний регламент захисту персональних даних, стаття 4 та стаття 7; Оновлена Конвенція 108, стаття 5.

1022 Робоча група «Стаття 29» (2011), *Висновок 15/2011 щодо визначення згоди*, РГ 187, від 13 липня 2011р., с. 18.

Відповідно до Загального регламенту захисту персональних даних персональні дані дітей молодше 16 років не можуть в принципі, оброблятися на підставі їхньої згоди[1023]. Якщо необхідна згода на обробку, її має надати один з батьків або опікун дитини. Діти заслуговують на особливий захист у зв'язку з тим, що вони можуть бути менше обізнаними з ризиками та наслідками, що стосуються обробки персональних даних. Це дуже важливо в контексті соціальних медіа, оскільки діти більше наражаються на деякі негативні наслідки, які може спричинити використання таких засобів зв'язку, наприклад кібербулінг, онлайн переслідування чи викрадення ідентичності.

Безпека та приватність/захист персональних даних за призначенням і за замовчуванням

За своєю природою обробка персональних даних пов'язана з ризиками з огляду на постійну можливість порушення умов безпеки, які призводять до випадкового або незаконного знищення, втрати, зміни, несанкціонованого доступу або розкриття персональних даних, що обробляються. Відповідно до європейського законодавства про захист персональних даних контролери та оператори зобов'язані вживати відповідних технічних та організаційних заходів для запобігання будь-якому несанкціонованому втручанню в операції обробки персональних даних. Провайдери служб соціальних мереж, які підпадають під дію європейських правил захисту персональних даних, також повинні дотримуватися цього зобов'язання.

Принципи захисту приватного життя/персональних даних за призначенням та за замовчуванням вимагають від контролерів забезпечувати, щоб використовувані ними продукти були безпечними, та автоматично застосовувати відповідні налаштування приватності та захисту даних. Це означає, що коли людина вирішила приєднатися до соціальної мережі, постачальник послуг не може автоматично робити всю інформацію про нового користувача сервісу доступною для всіх інших його користувачів. Під час приєднання до служби налаштування приватності та захисту персональних даних за замовчуванням повинні бути такими, щоб ця інформація була доступною лише для обраних цією людиною контактів. Розширення доступу для людей поза цим списком повинно бути можливим після зміни користувачем вручну налаштувань приватності та захисту персональних даних за замовчуванням. Це також може мати наслідки у випадках, коли відбувається витік даних, незважаючи на вжиті заходи безпеки.

1023 Див. Загальний регламент захисту персональних даних, стаття 8. Держави-члени ЄС можуть передбачати в законі нижчий вік за умови, що такий вік буде не менше 13 років.

У таких випадках провайдери служб повинні повідомляти користувачів, якщо це ймовірно призведе до високого ризику для прав і свобод суб'єкта даних[1024].

Приватність/захист персональних даних за призначенням та за замовчуванням є особливо важливими в контексті соціальних мереж, оскільки крім ризиків несанкціонованого доступу, можливих у більшості типів обробки, поширення особистої інформації в соціальних медіа створює додаткові ризики для безпеки. Часто це відбувається через недостатність розуміння людьми, *хто* може мати доступ до їхніх даних, і як ці особи можуть їх використати. З огляду на широко розповсюджене використання соціальних медіа, кількість випадків і жертв крадіжок ідентичності зросла.

Приклад: крадіжка ідентичності – це явище, коли певна особа отримує інформацію, дані чи документи, що належать іншій особі (жертві), а потім використовує цю інформацію, видаючи себе за жертву з метою отримання товарів і послуг від її імені. Наприклад, Пол має обліковий запис на вебсайті соціальної мережі. Пол працює вчителем та є активним членом своєї громади, він дуже комунікабельний і особливо не переймається щодо налаштувань приватності та захисту персональних даних свого облікового запису в соціальній мережі. У нього великий список контактів, в тому числі людей, яких він не обов'язково знає особисто. Оскільки він працює у великій школі і став досить популярним, тренуючи шкільну футбольну команду, він вважає, що ці люди, швидше за все, є батьками учнів чи друзями школи. Електронна адреса та день народження Пола відображаються в його обліковому записі в соціальній мережі. Крім того, Пол постійно публікує світлини свого собаки Тобі, що супроводжуються таким підписом: «Ми з Тобі на нашій ранковій пробіжці». Пол не збагнув, що одним з найпопулярніших питань, що ставиться для захисту електронної скриньки чи мобільного облікового запису є «яке ім'я вашої домашньої тварини». Використовуючи інформацію, доступну в профілі Пола в соціальній мережі, Ніку легко вдалося зламати облікові записи Пола.

Права фізичних осіб

Провайдери ССМ повинні поважати права фізичних осіб (див. *розділ 6.1*), в тому числі право бути поінформованим про мету обробки та про те, яким

1024 Там само, стаття 34.

чином персональні дані можуть використовуватися для цілей прямого маркетингу. Фізичним особам також повинно бути надано право доступу до персональних даних, які вони створили на платформі соціальних мереж, та вимагати їх видалення. Навіть коли фізичні особи погодились на обробку персональних даних та завантажили інформацію до інтернету, вони повинні мати можливість звернутися з вимогою «бути забутими» у разі, якщо вони більше не бажають користуватися послугами соціальної мережі. Право на мобільність даних додатково надає можливість користувачам отримувати копію персональних даних, наданих ними провайдеру служб соціальних мереж, у структурованому, загальновживаному і машиночитаному форматі та передавати свої дані від одного провайдера служб соціальних мереж до іншого[1025].

Контролери

Складним питанням, яке часто виникає в контексті соціальних медіа, є питання щодо контролера, тобто хто є суб'єктом, який має зобов'язання та має нести відповідальність за дотримання правил захисту персональних даних. Провайдери служб соціальних мереж вважаються контролерами відповідно до європейського законодавства про захист персональних даних. Це очевидно з огляду на широкі рамки визначення поняття «контролер» та той факт, що такі провайдери послуг визначають мету та засоби обробки персональних даних, які надають фізичні особи. Відповідно до законодавства ЄС контролери зобов'язані дотримуватися положень Загального регламенту захисту персональних даних, якщо вони пропонують послуги суб'єктам даних у ЄС, навіть якщо ті не мають осідку в ЄС.

Чи можуть користувачі послуг соціальних мереж також розглядатись як контролери? Якщо фізичні особи обробляють персональні дані «в процесі суто особистої чи побутової діяльності», норми захисту персональних даних не застосовуються. У європейському законодавстві про захист персональних даних це явище відоме як «побутовий виняток». Втім у деяких випадках користувач послуги соціальних мереж може не підпадати під побутовий виняток.

Користувачі добровільно діляться своєю особистою інформацією в режимі онлайн. Однак оприлюднена в режимі онлайн інформація часто містить особисту інформацію про інших фізичних осіб.

1025 Загальний регламент захисту персональних даних, стаття 21.

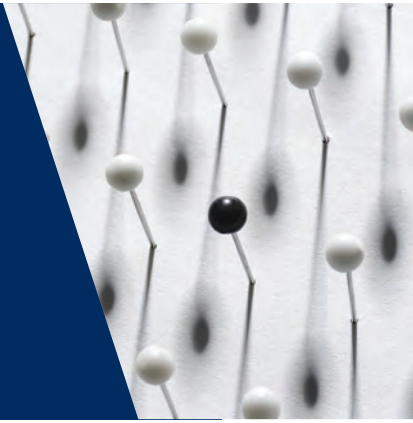
Приклад: у Пола є обліковий запис на дуже популярній платформі соціальної мережі. Пол намагається стати актором та використовує свій обліковий запис для розміщення фотографій, відеозаписів та постів, які вказують на його пристрасть до мистецтва. Популярність є дуже важливою для його майбутнього, тому він вирішив, що його профіль має бути доступним не лише для закритого списку його контактів, а для всіх інтернет-користувачів, незалежно від того, чи є вони учасниками мережі. Чи може Пол розміщувати світлини та відеозаписи себе зі своєю подругою Сарою без її згоди? Сара – вчителька початкових класів і намагається не посвячувати у своє приватне життя роботодавця, своїх учнів та їхніх батьків. Уявімо ситуацію, коли Сара, яка не користується соціальними мережами, дізнається від їхнього спільного друга Ніка, що її світлину на вечірці з Полом було розміщено в Інтернеті. У такому випадку обробка даних Полом не підпадає під дію законодавства ЄС, оскільки вона охоплюється «побутовим винятком».

Однак для користувачів важливо усвідомлювати та пам'ятати, що завантаження інформації про інших фізичних осіб без їхньої згоди може порушити їхні права на приватність та захист персональних даних. Навіть у випадках застосовності побутового винятку (наприклад, коли користувач має профіль, який є відкритим лише для переліку обраних ним чи нею контактів) користувач все ще може нести відповідальність за оприлюднення особистої інформації інших осіб. Хоча правила захисту персональних даних не застосовуються у випадку побутового винятку, відповідальність може виникнути відповідно до інших норм, що існують у певній країні, наприклад, щодо наклепу чи порушення особистих немайнових прав. Зрештою, лише користувачі ССМ захищені побутовими винятками, а контролери та оператори, які надають засоби для такої особистої обробки даних, підпадають під дію законодавства ЄС про захист персональних даних[1026].

Після реформи Директиви про конфіденційність та електронні комунікації правила щодо захисту даних, приватності та безпеки, які застосовуються до провайдерів послуг телекомунікацій відповідно до чинної законодавчої бази, також застосовуватимуться до комунікації між машинами та до електронних комунікаційних послуг, у тому числі, наприклад, до послуг на замовлення.

1026 Там само, п. 18 преамбули.

Додаткові джерела інформації



Глава 1

Араселі Мангас, М. (ред.) (2008), Хартія основних прав Європейського Союзу, Більбао, Фонд BBVA.

Берка, В. (2012), Основоположне право на захист персональних даних у конфлікті між свободою і безпекою, Відень, Видавництво «Manzsche Verlags-und Universitätsbuchhandlung».

Вайт, Р. і Ові, С. (2010), Європейська конвенція з прав людини, Оксфорд, Видавництво «Oxford University Press».

Воррен, С. і Брандейс, Л. (1890), «*Права на приватність»,* Гарвардський юридичний журнал (Harvard Law Review), Том 4, № 5, С. 193–220.

Гарріс, Д., О'Бойл, М., Ворбрік, Ц. і Бейтс, Е. (2009), Право Європейської конвенції з прав людини, Оксфорд, Видавництво «Oxford University Press».

Гіймайнс, Г. (2016), Європейський Союз як охоронець інтернет-приватності – історія статті 16 ДФЄС, Видавництво «Springer».

Гонсалес Фустер, Г. і Гелерт, Г. (2012), «Основне право на захист персональних даних в Європейському Союзі: у пошуках непізнаного права», Міжнародний журнал про право, комп'ютери та технології (*International Review of Law, Computers and Technology)*, Том 26 (1), с. 73–82.

Грабенвартер, К. і Пабел, К. (2012), Європейська конвенція з прав людини, Мюнхен, Видавництво «C. H. Beck».

Густінкс, П. (2016), «*Право ЄС про захист персональних даних: огляд Директиви 95/46/ЕС та проєкту Загального регламенту захисту персональних даних*».

Гутвірт, С., Пулле, У., Де Герт, П., Де Тервань, С. і Нувт, С. (ред) (2009), Повторний винахід захисту персональних даних, Видавництво «Springer».

Джарасс, Г. (2010), Хартія основних прав Європейського Союзу, Мюнхен, Видавництво «C. H. Beck».

Доксі, К. «Чотири основних права: пошук балансу», журнал «Міжнародне право приватності даних» (*International Data Privacy Law)*, Том 6, № 3, с. 195–209.

Європейські цифрові права (EDRi), *Вступ до захисту персональних даних*, Брюсель.

Кокотт, Д. і Собота, С. (2013), «Відмінність приватності та захисту персональних даних у практиці Суду ЄС та ЄСПЛ», Журнал «Міжнародне право приватності даних» (*International Data Privacy Law)*, Том 3, № 4, с. 222–228.

Краненбург, Г. (2015), «Google та право бути забутим», Журнал європейського права про захист персональних даних (*European Data Protection Law Review)*, Том 1, № 1, с. 70–79.

Лінскі, О. (2014), «Деконструкція захисту персональних даних: «додана вартість» права на захист персональних даних у правовому порядку ЄС», періодичне (квартальне) видання «Міжнародне та порівняльне право» (*International and Comparative Law Quarterly)*, Том 63, № 3, с. 569–597.

Лінскі, О. (2015), Основи права ЄС про захист персональних даних, Оксфорд, Видавництво «Oxford University Press».

Майєр, Дж. (2011), Хартія основних прав Європейського Союзу, Баден-Баден, Видавництво «Nomos».

Моубрей, А. (2012), Справи, матеріали та коментарі до Європейської конвенції з прав людини, Оксфорд, Видавництво «Oxford University Press».

Новак, М., Янушевскі, К. і Хофстеттер, Т. (2012), Усі права людини для всіх – віденський посібник з прав людини, Антверпен, Видавництва «Intersentia N. V.», «Neuer Wissenschaftlicher».

Пішарель, С. і Кутрон, Л. (2010), Хартія основних прав Європейського Союзу та Європейська конвенція з прав людини, Брюссель, Видавництво «Emile Bruylant».

Сімітіс, С. (1997), «Директива ЄС про захист даних – застій чи стимул?», Новий юридичний тижневик (Neue Juristische Wochenschrift), № 5, с. 281–288.

Фровайн, Й. і Пойкерт, В. (2009), Європейська конвенція з прав людини, Берлін, Видавництво «N. P. Engel».

Глава 2

Аквійсті, А., та Грос Р. (2009), «*Передбачення номерів соціального страхування на основі публічних даних*», Праці Національної академії наук, 07 липня 2009.

Гонсалес Фустер, Г. (2014), Виникнення права на захист персональних даних як фундаментального права в ЄС, Видавництво «Springer».

Дельгадо, Л. (2008), Приватність та захист персональних даних в Європейському Союзі, Мадрид, Видавництво «Dykinson S. L.».

Десжен-Пасану, Г. (2012), Захист інформації персонального характеру, Париж, Видавництво «LexisNexis».

Ді Мартіно, А. (2005), Захист персональних даних у європейському праві, Баден-Баден, Видавництво «Nomos».

Ді Маунтжой, І.-А., Ідальго, С. А., Верлісен, М., і Блондель В. Д. (2013), «Унікальність у натовпі: межі приватності людської мобільності», журнал «Наукові огляди» (*Nature Scientific Reports*), Том 3, 2013.

Кері, П. (2009), Захист персональних даних: Практичний посібник з права Сполученого Королівства і ЄС, Оксфорд, Видавництво «Oxford University Press».

Марган, Р. і Бордман, Р. (2012), 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.

Офіс Інформаційного комісара Сполученого Королівства (2012), *Анонімізація: управління ризиками захисту персональних даних. Кодекс практики.*

Самараті, П. і Свіні, Л. (1998), «*Захист приватності при розкритті інформації: k-анонімність та її застосування шляхом узагальнення та приховування*», Технічний звіт SRI-CSL-98-04.

Свіні, Л. (2002), «K-анонімність: модель для захисту приватності», Міжнародний журнал про невизначеність, неясність та системи знань (*International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*), Том 10, № 5, с. 557–570.

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».

Глави 3–6

АОП (2010), Розробка показників для захисту, поваги та заохочення прав дитини в Європейському Союзі (видання для конференції), Відень, АОП.

АОП (2011), Доступ до правосуддя в Європі: огляд викликів та можливостей, Люксембург, Бюро публікацій.

АОП (Агенція Європейського Союзу з основних прав) (2010), Захист персональних даних у Європейському Союзі: роль національних органів з питань захисту даних (Зміцнення структури основних прав у ЄС II), Люксембург, Бюро публікацій Європейського Союзу (Бюро публікацій).

Брюганн, У. (2012), «Директива 95/46/ЕС «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» у: Грабіц, Е., Гільф, М. і Неттесгайм, М. (ред.), Право Європейського Союзу, Том IV, A. 30, Мюнхен, Видавництво «C. H. Beck».

Дамманн, У. і Сімітіс, С. (1997), Директива ЄС про захист персональних даних, Баден-Баден, Видавництво «Nomos».

Де Герт, П. і Папаконстантіну, В. (2012), «Директива про захист персональних даних у сфері діяльності поліції та кримінального судочинства: коментар та аналіз», Журнал «Комп'ютери та право *SCL*» (*Computers & Law Magazine of SCL)*, Том 22, № 6, с. 1–5.

Де Герт, П. і Папаконстантіну, В. (2012), «Проєкт Регламенту про захист персональних даних на заміну Директиви 95/46/ЕС: ефективна система захисту фізичних осіб», Журнал комп'ютерного права та безпеки (*Computer Law & Security Review)*, Том 28, № 2, с. 130–142.

Ірландська служба охорони здоров'я та якості (2010), *Посібник оцінки впливу на приватність у галузі охорони здоров'я та соціального обслуговування*.

К'єркегор, С., Вотерс, Н., Грінліф, Г., Біргайв, Л. А., Ллойд, І. і Саксбі, С. (2011), «30 років – Огляд Конвенції 108 Ради Європи про захист персональних даних», Журнал комп'ютерного права та безпеки (*Computer Law & Security Review)*, Том 27, № 3, с. 223–231.

Каррен, Л. і Кей, Дж. (2010), «Відкликання згоди: «сліпа зона» в праві про захист персональних даних?», Журнал комп'ютерного права та безпеки (*Computer Law & Security Review)*, Том 26, № 3, с. 273–283.

Конде Ортіс, К. (2008), Захист персональних даних, Кадіс, Видавництво «Dykinson».

Кудре, Л. (2010), Захист персональних даних у Європейському Союзі, Саарбрюкен, Видавництво «Editions universitaires europeennes».

Офіс Інформаційного комісара Сполученого Королівства, *Оцінка впливу на приватність.*

Сімітіс, С. (2011 р.), Федеральний закон про захист персональних даних, Баден-Баден, Видавництво «Nomos».

Феретті, Федеріко (2012), «Європейська перспектива щодо згоди на обробку персональних даних через реконцептуалізацію європейського «дзеркала» захисту персональних даних після Лісабонської угоди: серйозне ставлення до прав», Європейський журнал приватного права (*European Review of Private Law)*, Том 20, № 2, с. 473–506.

Глава 7

Гутвірт, С., Пулле, У., Де Герт, П., Де Тервань, С. і Нувт, С. (2009), Повторний винахід захисту персональних даних?, Берлін, Видавництво «Springer».

Європейський інспектор із захисту персональних даних (2014), *Довідка щодо передачі персональних даних до третіх країн та міжнародних організацій інституціями та органами ЄС*.

Кюнер, С. (2007), Європейське інформаційне право, Оксфорд, Видавництво «Oxford University Press».

Кюнер, С. (2013), Законодавство про транскордонну передачу персональних даних і закон про конфіденційність даних, Оксфорд, Видавництво «Oxford University Press».

Робоча група «Стаття 29» (2005), *Робочий документ щодо загального тлумачення статті 26(1) Директиви 95/46/ЕС від 24 жовтня 1995.*

Глава 8

Бем, Ф. (2012), Обмін інформацією та захист персональних даних у просторі свободи, безпеки та справедливості. На шляху до гармонізованих принципів захисту персональних даних для обміну інформацією на рівні ЄС, Берлін, Видавництво «Springer».

Блазі Касагран, К. (2016), Глобальний захист персональних даних у сфері правопорядку, перспектива ЄС, Лондон, Видавництво «Routledge».

Гутвірт, С., Пулле, У. і Де Герт, П. (2010), Захист персональних даних у профільованому світі, Дордрехт, Видавництво «Springer».

Гутвірт, С., Пулле, У., Де Герт, П. і Лінс, Р. (2011), Комп'ютери, конфіденційність і захист персональних даних: Елемент вибору, Дордрехт, Видавництво «Springer».

Гутьєрес Зарза, А. (2015), Обмін інформацією та захист персональних даних у транскордонних кримінальних провадженнях у Європі, Берлін, Видавництво «Springer».

Де Герт, П. та Папаконстантіну, В. (2012), «Директива про захист персональних даних у сфері діяльності поліції та кримінального судочинства: коментар та аналіз», Журнал «Комп'ютери та право SCL» (Computers & Law Magazine of SCL), Том 22, № 6, с. 1–5.

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), *Захист персональних даних у Європолі*, Люксембург, Бюро публікацій.

Євроюст, Захист персональних даних у Євроюсті: Надійний, ефективний та спеціалізований режим, Гаага, Євроюст.

Констадінідес, Т. (2011), 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), *Роль Європейського Парламенту в укладенні трансатлантичних угод про передачу персональних даних після Лісабонської угоди*, Центр права зовнішніх зносин ЄС, Робочі матеріали ЦПЗЗ – 2013/2.

Глава 9

Бюллесбах, А., Гійрат, С., Пулле, У. і Хакон, Р. (2010), Короткий огляд європейського права у сфері інформаційних технологій, Амстердам, Видавництво «Kluwer Law International».

Гутвірт, С., Лінс, Р., Де Герт, П. і Пулле, У. (2012), Європейський захист персональних даних: чи в доброму стані?, Дордрехт, Видавництво «Springer».

Гутвірт, С., Пулле, У. і Де Герт, П. (2010), Захист персональних даних у профільованому світі, Дордрехт, Видавництво «Springer».

Гутвірт, С., Пулле, У., Де Герт, П. і Лінс, Р. (2011), Комп'ютери, конфіденційність і захист персональних даних: Елемент вибору, Дордрехт, Видавництво «Springer».

Констадінідес, Т. (2011), 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), Законодавство і практика захисту персональних даних, Лондон, Видавництво «Sweet & Maxwell».

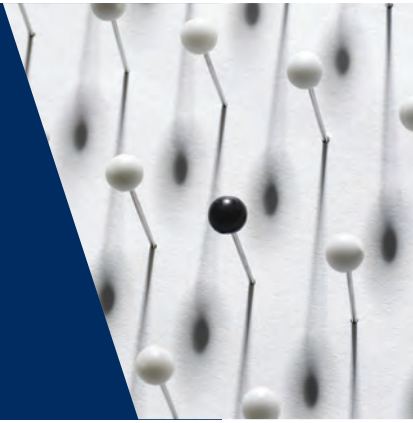
Глава 10

Ель Емам, Х. та Альварес, К. (2015), «Критична оціка Висновку Робочої групи «Стаття 29» 05/2014 про методи анонімізації», журнал «Міжнародне право приватності даних» (*International Data Privacy Law)*, Том 5, № 1, с. 73–87.

Майєр-Шенбергер, В. та Кейт, Ф. (2013), «Повідомлення та згода у світі Big Data», журнал «Міжнародне право приватності даних» (*International Data Privacy Law)*, Том 3, № 2, с. 67–73.

Рубінштейн, А. (2013), «Big Data: Кінець приватності чи новий початок?», журнал «Міжнародне право приватності даних» (*International Data Privacy Law)*, Том 3, № 2, с. 74–87.

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. Г. 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.
«М. К. проти Франції» (*M.K. v. France*), № 19522/09, 18 квітня 2013 р.
«Одієвр проти Франції» (*Odievre v. France*) [ВП], № 42326/98, 13 лютого 2003 р.

Баланс між захистом персональних даних та правом на вираження поглядів і правом на інформцію

«"Axel Springer AG" проти Німеччини» (*Axel Springer AG v. Germany*)[ВП], № 39954/08, 07 лютого 2012 р.
«"Coudec and Hachette Filipacchi Associés" проти Франції» (*Coudec and Hachette Filipacchi Associés v. France*) [ВП], № 40454/07, 10 листопада 2015 р.
«"Satakunnan Markkinapörssi Oy" та "Satamedia Oy" проти Фінляндії» (*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*), № 931/13, 27 червня 2017 р.
«Асоціація візуальних художників проти Австрії» (*Vereinigung bildender Künstler v. Austria*), № 68354/01, 25 січня 2007 р.

«Болен проти Німеччини» (*Bohlen v. Germany*), № 53495/09, 19 лютого 2015 р.
«Мюллер та інші проти Швейцарії» (*Müller and Others v. Switzerland*), № 10737/84, 24 травня 1988 р.
«Угорський Гельсінський комітет проти Угорщини» (*Magyar Helsinki Bizottság v. Hungary*) [ВП], № 18030/11, 08 листопада 2016 р.
«Фон Ганновер проти Німеччини» (*Von Hannover v. Germany*) (*No. 2*) [ВП], № 40660/08 та 60641/08, 07 лютого 2012 р.

Баланс між захистом персональних даних і свободою віросповідання

«Сінан Ішик проти Туреччини» (*Sinan Işık v. Turkey*), № 21924/05, 02 лютого 2010 р.

Виклики для захисту персональних даних в режимі онлайн

«K.U. проти Фінляндії» (*K.U. v. Finland*), № 2872/02, 02 грудня 2008 р.

Згода суб'єкта даних

«Y проти Туреччини» (*Y v. Turkey*), № 648/10, 17 лютого 2015 р.
«Елберте проти Латвії» (*Elberte v. Latvia*), № 61243/08, 13 січня 2015 р.
«Сінан Ішик проти Туреччини» (*Sinan Işık v. Turkey*), № 21924/05, 02 лютого 2010 р.

Листування

«Аманн проти Швейцарії» (*Amann v. Switzerland*) [ВП], № 27798/95, 16 лютого 2000 р.
«Асоціація за європейську інтеграцію і права людини і Екімджієв проти Болгарії» (*Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*), № 62540/00, 28 червня 2007 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.
«D. Л. проти Болгарії» (*D. L. v. Bulgaria*), № 7472/14, 19 травня 2016 р.
«Даля проти Франції» (*Dalea v. France*), № 964/07, 02 лютого 2010 р.
«Джемалеттін Джанлі проти Туреччини» (*Cemalettin Canli v. Turkey*), № 22427/04, 18 листопада 2008 р.
«Леандер проти Швеції» (*Leander v. Sweden*), № 9248/81, 26 березня 1987 р.

«Мелоун проти Сполученого Королівства» (*Malone v. the United Kingdom*), № 8691/79, 02 серпня 1984 р.
«Ротару проти Румунії» (*Rotaru v. Romania*) [ВП], № 28341/95, 04 травня 2000 р.
«С. та Марпер проти Сполученого Королівства» (*S. and Marper v. the United Kingdom*), № 30562/04 і 30566/04, 04 грудня 2008 р.
«"Санді Таймс" проти Сполученого Королівства» (*The Sunday Times v. the United Kingdom*), № 6538/74, 26 квітня 1979 р.
«Сільвер та інші проти Сполученого Королівства» (*Silver and Others v. the United Kingdom*), №№ 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 березня 1983 р.
«Хараламбі проти Румунії» (*Haralambie v. Romania*), № 21737/03, 27 жовтня 2009 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 інформації про судимість

«Б. Б. проти Франції» (*B. B. v. France*), № 5335/06, 17 грудня 2009 р.
«Брюне проти Франції» (*Brunet v. France*), № 21010/10, 18 вересня 2014 р.
«Ейкагі проти Франції» (*Aycaguer v. France*), № 8806/12, 22 червня 2017 р.
«М. К. проти Франції» (*M. K. v. France*), № 19522/09, 18 квітня 2013 р.
«М. М. проти Сполученого Королівства» (*M. M. v. the United Kingdom*), № 24029/07, 13 листопада 2012 р.

Захист даних

«К. Г. та інші проти Словаччини» (*K. H. and Others v. Slovakia*), № 32881/04, 28 квітня 2009 р.
«Хараламбі проти Румунії» (*Haralambie v. Romania*), № 21737/03, 27 жовтня 2009 р.

Бази ДНК

«С. та Марпер проти Сполученого Королівства» (*S. and Marper v. the United Kingdom*) [ВП], № 30562/04 та 30566/04, 04 грудня 2008 р.

GPS-дані

«Узун проти Німеччини» (*Uzun v. Germany*), № 35623/05, 02 вересня 2010 р.

Дані про стан здоров'я

«Y проти Туреччини» (*Y v. Turkey*), № 648/10, 17 лютого 2015 р.
«Авілкіна та інші проти Росії» (*Avilkina and Others v. Russia*), № 1585/09, 06 червня 2013 р.
«Бірюк проти Литви» (*Biriuk v. Lithuania*), № 23373/03, 25 листопада 2008 р.
«Жулук проти Сполученого Королівства» (*Szuluk v. the United Kingdom*), № 36936/05, 02 червня 2009 р.
«Z. проти Фінляндії» (*Z. v. Finland*), № 22009/93, 25 лютого 1997 р.
«I. 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.
«Л. Г. проти Латвії» (*L. H. v. Latvia*), № 52019/07, від 29 квітня 2014 р.
«M. C. 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*) [ВП], № 42326/98, 13 лютого 2003 р.
«Чуботару проти Молдови» (*Ciubotaru v. Moldova*), № 27138/04, 27 квітня 2010 р.

Інформація стосовно професійної діяльності

«G.S.B. проти Швейцарії» (*G.S.B. v. Switzerland*), № 28601/11, 22 грудня 2015 р.
«M. N. та інші проти Сан-Марино» (*M.N. and Others v. San Marino*), № 28005/12, 07 липня 2015 р.
«Мішо проти Франції» (*Michaud v. France*), № 12323/11, 06 грудня 2012 р.
«Нємец проти Німеччини» (*Niemietz v. Germany*), № 13710/88, 16 грудня 1992 р.

Перехоплення повідомлень

«Аманн проти Швейцарії» (*Amann v. Switzerland*) [ВП], № 27798/95, 16 лютого 2000 р.
«Бріто Феррінью Бексіга Вілла-Нова проти Португалії» (*Brito Ferrinho Bexiga Villa-Nova v. Portugal*), № 69436/10, 01 грудня 2015 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, від 02 червня 2009 р.
«Йордачі та інші проти Молдови» (*Iordachi and Others v. Moldova*), № 25198/02, 10 лютого 2009 р.

«Копланд проти Сполученого Королівства» (*Copland v. the United Kingdom*), № 62617/00, 3 квітня 2007 р.
«Копп проти Швейцарії» (*Kopp v. Switzerland*), № 23224/94, 25 березня 1998 р.
«Ліберті та інші проти Сполученого Королівства» (*Liberty and Others v. The United Kingdom*), № 58243/00, 01 липня 2008 р.
«Мелоун проти Сполученого Королівства» (*Malone v. the United Kingdom*), № 8691/79, 02 серпня 1984 р.
«Мустафа Сержін Танрікулу проти Туреччини» (*Mustafa Sezgin Tanrıkulu v. Turkey*), № 27473/06, 18 липня 2017 р.
«Прутеану проти Румунії» (*Pruteanu v. Romania*), № 30181/05, 03 лютого 2015 р.

Обов'язки контролерів

«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.

Персональні дані

«Аманн проти Швейцарії» (*Amann v. Switzerland*) [ВП], № 27798/95, 16 лютого 2000 р.
«"Бернх Ларсен Холдинг АС" та інші проти Норвегії» (*Bernh Larsen Holding AS and Others v. Norway*), № 24117/08, 14 березня 2013 р.
«Узун проти Німеччини» (*Uzun v. Germany*), № 35623/05, 02 вересня 2010 р.

Фотографії

«Фон Ганновер проти Німеччини» (*Von Hannover v. Germany*), № 59320/00, 24 червня 2004 р.
«Шякка проти Італії» (*Sciacca v. Italy*), № 50774/99, 11 січня 2005 р.

Право бути забутим

«"Satakunnan Markkinapörssi Oy" та "Satamedia Oy" проти Фінляндії» (*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*), № 931/13, 27 червня 2017 р.
«Зегерштед-Віберг та інші проти Швеції» (*Segerstedt-Wiberg and Others v. Sweden*), № 62332/00, 06 червня 2006 р.

Право на заперечення

«Леандер проти Швеції» (*Leander v. Sweden*), № 9248/81, 26 березня 1987 р.
«М. С. проти Швеції» (*M.S. v. Sweden*), № 20837/92, 27 серпня 1997 р.
«Мослі проти Сполученого Королівства» (*Mosley v. the United Kingdom*), № 48009/08, 10 травня 2011 р.
«Ротару проти Румунії» (*Rotaru v. Romania*) [ВП], № 28341/95, 04 травня 2000 р.
«Сінан Ішик проти Туреччини» (*Sinan Işık v. Turkey*), № 21924/05, 02 лютого 2010 р.

Чутливі дані

«Брюне проти Франції» (*Brunet v. France*), № 21010/10, 18 вересня 2014 р.
«І. проти Фінляндії» (*I v. Finland*), № 20511/03, 17 липня 2008 р.
«Мішо проти Франції» (*Michaud v. France*), № 12323/11, 06 грудня 2012 р.
«С. та Марпер проти Сполученого Королівства» (*S. and Marper v. the United Kingdom*) [ВП], № 30562/04 та 30566/04, 04 грудня 2008 р.

Нагляд та виконання (роль різних суб'єктів, зокрема наглядових органів)

«І. проти Фінляндії» (*I v. Finland*), № 20511/03, 17 липня 2008 р.
«К. У. проти Фінляндії» (*K. U. v. Finland*), № 2872/02, 02 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*) *(No. 2)* [ВП], № 40660/08 та 60641/08, 07 лютого 2012 р.

Методи спостереження

«Аллан проти Сполученого Королівства» (*Allan v. the United Kingdom*), № 48539/99, 05 листопада 2002 р
«Асоціація за європейську інтеграцію і права людини і Екімджієв проти Болгарії» (*Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*), № 62540/00, 28 червня 2007 р.
«Барбулеску проти Румунії» (*Bărbulescu v. Romania* [ВП]), № 61496/08, 05 вересня 2017 р.
«Версіні-Кампінкі та Краснянскі проти Франції» (*Versini-Campinchi and Crasnianski v. France*), № 49176/11, 16 червня 2016 р.

«Веттер проти Франції» (Vetter v. France), № 59842/00, 31 травня 2005 р.
«Вукота-Божич проти Швейцарії» (Vukota-Bojić v. Switzerland), № 61838/10, 18 жовтня 2016 р.
«D. Л. проти Болгарії» (D. L. v. Bulgaria), № 7472/14, 19 травня 2016 р.
«Драгоєвич проти Хорватії» (Dragojević v. Croatia), № 68955/11, 15 січня 2015 р.
«Карабейоглу проти Туреччини» (Karabeyolu v. Turkey), № 30083/10, 07 червня 2016 р.
«Класс та інші проти Німеччини» (Klass and Others v. Germany), № 5029/71, 06 вересня 1978 р.
«Роман Захаров проти Росії» (Roman Zakharov v. Russia) [ВП], № 47143/06, 04 грудня 2015 р.
«Ротару проти Румунії» (Rotaru v. Romania) [ВП], № 28341/95, 04 травня 2000 р.
«Сабо та Віші проти Угорщини» (Szabó and Vissy v. Hungary), № 37138/14, 12 січня 2016 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, 02 вересня 2010 р.

Відеоспостереження

«Кьопке проти Німеччини» (Köpke v. Germany), № 420/07, 05 жовтня 2010 р.
«Пек проти Сполученого Королівства» (Peck v. the United Kingdom), № 44647/98, 28 січня 2003 р.

Зразки голосу

«Вісс 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

Судова практика, пов'язана з Директивою про захист персональних даних

C-13/16, «Служба з дорожньо-транспортних пригод Поліції безпеки м. Риги проти тролейбусної компанії м. Риги» (*Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA 'Rīgas satiksme'*), 04 травня 2017.

[Принцип законної обробки: легітимний інтерес, який має третя сторона]

C-398/15, «Торгово-промислова та сільськогосподарська палата м. Лечче проти Сальваторе Манні» (*Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*), 09 березня 2017 р.

[Право на стирання персональних даних; право на заперечення проти обробки]

Об'єднані справи C-203/15 та C-698/15, «"Tele2 Sverige AB" проти Державного управління зв'язку та телекомунікації» та «Секретар внутрішніх справ проти Тома Вотсона та інших» (*Tele2 Sverige AB v. Post- och telestryrelsen and Secretary of State for the Home Department v. Tom Watson and Others*) [ВП], 21 грудня 2016 р.

[Конфіденційність електронних засобів зв'язку; провайдери послуг електронних засобів зв'язку; зобов'язання щодо загального та невибіркового зберігання даних трафіку та місцезнаходження; відсутність попереднього перегляду судом чи незалежним адміністративним органом; Хартія основних прав Європейського Союзу; сумісність з законодавством ЄС]

C-582/14, «Патрік Бреєр проти Федеративної Республіки Німеччини» (*Patrick Breyer v. Bundesrepublik Deutschland*), 19 жовтня 2016 р.

[Визначення «персональні дані»; адреси інтернет-протоколу; зберігання даних провайдером інтернет-медіапослуг; національне законодавство, яке не дозволяє брати до уваги легітимний інтерес контролера]

C-362/14, «Максиміліан Шремс проти Уповноваженого із захисту персональних даних» (*Maximilian Schrems v. Data Protection Commissioner*) [ВП], 06 жовтня 2015 р.

[Принцип законної обробки; основні права; чинність рішення «Safe Harbour»; повноваження незалежних наглядових органів]

C-230/14, «“Weltimmo s. r. o.” проти Контролюючого органу захисту даних та доступу до інформації Угорщини» (*Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*), 01 жовтня 2015 р.

[Повноваження незалежних наглядових органів]

C-201/14, «Смаранда Бара та інші проти Національного фонду медичного страхування та інших» (*Smaranda Bara and Others v. Casa Naţională de Asigurări de Sănătate and Others*), 01 жовтня 2015 р.

[Право бути поінформованим про обробку персональних даних]

C-212/13, «Франтішек Ринеш проти Офісу захисту персональних даних» (*František Ryneš v. Úřad pro ochranu osobních údajů*), 11 грудня 2014 р.

[Поняття «обробка даних» та «контролер»]

C-473/12, «Професійний інститут агентів з нерухомості (IPI) проти Джеффрі Енглберта та інших» (*Institut professionnel des agents immobiliers (IPI) v. Geoffrey Englebert and Others*), 07 листопада 2013 р.

[Право бути поінформованим про обробку персональних даних]

T-462/12 R, «“Pilkington Group Ltd” проти Європейської Комісії» (*Pilkington Group Ltd v. European Commission*), Наказ голови Загального суду, 11 березня 2013

C-342/12, «“Worten – Home Equipment SA” проти Контролюючого органу з дотримання умов праці» (*Worten – Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT)*, 30 травня 2013 р.

[Поняття «персональні дані»; облік робочого часу; принципи стосовно якості даних і критеріїв законності обробки даних; доступ національних органів, відповідальних за перевірку трудових умов; зобов’язання роботодавця надавати доступ до обліку робочого часу для невідкладного ознайомлення]

Об’єднані справи C-293/12 та C-594/12, «“Digital Rights Ireland Ltd.” проти Міністра зв’язку, морських та природних ресурсів та інших та Земельний уряд Каринтії та інші» (*Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*) [ВП], 08 квітня 2014 р.

[Порушення первинного законодавства ЄС Директивою про зберігання даних; законна обробка; обмеження мети та зберігання]

C-288/12, «Європейська Комісія проти Угорщини» (*European Commission v. Hungary*) [ВП], 08 квітня 2014 р.

[Законність звільнення з посади працівника офісу національного інспектора із захисту даних]

Об'єднані справи C-141/12 та C-372/12, «YS проти Міністра з питань імміграції, інтеграції та притулку» та «Міністр з питань імміграції, інтеграції та притулку проти M. та S.» (*YS v. Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v. M and S*), 17 липня 2014 р.

[Обсяг права суб'єкта даних на доступ; захист фізичних осіб щодо обробки персональних даних; поняття «персональні дані»; дані, що стосуються отримання посвідки на проживання, та правовий аналіз, що міститься в адміністративному документі, складеному до прийняття рішення; Хартія основних прав Європейського Союзу]

C-131/12, «"Google Spain SL", "Google Inc." проти Іспанського агентства захисту даних (AEPD) та Маріо Костеха Гонсалеса» (*Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*) [ВП], 13 травня 2014 р.

[Зобов'язання пошукових провайдерів за запитом суб'єкта даних утримуватися від демонстрації персональних даних у результатах пошуку; застосовність Директиви про захист персональних даних; поняття «обробка даних»; зміст поняття «контролери»; збалансування захисту персональних даних зі свободою вираження поглядів; право бути забутим]

C-614/10, «Європейська Комісія проти Республіки Австрії» (*European Commission v. Republic of Austria*) [ВП], 16 жовтня 2012 р.

[Незалежність національного наглядового органу]

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*), 24 листопада 2011 р.

[Правильна імплементація статті 7 (f) Директиви про захист персональних даних – «легітимний інтерес інших осіб» – у національному законодавстві]

C-360/10, «Бельгійська асоціація авторів, композиторів та видавців CVBA (SABAM) проти "Netlog NV"» (*Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v. Netlog NV*), 16 лютого 2012 р.

[Зобов'язання постачальників соціальних мереж запобігати незаконному використанню музичних та авдіовізуальних творів користувачами мережі]

C-70/10, «“Scarlet Extended SA” проти Бельгійської асоціації авторів, композиторів та видавців (SABAM)» (*Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 листопада 2011 р.

[Інформаційне суспільство; авторські права; інтернет; «піринговe» («одноранговe») програмне забезпечення; інтернет-провайдери; встановлення системи фільтрації електронних комунікацій для запобігання обміну файлами, що порушує авторські права; відсутність загального обов’язку відстежувати передану інформацію]

C-543/09, «“Deutsche Telekom” проти Федеративної Республіки Німеччини» (*Deutsche Telekom AG v. Bundesrepublik Deutschland*), 05 травня 2011 р.

[Необхідність поновлення згоди]

Об’єднані справи C-92/09 та C-93/09, «“Volker und Markus Schecke GbR” та Хартмут Ейферт проти землі Гессен» (*Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*) [ВП], 09 листопада 2010 р.

[Поняття «персональні дані»; пропорційність правового зобов’язання публікувати персональні дані бенефіціарів певних сільськогосподарських фондів ЄС]

C-553/07, «Мер та члени міської ради Роттердама проти М.Е.Е. Рейкебура» (*College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer*), 07 травня 2009 р.

[Право суб’єкта даних на доступ]

C-518/07, «Європейська Комісія проти Федеративної Республіки Німеччини» (*European Commission v. Federal Republic of Germany*) [ВП], 09 березня 2010 р.

[Незалежність національного наглядового органу]

C-73/07, «Уповноважений із захисту персональних даних Фінляндії проти “Satakunnan Markkinapörssi Oy” і “Satamedia Oy”» (*Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*) [ВП], 16 грудня 2008 р.

[Концепція «журналістської діяльності» за змістом статті 9 Директиви про захист персональних даних]

C-524/06, «Гайнц Губер проти Федеративної Республіки Німеччини» (*Heinz Huber v. Bundesrepublik Deutschland*) [ВП], 16 грудня 2008 р.

[Законність зберігання даних про іноземців у статистичних реєстрах]

C-275/06, «Музичні продюсери Іспанії (Promusicae) проти "Telefonica de Espana SAU"» (*Productores de Música de España (Promusicae) v. Telefónica de España SAU*) [ВП], 29 січня 2008 р.

[Поняття «персональні дані»; обов'язок постачальників доступу до інтернету розкривати Асоціації захисту інтелектуальної власності особистість користувачів системи обміну файлами «KaZaA»]

C-101/01, Кримінальне провадження проти Bodil Lindqvist (*Criminal proceedings against Bodil Lindqvist*), 06 листопада 2003 р.

[Спеціальні категорії персональних даних]

Об'єднані справи C-465/00, C-138/01 та C-139/01, «Рахункова палата проти австрійської телерадіокомпанії "Österreichischer Rundfunk" та інших» та «Кріста Нойкомм і Джозеф Лауерманн проти австрійської телерадіокомпанії "Österreichischer Rundfunk"» (*Rechnungshof v. Österreichischer Rundfunk and Others and Christa Neukomm and Jospeh Lauermann v. Österreichischer Rundfunk*), 20 травня 2003 р.

[Пропорційність правового зобов'язання публікувати персональні дані про зарплати службовців певних категорій установ державного сектору]

C-434/16, «Пітер Новак проти Комісара із захисту персональних даних» (*Peter Nowak v. Data Protection Commissioner*), Думка Генерального адвоката Кокотта, 20 липня 2017 р.

[Поняття персональних даних; доступ до власних результатів екзамену; виправлення екзаменатора]

C-291/12, «Міхаель Шварц проти міста Бохума» (*Michael Schwarz v. Stadt Bochum*), 17 жовтня 2013 р.

[Посилання на преюдиційне рішення; простір свободи, безпеки та справедливості; біометричний паспорт; відбитки пальців; правова підстава; пропорційність]

Судова практика, пов'язана з Директивою 2016/681

Висновок 1/15 Суду (Велика Палата), 26 липень 2017 р.

[Правова підстава; проєкт угоди між Канадою та Європейський Союзом про передачу та обробку даних Записів реєстрації пасажирів; сумісність проєкту угоди зі статтею 16 ДФЄС та статтями 7 та 8, а також 52 (1) Хартії основних прав Європейського Союзу]

Судова практика, пов'язана з Регламентом захисту персональних даних інституціями ЄС

C-615/13 P, «"ClientEarth" та "PAN Europe" проти Європейського агентства безпечності харчових продуктів» (*ClientEarth, Pesticide Action Network Europe (PAN Europe) v. European Food Safety Authority (EFSA), European Commission*), 16 липня 2015 р.

[Доступ до документів]

C-28/08 P, «Європейська Комісія проти "The Bavarian Lager Co. Ltd"» (*European Commission v. The Bavarian Lager Co. Ltd.)* [ВП], 29 червня 2010 р.

[Доступ до документів]

Судова практика, пов'язана з Директивою 2002/58/ЕС

C-536/15, «"Tele2 (Netherlands) BV" та інші проти Управління споживачів та ринку (УСР)» (*Tele2 (Netherlands) BV and Others v. Autoriteit Consument en Markt (AMC)*), 15 березня 2017 р.

[Принцип недискримінації; розкриття персональних даних стосовно абонентів з метою забезпечення загальнодоступних довідкових служб та каталогів; абонентська згода; особливості щодо держави-члена, в якій забезпечуються загальнодоступні довідкові служби та каталоги]

Об'єднані справи C-203/15 та C-698/15, «"Tele2 Sverige AB" проти Державного управління зв'язку та телекомунікації» та «Секретар внутрішніх справ проти Тома Вотсона та інших» (*Tele2 Sverige AB v. Post- och telestryrelsen and Secretary of State for the Home Department v. Tom Watson and Others*) [ВП], 21 грудня 2016 р.

[Конфіденційність засобів електронного зв'язку; провайдери послуг електронного зв'язку; обов'язок, що стосується загального та невибіркового зберігання даних трафіку та місцезнаходження; відсутність попереднього перегляду судом чи незалежним адміністративним органом; Хартія основних прав Європейського Союзу; сумісність з правом ЄС]

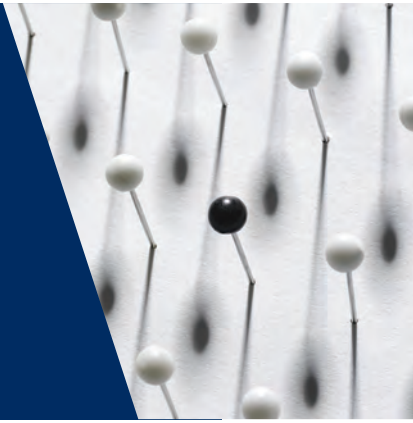
C-70/10, «"Scarlet Extended SA" проти Бельгійської асоціації авторів, композиторів та видавців (SABAM)» (*Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*), 24 листопада 2011 р.

[Інформаційне суспільство; авторські права; інтернет; «піринговe» («одноранговe») програмне забезпечення; інтернет-провайдери; встановлення системи фільтрації електронних комунікацій для запобігання обміну

файлами, що порушує авторські права; відсутність загального обов'язку відстежувати передану інформацію]

C-461/10, «"*Bonnier Audio AB" та інші проти "Perfect Communication Sweden AB"*» (*Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v. Perfect Communication Sweden AB*), 19 квітня 2012 р.

[Авторське право та суміжні права; обробка даних інтернетом; порушення виняткового права; аудіокниги, до яких надається доступ в інтернеті через FTP-сервер за IP-адресою, наданою інтернет-провайдером; припис щодо надання провайдером імені та адреси користувача IP-адреси]



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., 2020. — 432 с.

ISBN 978-617-684-261-3

Переклад Вадима Кастеллі.

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

EDPS

Швидкий розвиток інформаційних технологій посилив потребу в надійному захисті персональних даних, право на який гарантують документи Європейського Союзу (ЄС) і Ради Європи (РЄ). Забезпечення цього важливого права пов'язане з новими серйозними викликами, оскільки технологічний прогрес розширює межі таких сфер, як, наприклад, спостереження, перехоплення комунікацій і зберігання даних. Цей посібник призначений для ознайомлення юристів-практиків, які не спеціалізуються у сфері захисту персональних даних, з цією новою сферою права. Тут надається загальна інформація щодо застосовних нормативно-правових актів ЄС і РЄ. Також наводяться приклади ключової судової практики з посиланнями на важливі рішення як Суду Європейського Союзу, так і Європейського суду з прав людини. У посібнику також представлені гіпотетичні ситуації, які слугують практичною ілюстрацією різноманітних питань, що виникають у цій сфері, яка постійно розвивається.

АГЕНЦІЯ ЄВРОПЕЙСЬКОГО СОЮЗУ З ПИТАНЬ ОСНОВОПОЛОЖНИХ ПРАВ
Шварценбергплац, 11 - 1040 Відень - Австрія
Тел. +43 (1) 580 30-0 - Факс +43 (1) 580 30-699
fra.europa.eu - info@fra.europa.eu - @EURightsAgency

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 - @ECHRPublication

ЄВРОПЕЙСЬКИЙ ІНСПЕКТОР ІЗ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ
Вулиця Верц, 60 – 1047 Брюсель – Бельгія
Тел. +32 2 283 19 00
www.edps.europa.eu – edps@edps.europa.eu – logo@EU_EDPS

Publications Office

ISBN 978-92-871-9849-5 (CoE)
ISBN 978-92-9491-901-4 (FRA)

ISBN 978-617-684-261-3