



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

Посібник із судової практики
Європейського суду
з прав людини

Захист даних

Оновлено 31 серпня 2024 року

Підготовлено Секретаріатом Суду. Не покладає зобов'язань на Суд.

Видавців або організацій, які бажають перекласти та/або відтворити цей Посібник повністю або частково у формі друкованої чи електронної публікації, просимо заповнити форму зворотного зв'язку: [«запит відтворення або повторної публікації перекладу»](#) для отримання інформації щодо процедури авторизації.

Якщо ви бажаєте дізнатися, який Посібник із судової практики знаходиться наразі на етапі перекладу, див. перелік [очікуваних перекладів](#).

Цей Посібник спочатку було укладено французькою мовою. Він регулярно оновлюється, дата останнього оновлення: 31 серпня 2024 року. До нього можуть бути внесені редакційні виправлення.

Посібники з судової практики можна завантажити за посиланням <https://ks.echr.coe.int>. Оновлення публікації відстежуйте на сторінці Суду у Твіттері за посиланням: https://twitter.com/ECHR_CEDH.

Цей переклад опубліковано за домовленістю з Радою Європи, Європейським судом з прав людини та Верховним Судом (Україна) і виконано бюро перекладів «Профпереклад».

© Рада Європи / Європейський суд з прав людини, 2025

Зміст

Зміст	3
Передмова	6
Вступ	7
I. Основні визначення та принципи захисту даних	7
A. Термінологія у сфері захисту даних.....	7
1. Поняття персональних даних та його обсяг	7
2. Конкретні категорії даних.....	12
a. Так звані «конфіденційні» категорії.....	12
i. Дані, що розкривають расове чи етнічне походження.....	12
ii. Дані, що розкривають політичні погляди, релігійні або інші переконання, включно з філософськими	13
iii. Дані про членство в профспілці	13
iv. Генетичні та біометричні дані	14
v. Дані про здоров'я, сексуальне життя та сексуальну орієнтацію.....	15
vi. Дані про кримінальні правопорушення та засудження.....	17
b. Інші категорії даних.....	18
i. Дані про зайнятість	18
ii. Фінансові дані.....	18
iii. Дані трафіку	19
iv. Зразки голосу.....	21
v. Дані про місцезнаходження за допомогою GPS	21
vi. Фотографії.....	22
B. Два аспекти (негативний і позитивний) захисту даних	25
C. Триступневий тест захисту даних.....	29
1. Чи було втручання законним	29
2. Чи переслідувало втручання законну мету.....	33
3. Чи було втручання «необхідним у демократичному суспільстві»	34
a. Вимога мінімізації обсягу зібраних або записаних даних	35
b. Вимога точності та оновлення даних	35
c. Вимога зберігати дані не довше, ніж це необхідно для досягнення мети, з якою вони були зафіксовані	36
d. Вимога обмеження використання даних метою, для якої вони були зафіксовані	37
e. Вимога прозорості процедур обробки даних.....	38
II. Захист даних та право на повагу до приватного життя (стаття 8 Конвенції)	38
A. Операції з даними, що можуть порушувати право на повагу до приватного життя.....	39
1. Збирання персональних даних	39
a. Збирання даних органами влади за допомогою прихованого спостереження	39
i. Прослуховування та реєстрація телефонних дзвінків.....	39
ii. Перехоплення повідомлень пейджера.....	41
iii. Аудіо- та відеоспостереження	41
iv. Геолокація транспортного засобу за допомогою GPS	43

v. Стеження приватними детективами	43
vi. Моніторинг кореспонденції	43
vii. Негласне спостереження, шпигунство і операції з масового спостереження.....	44
b. Збирання даних роботодавцями на робочому місці.....	45
c. Збирання даних для використання як доказів у судових справах	48
i. Обшуки та вилучення.....	48
ii. Примусові медичні дії для отримання клітинних зразків.....	52
d. Збір персональних даних у медичному контексті.....	53
e. Примусова передача персональних даних.....	54
2. Зберігання персональних даних	55
a. Зберігання персональних даних з метою боротьби зі злочинністю	56
i. Безсистемний і недиференційований характер збережених даних	57
ii. Строк зберігання даних	58
iii. Гарантії щодо знищення або видалення збережених даних	61
iv. Гарантії, спрямовані на регулювання доступу третіх осіб і захист цілісності та конфіденційності даних.....	62
b. Зберігання персональних даних у медичному контексті	63
c. Зберігання персональних даних в інтернеті для журналістських цілей	64
3. Розголошення персональних даних	64
a. Вплив попередньої згоди	65
b. Розголошення даних в контексті судового провадження	67
c. Розголошення даних з метою захисту здоров'я населення	70
d. Розголошення даних з метою захисту національної безпеки.....	71
e. Розголошення даних з метою захисту економічного добробуту країни.....	72
f. Масове розголошення персональних даних.....	73
V. Права суб'єктів даних.....	73
1. Право на доступ до власних даних.....	73
2. Право на виправлення.....	77
3. Право на видалення даних.....	78
a. «Право на забуття»	79
b. Інші контексти	82
4. Право на особливі процесуальні гарантії та ефективні процесуальні норми для захисту своїх прав	83

III. Взаємодія з іншими положеннями Конвенції та Протоколами до неї..... 87

A. Захист даних і матеріальні права.....	88
1. Захист даних і свобода думки, совісті та релігії (стаття 9 Конвенції)	89
2. Захист даних і свобода вираження поглядів (стаття 10 Конвенції).....	90
3. Захист даних і заборона дискримінації (стаття 14 Конвенції)	94
4. Захист даних і право на мирне володіння майном (Стаття 1 Першого протоколу)	95
5. Захист даних і свобода пересування (стаття 2 Протоколу № 4).....	96
B. Захист даних і процесуальні права	97
1. Право на справедливий суд (стаття 6 Конвенції)	97
a. Загальні гарантії (пункт 1 статті 6 Конвенції).....	97
i. Рівність сторін і дотримання принципу змагальності у провадженнях, що стосуються конфіденційної або секретної інформації	98
ii. Вмотивованість судових рішень і захист даних.....	98

iii. Використання як доказів персональних даних, зібраних незаконно або з порушенням статті 8.....	99
iv. Публічний судовий розгляд та публічне проголошення судового рішення і секретність даних	100
v. Тривалість судових проваджень щодо захисту даних	100
b. Конкретні гарантії (пункти 2 і 3 статті 6 Конвенції).....	101
i. Захист даних і право на презумпцію невинуватості (пункт 2 статті 6 Конвенції)	101
ii. Захист даних і право на захист (підпункт «b» пункту 3 статті 6 Конвенції).....	102
2. Право на ефективний засіб юридичного захисту (стаття 13 Конвенції)	102
3. Право на свободу та особисту недоторканність (стаття 5 Конвенції)	105
IV. Сучасні виклики захисту даних	106
A. Технологічний прогрес, алгоритми та штучний інтелект.....	106
B. Інтернет та пошукові системи	108
C. Передача даних і потоки даних	109
Перелік цитованих справ	111

Передмова

Цей Посібник входить до низки Посібників із судової практики, опублікованих Європейським судом з прав людини (надалі — «Суд», «Європейський суд» або «Страсбурзький суд»), для інформування практикуючих юристів про основоположні рішення та ухвали, постановлені Страсбурзьким судом. У цьому конкретному Посібнику аналізується та узагальнюється судова практика щодо різних статей Європейської конвенції з прав людини (надалі — «Конвенція» або «Європейська конвенція»), що стосуються захисту даних. Його слід читати разом з посібниками із судової практики за статтею, на яку він містить систематичні посилання.

Цитована судова практика була відібрана серед провідних, найбільш важливих та/або недавніх рішень та ухвал *.

Рішення та ухвали Суду слугують не лише для того, щоб вирішувати справи, передані на розгляд Суду, а й загалом для роз'яснення, захисту та розвитку норм, встановлених Конвенцією, сприяючи тим самим дотриманню Державами зобов'язань, взятих ними як Договірними Сторонами (*«Ірландія проти Сполученого Королівства» (Ireland v. the United Kingdom)*), 18 січня 1978 року, § 154, серія А № 25, і нещодавно — *«Єронович проти Латвії» (Jeronovičs v. Latvia)* [ВП], № 44898/10, § 109, 05 липня 2016 року).

Відповідно, місія створеної Конвенцією системи полягає в тому, щоб визначити, в інтересах суспільства, питання державної політики, тим самим підвищуючи стандарти захисту прав людини та поширюючи судову практику у сфері прав людини серед усього співтовариства Держав-учасниць Конвенції (*«Константін Маркін проти Росії» (Konstantin Markin v. Russia)*) [ВП], № 30078/06, § 89, ЄСПЛ 2012). Дійсно, Суд підкреслив роль Конвенції як «конституційного інструмента європейського громадського порядку» у сфері прав людини (*«Босфорус Гава Йолларі Турізм ве Тікарет Анонім Шіркети проти Ірландії» (Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi v. Ireland)* [ВП], № 45036/98, § 156, ЄСПЛ 2005-VI, і нещодавно — *«Н.Д. та Н.Т. проти Іспанії» (N.D. and N.T. v. Spain)* [ВП], №№ 8675/15 та 8697/15, § 110, 13 лютого 2020 року).

Протокол № 15 до Конвенції нещодавно включив принцип субсидіарності до Преамбули Конвенції. Цей принцип «покладає спільну відповідальність на Держави-учасниці та Суд» щодо захисту прав людини, і національні органи влади та суди повинні тлумачити й застосовувати національне законодавство таким чином, щоб забезпечити повну реалізацію прав і свобод, визначених у Конвенції та Протоколах до неї (*«Гженда проти Польщі» (Grzęda v. Poland)* [ВП], § 324).

* Цитована судова практика може бути викладена однією або обома офіційними мовами (англійською та французькою) Суду та Європейської комісії з прав людини. Якщо не вказано інше, усі посилання стосуються рішення по суті справи, що була винесена Палатою Суду. Скорочення «(ухв.)» вказує на те, що наводиться цитата з ухвали Суду, а аббревіатура «[ВП]» — на те, що справа розглядалася Великою Палатою. Рішення Палати, які не були остаточними на момент публікації цього оновлення, позначено зірочкою (*).

Вступ

1. Технологічний прогрес призвів до якісного стрибка у сфері спостереження, перехоплення комунікацій та збереження даних, що і собі спричинило серйозні виклики у сфері захисту персональних даних. З часу винесення рішення у справі *«Леандер проти Швеції» (Leander v. Sweden)* 1987 року, в якому «старий» Суд вперше проаналізував питання щодо зберігання державним органом персональних даних фізичної особи, практика органів Конвенції у цій сфері зазнала значного розвитку.

2. За роки своєї діяльності Суд розглянув багато ситуацій, в яких порушувалися питання, пов'язані із захистом персональних даних. Тепер практика органів Конвенції охоплює широкий спектр операцій, пов'язаних із персональними даними, як-от збір, зберігання, використання та поширення таких даних, і вона буде детально описана у цьому посібнику. Ця практика розвивалася відповідно до швидкого розвитку інформаційно-комунікаційних технологій.

I. Основні визначення та принципи захисту даних

3. Право на захист персональних даних не є автономним правом серед різних прав і свобод, передбачених Конвенцією. Однак, Суд визнав, що захист персональних даних має основоположне значення для здійснення особою права на повагу до приватного і сімейного життя, житла і кореспонденції, гарантованого статтею 8 Конвенції (*«Сатакуннан Марккінапорссі Ой та Сатамедіа Ой проти Фінляндії» (Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland)* [ВП], 2017, § 137; *«Z проти Фінляндії» (Z v. Finland)*, 1997, § 95; *«Л.Б. проти Угорщини» (L.B. v. Hungary)* [ВП], 2023, § 103). Ця стаття є основним механізмом, за допомогою якого здійснюється захист персональних даних у системі Конвенції, хоча міркування, пов'язані із цим захистом, також набувають значення й за іншими положеннями Конвенції та Протоколами до неї.

A. Термінологія у сфері захисту даних

4. Розвиток технологій призвів до збільшення кількості операцій із персональними даними, які можуть становити «автоматизовану обробку». Незважаючи на широкий підхід Суду до визначення поняття «приватне життя», що дозволив йому створити судову практику відповідно до розвитку суспільства, певна операція з обробки даних не обов'язково підпадає під дію статті 8 або автоматично порушує інтереси, захищені цією статтею.

1. Поняття персональних даних та його обсяг

5. У своїх рішеннях Суд роз'яснює поняття «персональні дані», посилаючись на [Конвенцію Ради Європи № 108 про захист осіб у зв'язку з автоматизованою обробкою персональних даних](#) від 28 січня 1981 року, яка набрала чинності у 1985 році та була оновлена у 2018 році (*«Конвенція 108»*). Її мета — «забезпечення на території кожної Сторони для кожної особи... дотримання її прав та основоположних свобод, і зокрема її права на недоторканість приватного життя у зв'язку з автоматизованою обробкою персональних даних, які її стосуються» (стаття 1) (*«Аманн проти Швейцарії» (Amann v. Switzerland)* [ВП], 2000, § 65; *«Гараламбіє проти Румунії» (Haralambie v. Romania)*, 2009, § 77). Суд чітко вказав, що відповідно до статті 2 [Конвенції 108](#) поняття «персональні дані» визначається як «будь-яка інформація, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною» (*«Аманн проти Швейцарії» (Amann v. Switzerland)* [ВП], 2000, § 65; *«Гараламбіє проти Румунії» (Haralambie v. Romania)*, 2009, § 77).

6. Такі дані охоплюють не лише інформацію, що безпосередньо ідентифікує фізичну особу («суб'єкта даних»), таку як прізвище та ім'я («*Гійо проти Франції*» (*Guillot v. France*), 1996, §§ 21-22; «*Ментзен проти Латвії*» (*Mentzen v. Latvia*) (ухв.), 2004; «*Гюзель Ердагьоз проти Туреччини*» (*Güzel Erdagöz v. Turkey*), 2008, § 43; «*Гарнага проти України*» (*Garnaga v. Ukraine*), 2013, § 36; «*Генрі Кісмун проти Франції*» (*Henry Kismoun v. France*), 2013, § 25; «*Гайовський проти Словаччини*» (*Hájovský v. Slovakia*), 2021, §§ 11-12 і 41), а й будь-який елемент, що опосередковано визначає особу, наприклад, динамічна IP-адреса («*Бенедік проти Словенії*» (*Benedik v. Slovenia*), 2018, §§ 107-108).

7. Хоча питання захисту персональних даних здебільшого стосується фізичних осіб та їхнього права на повагу до приватного життя, передбаченого статтею 8, юридичні особи також вправі посилалися на це право в Суді, якщо їх безпосередньо зачіпає захід, який порушує їхнє право на повагу до «кореспонденції» або «житла». Так було, наприклад, у справі, коли компанію зобов'язали надати копію всіх даних на сервері, який використовувався спільно з іншими компаніями («*Берн Ларсен Голдинг АС та інші проти Норвегії*» (*Bernh Larsen Holding AS and Others v. Norway*), 2013, § 106), або коли Міністерство оборони на підставі ордеру перехопило комунікації неурядової організації (НУО), що захищають громадянські свободи («*Ліберті та інші проти Сполученого Королівства*» (*Liberty and Others v. the United Kingdom*), 2008, §§ 56-57). Однак у справі, що стосувалася заходів, пов'язаних із захистом персональних даних членів релігійної організації та повагою до їхнього «приватного життя», організація не зазнала прямого впливу, а отже, не була «потерпілою» у розумінні статті 34 Конвенції («*Авілкіна та інші проти Росії*» (*Avilkina and Others v. Russia*), 2013, § 59).

8. Персональні дані можуть приймати дуже різні форми. Наприклад:

- Інформація про абонентів інтернету, пов'язана з конкретними динамічними IP-адресами, присвоєними в певний час («*Бенедік проти Словенії*» (*Benedik v. Slovenia*), 2018, §§ 108-109).
- Записи, зроблені для використання як зразки голосу, що мають постійний характер і підлягають аналізу, безпосередньо пов'язаному з визначенням особи в контексті інших персональних даних («*П.Г. і Дж.Г. проти Сполученого Королівства*» (*P.G. and J.H. v. the United Kingdom*), 2001, § 59).
- Зразки клітин і профілі ДНК («*С. і Марпер проти Сполученого Королівства*» (*S. and Marper v. the United Kingdom*) [ВП], 2008, §§ 70-77) або відбитки пальців (*там само*, § 84), які, попри об'єктивний і неспростовний характер, містили унікальну інформацію про відповідну особу й дозволяли її точну ідентифікацію в широкому діапазоні обставин (*там само*, § 85).
- Інформація про конкретну особу, отримана з банківських документів, незалежно від того, чи стосується вона конфіденційних даних або професійної діяльності («*М.Н. та інші проти Сан-Маріно*» (*M.N. and Others v. San Marino*), 2015, §§ 51 і далі).
- Дані про рід занять конкретно визначеної особи або особи, яку можна конкретно визначити, зібрані та збережені поліцією («*Хелілі проти Швейцарії*» (*Khelili v. Switzerland*), 2011, § 56).
- Дані про використання інтернету та обміну повідомленнями (Yahoo) працівником на робочому місці, отримані за допомогою спостереження («*Барбулеску проти Румунії*» (*Bărbulescu v. Romania*) [ВП], 2017, §§ 18, 74-81).
- Копія електронних даних, вилучених у юридичної фірми, навіть якщо вони не були розшифровані, транскрибовані або офіційно приписані їхнім власникам («*Кірдьок та інші проти Туреччини*» (*Kirdök and Others v. Turkey*), 2019, § 36).
- Дані, зібрані в контексті негласного відеоспостереження в університеті («*Антовиц і Мірковиц проти Чорногорії*» (*Antović and Mirković v. Montenegro*), 2017, §§ 44-45).

- Інформація про оподатковуваний дохід та активи великої кількості осіб, попри те, що громадськість могла отримати доступ до таких даних за певних умов («*Сатакуннан Марккінапорссі Ой та Сатамедіа Ой проти Фінляндії*» (*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*) [ВП], 2017, § 138).
- Дані про народження та відмову від фізичної особи, включаючи інформацію, необхідну для встановлення істини про важливий аспект особистої ідентичності («*Гаскін проти Сполученого Королівства*» (*Gaskin v. the United Kingdom*), 1989, § 39; «*Мікуліч проти Хорватії*» (*Mikulić v. Croatia*), 2002, §§ 54-64; «*Одієвре проти Франції*» (*Odièvre v. France*) [ВП], 2003, §§ 28-29; «*Говен-Фурні і Сілію проти Франції*» (*Gauvin-Fournis and Silliau v. France*), 2023, §§ 106 і 112; «*Шерр'єр проти Франції*» (*Cherrier v. France*), 2024, § 50).
- Дані, включені до угоди про розлучення, що містять деталі щодо розподілу спільного майна подружжя, опіки та проживання неповнолітніх дітей, угоди про аліменти та огляд активів / доходів заявника («*Лібшер проти Австрії*» (*Liebscher v. Austria*), 2021, §§ 31 і 68).
- Відеозаписи розмов, зроблені за допомогою прихованої камери особою в професійному контексті, які згодом були використані в кримінальному провадженні проти заявника («*Сарбу проти Румунії*» (*Sârbu v. Romania*), 2023, §§ 39-41).

9. Відповідно до статті 2 Конвенції 108 «обробка даних» включає «будь-яку операцію або сукупність операцій, здійснюваних над персональними даними, таких як збирання, зберігання, збереження, зміна, витяг, розголошення, надання доступу, стирання, знищення або проведення логічних та/або арифметичних операцій над такими даними». Розвиток технологій призвів до збільшення кількості операцій із персональними даними, які можуть становити обробку. Суд визначив такі типові приклади:

- Збір поліцією в інтернет-провайдера інформації про абонентів, пов'язаної з конкретною динамічною IP-адресою особи («*Бенедік проти Словенії*» (*Benedik v. Slovenia*), 2018, §§ 108-109).
- Факт збору та зберігання публічної інформації про особу, наприклад, про її політичну діяльність («*Ротару проти Румунії*» (*Rotaru v. Romania*) [ВП], 2000, §§ 43-44; «*Асоціація «21 грудня 1989» та інші проти Румунії*» (*Association "21 December 1989" and Others v. Romania*), 2011, §§ 167-168; («*Аманн проти Швейцарії*» (*Amann v. Switzerland*) [ВП], 2000, § 65-67; «*Кетт проти Сполученого Королівства*» (*Catt v. the United Kingdom*), 2019, § 93).
- Внесення особи до внутрішньої судової бази даних відповідного міністерства («*Л.Ф. проти Франції*» (*L.F. v. France*) (ухв.), 2024, § 30); до національної судової бази даних сексуальних злочинців («*Гардель проти Франції*» (*Gardel v. France*), 2009, § 58); або до національної бази даних щодо будь-якого кримінального провадження, порушеного проти особи («*Н.Ф. та інші проти Росії*» (*N.F. and Others v. Russia*), 2023, §§ 34 і 49), а також збір та зберігання відбитків пальців підозрюваного («*М.К. проти Франції*» (*M.K. v. France*), 2013, § 29)
- Негласний запис зразків голосу у поліцейській дільниці для постійного зберігання, які будуть використані для ідентифікації відповідних осіб шляхом аналізу в контексті інших персональних даних («*П.Г. і Дж.Г. проти Сполученого Королівства*» (*P.G. and J.H. v. the United Kingdom*), 2001, §§ 59-60).
- Зйомка особи в кімнаті для допитів у поліції камерами, встановленими з міркувань безпеки і повністю видимими, з постійним записом відзнятого матеріалу і включенням його в монтаж для подальшого використання («*Перрі проти Сполученого Королівства*» (*Perry v. the United Kingdom*), 2003, § 41).

- Систематичний збір та зберігання даних GPS-моніторингу, що вказують на місцезнаходження та публічні пересування суб'єкта (*«Узун проти Німеччини» (Uzun v. Germany)*, 2010, §§ 49-53).
- Публікація в журналі статті, проілюстрованої фотографіями знаменитостей, зробленими без їхнього відома (*«Фон Ганновер проти Німеччини» (№ 2) (Von Hannover v. Germany (no. 2))* [ВП], 2012, §§ 95-99).
- Запис і оприлюднення в засобах масової інформації відеозаписів з камер відеоспостереження, на яких особа намагається вчинити самогубство в громадському місці (*«Пек проти Сполученого Королівства» (Peck v. the United Kingdom)*, 2003, §§ 59-63).
- Запис і зберігання поліцією даних про передбачуваний рід занять особи (*«Хелілі проти Швейцарії» (Khelili v. Switzerland)*, 2011, § 56).
- Розголошення психіатричною лікарнею журналістам дуже чутливої конфіденційної інформації про приватне життя пацієнта (*«Моккуте проти Литви» (Mockutė v. Lithuania)*, 2018, § 99).
- Збір Державою в рамках антидопінгових заходів у спорті інформації про місцезнаходження та щоденні заняття, навіть у вихідні дні, спортсменів високого рівня (*«Національна федерація асоціацій і спілок спортсменів та інші проти Франції» (National Federation of Sportspersons' Associations and Unions (FNASS) and Others v. France)*, 2018, §§ 155-159).
- Систематичне сканування та завантаження приватної кореспонденції ув'язнених, як вхідної, так і вихідної, на сервер Національної судової мережі (*«Нух Узун та інші проти Туреччини» (Nuh Uzun and Others v. Turkey)*, 2022, §§ 80-82).
- Використання технології розпізнавання обличчя для того, щоб, по-перше, ідентифікувати заявника, який проводив одиночну демонстрацію без попереднього повідомлення, за фотографіями та відео, опублікованими на каналі Телеграм, і, по-друге, знайти та заарештувати його під час поїздки в метро (*«Глухін проти Росії» (Glukhin v. Russia)*, 2023, § 73).

10. Такі заходи майже завжди розглядаються Судом як втручання, з різним ступенем серйозності, у право на повагу до приватного життя, житла чи кореспонденції суб'єктів даних.

11. Однак не всі операції з персональними даними підпадають під дію статті 8 або автоматично порушують відповідні права. Наприклад, у справі *«Мехмедович проти Швейцарії» (Mehmedovic v. Switzerland)* (ухв.), 2018 (§ 18), Суд дійшов висновку, що розрізнена інформація про заявницю, яка була зібрана випадково і не мала відношення до розслідування, не становила систематичного або постійного збору даних, і тому не порушувала її право на повагу до приватного життя. Ба більше, у справі *«Какісісой та інші проти Кіпру» (Cakicisoy and Others v. Cyprus)* (ухв.), 2014, §§ 50-52, той факт, що органи влади взяли зразки крові у заявників для отримання їхнього ДНК-профілю в рамках програми ексгумації з метою ідентифікації останків їхніх померлих родичів, а зразки були знищені після закінчення строку дії згоди, не був визнаний втручанням у право заявників на повагу до їхнього приватного життя.

12. З практики Суду видно, що операції з персональними даними підпадають під дію статті 8, якщо інформація була зібрана про конкретну особу (*«Аманн проти Швейцарії» (Amann v. Switzerland)* [ВП], 2000, § 66-67; *«Ротару проти Румунії» (Rotaru v. Romania)* [ВП], 2000, §§ 43-44); якщо дані були предметом систематичного або постійного запису (*«Узун проти Німеччини» (Uzun v. Germany)*, 2010, § 51), або якщо їх використовували для аналізу, спрямованого на ідентифікацію особи на основі інших персональних даних (*«П.Г. і Дж.Г. проти Сполученого Королівства» (P.G. and J.H. v. the United Kingdom)*, 2001, § 57), або якщо дані були оприлюднені у спосіб або в обсязі, що перевищує обґрунтовані очікування суб'єкта (*«Пек проти Сполученого Королівства» (Peck v. the United Kingdom)*, 2003, §§ 58-59); *«Пеппі проти*

Сполученого Королівства» (Perry v. the United Kingdom), 2003, § 38). Іншими важливими аспектами є контекст, у якому була записана і збережена інформація, характер записів, спосіб використання цих записів, а також результати, які можуть бути отримані («*С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom)* [ВП], 2008, § 67).

13. Важливим, хоча й не завжди вирішальним елементом, є те, чи мала особа обґрунтоване очікування захисту свого приватного життя («*Перрі проти Сполученого Королівства» (Perry v. the United Kingdom)*, 2003, § 37); «*Барбулеску проти Румунії» (Bărbulescu v. Romania)* [ВП], 2017, §80; «*Глухін проти Росії» (Glukhin v. Russia)*, 2023, § 66). Щодо діяльності в інтернеті, анонімність особистої інформації стає ключовим фактором у цій оцінці. Той факт, що абонент інтернет-провайдера не приховав свою динамічну IP-адресу, не є вирішальним у визначенні того, чи були його очікування на захист приватного життя обґрунтованими («*Бенедік проти Словенії» (Benedik v. Slovenia)*, 2018, § 116). На робочому місці інструкції роботодавця не можуть звести приватне соціальне життя на робочому місці до нуля. Повага до приватного життя та таємниці кореспонденції продовжує існувати, хоча може бути обмежена у випадках, коли це необхідно («*Барбулеску проти Румунії» (Bărbulescu v. Romania)* [ВП], 2017, §§80-81; див. також у професійному контексті «*Сарбу проти Румунії» (Sârbu v. Romania)*, 2023, §§ 37-38). Також у контексті моніторингу електронної кореспонденції політичною партією своїх членів («*Тена Аррегуї проти Іспанії» (Tena Arregui v. Spain)*, 2024, § 38). Моніторинг дій або пересування особи в громадських місцях за допомогою механізмів спостереження може підпадати під дію статті 8, якщо здійснюється системний або постійний запис таких персональних даних («*Глухін проти Росії» (Glukhin v. Russia)*, 2023, § 66), або якщо їх розголошення перевищує межі того, що можна було обґрунтовано очікувати («*Пек проти Сполученого Королівства» (Peck v. the United Kingdom)*, 2003, § 62; «*Перрі проти Сполученого Королівства» (Perry v. the United Kingdom)*, 2003, §§ 41-43). Що стосується статей у пресі про арешт телевізійного актора, проілюстрованих фотографіями, Суд встановив, що «законні очікування» актора на ефективний захист його приватного життя були зменшені через те, що він «активно прагнув бути в центрі уваги», розкриваючи подробиці свого приватного життя в низці інтерв'ю («*Аксель Шпрінгер АГ проти Німеччини» (Axel Springer AG v. Germany)* [ВП], 2012, § 101).

14. Що стосується характеру зібраних даних, деякі типи персональних даних і певні методи їх обробки є більш проблематичними, ніж інші, оскільки вони розкривають конфіденційну інформацію про поведінку, думки або почуття осіб («*Узун проти Німеччини» (Uzun v. Germany)*, 2010, § 52), де Суд порівняв дані, зібрані за допомогою GPS, з даними, зібраними за допомогою відео- чи аудіоспостереження). Зберігання або розголошення, без згоди суб'єкта, дуже інтимних або конфіденційних даних, що стосуються, наприклад, здоров'я особи, обов'язково підпадає під дію статті 8 («*Z проти Фінляндії» (Z v. Finland)*, 1997, § 71; «*Раду проти Молдови» (Radu v. Republic of Moldova)*, 2014, § 27; «*Моккуте проти Литви» (Mockutė v. Lithuania)*, 2018, §§ 93-95). Зважаючи на характер та обсяг персональної інформації, що міститься в клітинних зразках, їхнє зберігання саме по собі має розглядатися як втручання в право на повагу до приватного життя відповідних осіб, навіть якщо лише обмежена частина цієї інформації фактично вилучається або використовується органами влади і не спричиняє безпосередньої шкоди («*С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom)* [ВП], 2008, §§ 70-77).

15. Той факт, що персональні дані вже є суспільним надбанням або можуть бути доступними для громадськості, не обов'язково виводить їх з-під захисту статті 8 («*Сатакуннан Марккінапорссі Ой та Сатамедіа Ой проти Фінляндії» (Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland)* [ВП], 2017, § 134; «*Л.Б. проти Угорщини» (L.B. v. Hungary)* [ВП], 2023, § 104). Дані публічного характеру можуть підпадати під «приватне життя» особи, якщо вони збираються та зберігаються систематично («*П.Г. і Дж.Г. проти Сполученого Королівства» (P.G. and J.H. v. the United Kingdom)*, 2001, § 57; «*Пек проти Сполученого Королівства» (Peck v. the*

United Kingdom), 2003, §§ 58-59); «*Перрі проти Сполученого Королівства*» (*Perry v. the United Kingdom*), 2003, § 38), навіть без використання методів таємного спостереження («*Ротару проти Румунії*» (*Rotaru v. Romania*) [ВП], 2000, §§ 43-44; «*Антовіч і Мірковіч проти Чорногорії*» (*Antović and Mirković v. Montenegro*, 2017, §§ 44-45). Стаття 8 Конвенції передбачає право на певну форму інформаційного самовизначення, що дозволяє особам покладатися на своє право на недоторканність приватного життя щодо даних, які, хоча і є нейтральними, але збираються, обробляються та поширюються колективно, у такій формі або у такий спосіб, що можуть зачіпати права, передбачені статтею 8 («*Сатакуннан Марккінапорссі Ой та Сатамедіа Ой проти Фінляндії*» (*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*) [ВП], 2017, § 137; «*Л.В. проти Угорщини*» (*L.V. v. Hungary*) [ВП], 2023, § 103).

16. У більшості випадків, коли обробка персональних даних мала на меті дозволити органам влади провести розслідування щодо суб'єкта даних або зібрати докази у судових провадженнях у національних судах, Суд визнав, що така обробка підпадає під дію статті 8 і тягне за собою втручання у повагу до приватного життя відповідної особи («*Перрі проти Сполученого Королівства*» (*Perry v. the United Kingdom*), 2003, §§ 39-43; «*Узун проти Німеччини*» (*Uzun v. Germany*), 2010, §§ 51-52; «*Вукота-Боїч проти Швейцарії*» (*Vukota-Bojić v. Switzerland*), 2016, §§ 57-59; «*Лопез Рібалда та інші проти Іспанії*» (*López Ribalda and Others v. Spain*) [ВП], 2019, § 94; «*Сарбу проти Румунії*» (*Sârbu v. Romania*), 2023, §§ 38 і 41; порівняйте з «*Лупкер та інші проти Нідерландів*» (*Lupker and Others v. the Netherlands*), 1992, щодо використання поліцією з метою ідентифікації заявників фотографій, які були добровільно передані органам влади або зроблені під час попередніх арештів; «*Фрідл проти Австрії*» (*Friedl v. Austria*), 1994, §§ 50-51, щодо фотографування владою під час демонстрації з метою розслідування порушень правил дорожнього руху).

17. Нарешті, щоб стаття 8 застосовувалася, результати обробки персональних даних повинні досягти певного рівня серйозності та бути вчиненим так, щоб завдати шкоди особистому здійсненню права на повагу до приватного життя («*М.Л. та В.В. проти Німеччини*» (*M.L. and W.W. v. Germany*), 2018, § 88). У справі «*Вучина проти Хорватії*» (*Vučina v. Croatia*) (ухв.) 2019 (§ 50) Суд відхилив як несумісну *ratione materiae* (через обставини, пов'язані з предметом розгляду) скаргу на публікацію фотографії в жіночому журналі під помилковим заголовком, де заявниця була зображена як інша особа. На думку Суду, низький ступінь серйозності цієї помилки і незначні незручності не були достатніми для застосування статті 8.

2. Конкретні категорії даних

18. На думку Суду, певна дуже особиста або конфіденційна інформація однозначно виправдовує посилений захист. Інші категорії даних також потребують уваги з огляду на технологічний розвиток, який розширює можливості доступу до таких даних і призводить до більшої міжпрограмної взаємодії.

а. Так звані «конфіденційні» категорії

19. Відповідно до статті 6 Конвенції 108, персональні дані, що розкривають расове походження, політичні погляди, релігійні або інші переконання, а також інформація про стан здоров'я чи статеве життя особи або про будь-яку судимість, не можуть оброблятися автоматично, якщо національне законодавство не передбачає відповідних гарантій. Інформація, що підпадає під ці категорії, описується Судом як «конфіденційна» і, на його думку, вимагає підвищеного рівня захисту.

і. Дані, що розкривають расове чи етнічне походження

20. Етнічна ідентичність особи повинна розглядатися як важливий елемент приватного життя («*С. і Марпер проти Сполученого Королівства*» (*S. and Marper v. the United Kingdom*) [ВП],

2008, § 66); *«Чиботару проти Молдови» (Ciubotaru v. Moldova)*, 2010, § 49). Дані викликають особливе занепокоєння, якщо вони можуть розкрити етнічне або інше походження особи, зважаючи на швидкий темп розвитку генетики та інформаційних технологій (*«С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom)* [ВП], 2008, § 71). Зразки і профілі ДНК містять багато конфіденційної інформації та дозволяють органам влади встановлювати генетичні зв'язки між особами й оцінювати їхнє ймовірне етнічне походження (*там само*, §§ 72-77; *«Айсагюер проти Франції» (Aysaguer v. France)*, 2017, § 33). У справі, що стосувалася запису етнічного походження особи в офіційних реєстрах, Суд, підкреслюючи надзвичайно чутливий характер запису таких даних, визнав існування позитивного зобов'язання Держави запровадити процедуру, яка б дозволила суб'єкту даних змінити записану етнічну приналежність на підставі об'єктивно перевірених доказів (*«Чиботару проти Молдови» (Ciubotaru v. Moldova)*, 2010, §§ 52-59).

ii. Дані, що розкривають політичні погляди, релігійні або інші переконання, включно з філософськими

21. Дані, що розкривають політичні погляди, вважаються «конфіденційною» категорією персональних даних, і, на думку Суду, неприпустимо, щоб національні органи влади ігнорували цей аспект, обробляючи такі дані відповідно до звичайних національних правил, не беручи до уваги необхідність підвищеного захисту (*«Кетт проти Сполученого Королівства» (Catt v. the United Kingdom)*, 2019, § 112). У справі *«Кетт проти Сполученого Королівства» (Catt v. the United Kingdom)*, що стосувалася зберігання в поліцейській базі даних інформації про мирного демонстранта, національні суди лише посилалися на загальне законодавство про захист даних при розгляді законності втручання. Суд визнав порушення статті 8, зазначивши, що конфіденційний характер даних повинен був бути ключовим елементом справи (*там само*, § 112). Суд також встановив порушення статті 8 у справі *«М.Д. та інші проти Іспанії» (M.D. and Others v. Spain)*, 2022 (§§ 63-64), щодо протоколу поліції стосовно суддів і магістратів, які виконували свої функції в Каталонії та підписали маніфест із юридичною думкою щодо так званого «права вирішувати» каталонців. У протоколі були розкриті політичні погляди деяких заявників. Суд підкреслив, що персональні дані, які розкривають політичні погляди, повинні мати підвищений рівень захисту (*«Глухін проти Росії» (Glukhin v. Russia)*, 2023, §§ 76 і 86, коли персональні дані заявника, які були оброблені, містили інформацію про його участь у мирному протесті).

22. У справах *«Сінан Ішик проти Туреччини» (Sinan Işık v. Turkey)*, 2010 (§ 37) та *«Моккуте проти Литви» (Mockutė v. Lithuania)*, 2018 (§ 117) Суд розглядав право на захист персональних даних, що розкривають релігійні або інші переконання особи, включно з філософськими. Стосовно питання зазначення релігії в посвідченнях особи Суд підкреслив важливість права на захист даних, що стосуються релігійних переконань, які є одним із найважливіших елементів ідентичності віруючих та їхньої життєвої концепції, захищеної статтею 9 Конвенції (*«Сінан Ішик проти Туреччини» (Sinan Işık v. Turkey)*, 2010, § 37).

iii. Дані про членство в профспілці

23. Персональні дані, що розкривають членство особи в профспілці, також можуть бути «конфіденційними» і потребувати підвищеного захисту. У справі *«Кетт проти Сполученого Королівства» (Catt v. the United Kingdom)*, 2019 (§ 112) поліція збрала інформацію про участь заявника в демонстраціях, організованих профспілками, зокрема його ім'я, дату народження й адресу. У деяких випадках також була описана його зовнішність і надано фотографії, зроблені під час демонстрацій (*там само*, § 10). Участь у мирному протесті має особливий захист відповідно до статті 11 Конвенції, яка також забезпечує спеціальний захист для профспілок (*там само*, § 123). Хоча збір поліцією персональних даних про заявника можна вважати виправданим, Суд зазначив, що не було нагальної потреби зберігати ці дані за відсутності

чітких правил, які встановлюють максимальний строк їхнього зберігання (*там само*, §§ 117-119).

iv. Генетичні та біометричні дані

24. Суд розглянув низку справ, що стосувалися збору або зберігання

- клітинних зразків («*Ван дер Вельден проти Нідерландів*» (*Van der Velden v. the Netherlands*) (ухв.), 2005; «*Шмідт проти Німеччини*» (*Schmidt v. Germany*) (ухв.), 2006; «*С. і Марпер проти Сполученого Королівства*» (*S. and Marper v. the United Kingdom*) [ВП], 2008; «*Канонн проти Франції*» (*Canonne v. France*) (ухв.), 2015; «*Каруана проти Мальти*» (*Caruana v. Malta*) (ухв.), 2018; «*Трайковські та Чіповські проти Північної Македонії*» (*Trajkovski and Chipovski v. North Macedonia*), 2020; «*Болевіч проти Сербії*» (*Boljević v. Serbia*), 2020);
- ДНК-профілів: «*Ван дер Вельден проти Нідерландів*» (*Van der Velden v. the Netherlands*) (ухв.), 2005; «*Шмідт проти Німеччини*» (*Schmidt v. Germany*) (ухв.), 2006; «*С. і Марпер проти Сполученого Королівства*» (*S. and Marper v. the United Kingdom*) [ВП], 2008; «*В. проти Нідерландів*» (*W. v. the Netherlands*) (ухв.), 2009; «*Перуззо і Мартенс проти Німеччини*» (*Peruzzo and Martens v. Germany*) (ухв.), 2013; «*Канонн проти Франції*» (*Canonne v. France*) (ухв.), 2015; «*Айкагуер проти Франції*» (*Ayscaguer v. France*), 2017; «*Міфсуд проти Мальти*» (*Mifsud v. Malta*), 2019; «*Горран проти Сполученого Королівства*» (*Gaughran v. the United Kingdom*), 2020; «*Трайковські та Чіповські проти Північної Македонії*» (*Trajkovski and Chipovski v. North Macedonia*), 2020; «*Драган Петровіч проти Сербії*» (*Dragan Petrović v. Serbia*), 2020;
- відбитків пальців: «*Маквей, Оніл та Еванс проти Сполученого Королівства*» (*McVeigh, O'Neill and Evans v. the United Kingdom*), 1981; «*Кіннунен проти Фінляндії*» (*Kinnunen v. Finland*), 1993; «*С. і Марпер проти Сполученого Королівства*» (*S. and Marper v. the United Kingdom*) [ВП], 2008; «*Дімітров-Казаків проти Болгарії*» (*Dimitrov-Kazakov v. Bulgaria*), 2011; «*М.К. проти Франції*» (*M.K. v. France*), 2013; «*Супруненко проти Росії*» (*Suprunenko v. Russia*) (ухв.), 2018; «*Горран проти Сполученого Королівства*» (*Gaughran v. the United Kingdom*), 2020; «*П.Н. проти Німеччини*» (*P.N. v. Germany*), 2020; «*Віллемс проти Нідерландів*» (*Willems v. the Netherlands*) (ухв.), 2021;
- відбитків долонь «*П.Н. проти Німеччини*» (*P.N. v. Germany*), 2020.
- зразків голосу («*П.Г. і Дж.Г. проти Сполученого Королівства*» (*P.G. and J.H. v. the United Kingdom*), 2001; «*Еллен проти Сполученого Королівства*» (*Allan v. the United Kingdom*), 2002; «*Дюерга проти Нідерландів*» (*Doerga v. the Netherlands*), 2004; «*Веттер проти Франції*» (*Vetter v. France*), 2005; «*Віссе проти Франції*» (*Wisse v. France*), 2005).

25. Беручи до уваги швидкі темпи розвитку генетики та інформаційних технологій, Суд не може відкидати можливість того, що в майбутньому інтереси приватного життя, пов'язані з генетичною інформацією, можуть зазнати негативного впливу у новий спосіб або у спосіб, який сьогодні неможливо точно передбачити («*С. і Марпер проти Сполученого Королівства*» (*S. and Marper v. the United Kingdom*) [ВП], 2008, § 71).

26. Що стосується клітинних зразків, то з огляду на характер і обсяг персональної інформації, яку вони містять, їх зберігання саме по собі повинно розглядатися як втручання в право на повагу до приватного життя відповідних осіб. Той факт, що лише обмежена частина цієї інформації фактично вилучається або використовується органами влади за допомогою ДНК-профілювання, і що в кожному конкретному випадку не завдається безпосередньої шкоди, не змінює цього висновку (*там само*, § 73; «*Аманн проти Швейцарії*» (*Amann v. Switzerland*) [ВП], 2000, § 69).

27. Що стосується ДНК-профілів, то можливість зробити з них висновки про етнічне походження особи робить їх зберігання ще більш конфіденційним і сприйнятливим до впливу на право на приватне життя, що вимагає посиленого захисту (*«С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom)* [ВП], 2008, § 76). Хоча інформація, що міститься в профілях, може вважатися об'єктивною і неспростовною, її здатність слугувати засобом виявлення генетичних зв'язків між особами сама по собі є достатньою для висновку про те, що її зберігання втручається в право на приватне життя відповідних осіб, незважаючи на будь-які гарантії або ступінь ймовірності заподіяння шкоди в кожному конкретному випадку (*там само*, § 75; *«Аманн проти Швейцарії» (Amann v. Switzerland)* [ВП], 2000, § 69). На цей висновок не впливає той факт, що, оскільки інформація міститься в закодованій формі, вона є зрозумілою лише за допомогою комп'ютерних технологій і може бути інтерпретована лише обмеженим колом осіб (*«С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom)* [ВП], 2008, §§ 74-75).

28. Що стосується відбитків пальців, то оскільки вони об'єктивно містять унікальну інформацію про відповідну особу, що дозволяє її ідентифікувати з точністю в широкому діапазоні обставин, зберігання цієї інформації без згоди відповідної особи не може розглядатися як нейтральне або несуттєве (*там само*, § 84). Хоча зберігання відбитків пальців у документах органів влади у зв'язку з ідентифікованою особою або особою, яку можна ідентифікувати, може мати менший вплив на приватне життя, ніж зберігання зразків клітин і профілів ДНК (*там само*, § 69), воно може викликати важливе занепокоєння щодо приватного життя, незважаючи на об'єктивний і неспростовний характер таких даних (*там само*, § 85). Це рішення відступає від судової практики, встановленої Комісією у справі *«Кіннунен проти Фінляндії» (Kinnunen v. Finland)*, 1996). У справі *«Віллемс проти Нідерландів» (Willems v. the Netherlands)* (ухв.), 2021, скарги щодо обов'язку відповідно до Закону про паспорти здавати відбитки пальців при подачі заяви на отримання паспорта, а також зберігання таких відбитків на електронному чіпі після включення у внутрішнє законодавство Регламенту ЄС про стандарти щодо елементів безпеки та біометричних даних у паспортах та проїзних документах, що видаються Державними членами, були відхилені як явно необґрунтовані через «презумпцію еквівалентного захисту» у праві ЄС (*там само*, §§ 26-36).

29. Через інформацію, яку вони містять, зберігання зразків клітин і профілів ДНК має більший вплив на приватне життя, ніж зберігання відбитків пальців (*«С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom)* [ВП], 2008, § 86). Однак, хоча при вирішенні питання про обґрунтованість може виникнути необхідність розрізняти взяття, використання та зберігання відбитків пальців, з одного боку, та зразків і профілів, з іншого, збереження відбитків пальців *per se* (саме) по собі є втручанням у право на повагу до приватного життя.

30. За певних обставин, особливо у справах про батьківство, органи влади можуть примусити особу пройти тест ДНК, за умови дотримання її права на захист і встановлення національними судами справедливого балансу між інтересами, які стоять на кону (*«Міфсуд проти Мальти» (Mifsud v. Malta)*, 2019, §§ 77-78). Стаття 8 сама по собі не забороняє застосування медичних процедур всупереч волі підозрюваного або свідка з метою отримання доказів, оскільки такі методи, зокрема у цивільній сфері, самі по собі не суперечать верховенству права та природній справедливості (*там само*, § 71). Система, яка не має засобів примусити передбачуваного батька виконати рішення суду про проведення тесту ДНК, може в принципі вважатися сумісною із зобов'язаннями, що випливають зі статті 8, особливо якщо вона передбачає альтернативні засоби, що дозволяють незалежному органу швидко вирішити питання про батьківство (*«Мікуліч проти Хорватії» (Mikulić v. Croatia)*, 2002, §§ 55, 64).

v. Дані про здоров'я, сексуальне життя та сексуальну орієнтацію

31. Інформація про стан здоров'я особи становить ключовий елемент приватного життя (*«Івон Шаве, в дівоцтві Жульєн, проти Франції» (Yvonne Chave née Jullien v. France)*, 1991, § 75; *«Л.Л.*

проти Франції» (L.L. v. France), 2006; *«Раду проти Молдови» (Radu v. Moldova)*, 2014; *«Л.Г. проти Латвії» (L.H. v. Latvia)*, 2014, § 56; *«Коновалова проти Росії» (Konovalova v. Russia)*, 2014, §§ 27, 41; *«Й.Й. проти Росії» (Y.Y. v. Russia)*, 2016, § 38; *«Суріков проти України» (Surikov v. Ukraine)*, 2017; *«Францу проти Румунії» (Frâncu v. Romania)*, 2020, § 52). Повага до конфіденційності цієї інформації вкрай важлива. І йдеться не лише про повагу до права пацієнта на недоторканність приватного життя, а й про збереження його або її довіри до медичної професії та до служб охорони здоров'я загалом. Ці міркування особливо обґрунтовані у частині, що стосується захисту конфіденційності інформації про ВІЛ-інфекцію у людини (*«Z проти Фінляндії» (Z v. Finland)*, 1997, § 96; *«Кіютін проти Росії» (Kiyutin v. Russia)*, 2011, § 64; *«Армонієне проти Литви» (Armonienė v. Lithuania)*, 2008, § 40; *«Бірюк проти Литви» (Biriuk v. Lithuania)*, 2008, § 39; *«І. проти Фінляндії» (I. v. Finland)*, 2008, § 38; *«К.К. проти Іспанії» (C.C. v. Spain)*, 2009, § 33; *«Й. проти Туреччини» (Y. v. Turkey)* (ухв.), 2015, § 65; *«П.Т. проти Республіки Молдова» (P.T. v. Republic of Moldova)*, 2020, §§ 5-6, 26; *«Й.Г. проти Росії» (Y.G. v. Russia)*, 2022, § 45). Розголошення таких даних може кардинально вплинути на приватне та сімейне життя особи, а також соціальне та трудове становище, наражаючи особу на осуд і ризик остракізму (*«Z проти Фінляндії» (Z v. Finland)*, 1997, § 96; *«К.К. проти Іспанії» (C.C. v. Spain)*, 2009, § 33; *«П. і С. проти Польщі» (P. and S. v. Poland)*, 2012, § 128; *«Авілкіна та інші проти Росії» (Avilkina and Others v. Russia)*, 2013, § 45; *«Й. проти Туреччини» (Y. v. Turkey)* (ухв.), 2015, § 65; *«Й.Г. проти Росії» (Y.G. v. Russia)*, 2022, § 45).

32. Таким чином, інтерес у захисті конфіденційності такої інформації матиме значний вплив при визначенні того, чи було втручання пропорційним переслідуючій законній меті. Таке втручання не може бути сумісним зі статтею 8 Конвенції, якщо воно не виправдане вищою вимогою суспільного інтересу (*«Z проти Фінляндії» (Z v. Finland)*, 1997, § 96). З огляду на надзвичайно інтимний і конфіденційний характер інформації про ВІЛ-статус особи, будь-які заходи Держави, що примушують повідомляти або розкривати таку інформацію без згоди пацієнта, вимагають найретельнішої перевірки з боку Суду (*ibid.*, § 96).

33. Таким чином, Суд визнав порушення статті 8, наприклад, у справах *«Z проти Фінляндії» (Z v. Finland)*, 1997, §§ 113-114, у зв'язку з публікацією даних про особу та ВІЛ-статус жінки в судовому рішенні, винесеному під час кримінального провадження проти її чоловіка, про що повідомляла преса; *«Л.Л. проти Франції» (L.L. v. France)*, 2006, §§ 32-48, щодо відтворення в рішенні про розлучення витягу з особистого медичного документа; *«І. проти Фінляндії» (I. v. Finland)*, 2008, §§ 35-49, щодо недостатнього захисту від несанкціонованого доступу до медичної картки ВІЛ-позитивної медсестри; *«К.К. проти Іспанії» (C.C. v. Spain)*, 2009, §§ 26-41, щодо публікації особи заявника в судовому рішенні, пов'язаному з його ВІЛ-статусом; *«П. і С. проти Польщі» (P. and S. v. Poland)*, 2012, §§ 128-137, щодо розголошення державною лікарнею інформації про вагітну дівчину, яка хотіла зробити аборт після зґвалтування; *«Коновалова проти Росії» (Konovalova v. Russia)*, 2014, §§ 39-50, де заявниця скаржилася на те, що їй довелося народжувати перед студентами-медиками без її згоди; *«П.Т. проти Республіки Молдова» (P.T. v. Republic of Moldova)*, 2020, §§ 24-33, за непотрібну присутність конфіденційних медичних даних у довідці, призначеній для різного використання; *«Францу проти Румунії» (Frâncu v. Romania)*, 2020, § 52, щодо відмови у проведенні приватного слухання у справі про корупцію проти мера за заявою про звільнення за станом здоров'я; та *«Й.Г. проти Росії» (Y.G. v. Russia)*, 2022, §§ 46-53, де заявник скаржився на те, що база даних, яка містила, зокрема, його медичні дані, була доступна для продажу на ринку, та *«А. П. проти Вірменії» (A.P. v. Armenia)*, 2024, §§ 150-159, де заявниця скаржилася на те, що її повне ім'я та адреса, а також повні тексти судових рішень про відхилення її цивільного позову про відшкодування шкоди за сексуальне насильство були розкриті в загальнодоступній онлайн-базі даних судової влади, незважаючи на її конкретне прохання не публікувати цю інформацію.

34. Інформація про психічне здоров'я особи є досить конфіденційною інформацією (*«Моккуте проти Литви» (Mockuté v. Lithuania)*, 2018, § 94, щодо розголошення психіатричною лікарнею

даних про психічне здоров'я пацієнта; *«Маланічева проти Росії» (Malanicheva v. Russia)* (ухв.), 2016, §§ 13, 15-18, щодо запису в медичній справі в лікарні даних про примусове розміщення заявників), як і дані, що розкривають сексуальну ідентифікацію або орієнтацію (*«Даджеон проти Сполученого Королівства» (Dudgeon v. the United Kingdom)*, 1981, § 41; *«Дж.Л. проти Італії» (J.L. v. Italy)*, 2021, § 136; *«Дрелон проти Франції» (Drelon v. France)*, 2022, § 79) та статеве життя особи, наприклад, дані про аборт, передані від одного органу державної влади до іншого без згоди суб'єкта даних (*«М.С. проти Швеції» (M.S. v. Sweden)*, 1997, §§ 41-42). Національне законодавство повинно надавати відповідні гарантії для запобігання будь-якій передачі або розголошенню таких даних, які не відповідають гарантіям, передбаченим статтею 8 (*«Z проти Фінляндії» (Z v. Finland)*, 1997, § 95).

ві. Дані про кримінальні правопорушення та засудження

35. Дані, що стосуються правопорушень, кримінальних проваджень, засуджень або пов'язаних із ними превентивних заходів, становлять категорію даних, які вимагають підвищеного захисту відповідно до статті 6 Конвенції 108 (*«М.М. проти Сполученого Королівства» (M.M. v. the United Kingdom)*, 2012, § 188; *«Маргарі проти Греції» (Margari v. Greece)*, 2023, § 59). Тому вкрай важливо, щоб при публікації конфіденційних даних у контексті відкритого кримінального провадження або розслідування кримінальних правопорушень ці дані точно відображали ситуацію та висунуті обвинуваченому звинувачення, а також враховували дотримання презумпції невинуватості (*там само*). Будь-яка обробка персональних даних, що стосується особи, проти якої було знято обвинувачення (*«Брунет проти Франції» (Brunet v. France)*, 2014, §§ 38-40; *«Н.Ф. та інші проти Росії» (N.F. and Others v. Russia)*, 2023, § 38), якій було винесено попередження (*«М.М. проти Сполученого Королівства» (M.M. v. the United Kingdom)*, 2012, §§ 188-190), яку було визнано винною та засуджено (*«Гардель проти Франції» (Gardel v. France)*, 2009, § 58; *«Перуззо і Мартенс проти Німеччини» (Peruzzo and Martens v. Germany)* (ухв.), 2013, § 44; *«Трайковські та Чіповські проти Північної Македонії» (Trajkovski and Chipovski v. North Macedonia)*, 2020, § 46; *«Н.Ф. та інші проти Росії» (N.F. and Others v. Russia)*, 2023, § 38) або підданої відповідному запобіжному заходу, такому як затримання у відділку поліції (*«Супруненко проти Росії» (Suprunenko v. Russia)*, (ухв.), 2018, § 61), становитиме втручання у право суб'єкта даних на повагу до його приватного життя.

36. На думку Суду, хоча дані, що містяться в судимості, в певному сенсі є публічною інформацією, їхнє систематичне зберігання в центральних архівах означає, що вони доступні для розголошення через тривалий час після події, коли всі, крім зацікавленої особи, ймовірно, забули про неї. Таким чином, оскільки саме засудження або застереження відходить у минуле, воно стає частиною приватного життя особи, яке має поважатися (*«М.М. проти Сполученого Королівства» (M.M. v. the United Kingdom)*, 2012, § 188), тим більше, коли дані стосуються далекого минулого особи (*«Б.Б. проти Франції» (B.B. v. France)*, 2009, § 57; *«Кетт проти Сполученого Королівства» (Catt v. the United Kingdom)*, 2019, § 93; *«М.Л. та В.В. проти Німеччини» (M.L. and W.W. v. Germany)*, 2018, §§ 98-100).

37. Захід, пов'язаний зі збереженням у поліцейських реєстрах ідентифікаційних даних, відбитків пальців і фотографій особи, може мати для неї серйозні наслідки, ускладнюючи повсякденне життя *«Дімітров-Казаків проти Болгарії» (Dimitrov-Kazakov v. Bulgaria)*, 2011, §§ 8, 10, 13, 30). У справі, що стосувалася внесення особи як «правопорушника» до поліцейських протоколів після того, як його допитали про зґвалтування, і збереження цього запису, незважаючи на те, що обвинувачення не було висунуто, Суд визнав порушення статті 8, встановивши, що суб'єкт даних, саме через цей запис, був об'єктом кількох поліцейських перевірок у зв'язку зі скаргами на зґвалтування або зникненням молодих дівчат (*там само*., §§ 8, 10, 13, 30).

38. Крім того, тривале зберігання даних про заміну заявникові адміністративного стягнення (форма вирішення кримінальної справи без винесення обвинувального вироку) становило

втручання в його право на повагу до приватного життя, передбачене статтею 8 Конвенції («Тончев проти Болгарії» (*Tonchev v. Bulgaria*), 2024, § 125). Згідно з практикою Суду, саме лише зберігання таких даних органом державної влади становить втручання, незалежно від того, чи будуть ці дані згодом використані або яким чином. Суд визнав порушення статті 8 Конвенції, оскільки відповідні положення болгарського законодавства були достатньо розпливчастими, щоб викликати плутанину серед національних органів, відповідальних за їхнє тлумачення та застосування, а отже, регулювання не було достатньо передбачуваним. Крім того, ці розбіжності поширювалися на застосування права ЄС про захист даних (принцип обмеження терміну зберігання; там само, § 137).

б. Інші категорії даних

40. Окрім даних, описаних як «чутливі», інші категорії персональних даних також викликають занепокоєння, особливо з огляду на все більш витончені методи спостереження і здатність інформаційно-комунікаційних технологій ускладнювати повсякденне життя суб'єктів даних.

і. Дані про зайнятість

40. Запис даних, пов'язаних з працевлаштуванням, про ідентифіковану особу або особу, яку можна ідентифікувати, та їх зберігання — це втручання у право суб'єкта даних на повагу до його приватного та сімейного життя відповідно до статті 8 («Хелілі проти Швейцарії» (*Khelili v. Switzerland*), 2011, § 56; «Соро проти Естонії» (*Sõro v. Estonia*), 2015, §§ 49 і 56; «Флоріндо де Альмейда Васконселос Грамаксо проти Португалії» (*Florindo de Almeida Vasconcelos Gramaxo v. Portugal*), 2022, §§ 95-96). З огляду на те, що інформація, яка збирається органами влади та зберігається в їхніх документах, сьогодні є предметом автоматизованої обробки, що значно полегшує доступ до таких даних та їх передачу, такі заходи можуть мати серйозні наслідки, здатні завдати шкоди репутації осіб або ускладнити їхнє повсякденне життя. Суд встановив порушення статті 8 у справах «Хелілі проти Швейцарії» (*Khelili v. Switzerland*), 2011, § 64, де заявниця була записана поліцією як «повія», а запис згодом був виправлений і замінений на «швачка» в базі даних, та «Соро проти Естонії» (*Sõro v. Estonia*), 2015, § 63, де заявника зобов'язали звільнитися з роботи після розголошення даних про його роботу водієм у колишніх службах безпеки. У справі «Флоріндо де Альмейда Васконселос Грамаксо проти Португалії» (*Florindo de Almeida Vasconcelos Gramaxo v. Portugal*), 2022, §§ 95-96, роботодавець заявника встановив систему GPS у службовому автомобілі заявника з метою моніторингу відстаней, що були подолані під час його професійної діяльності та, за необхідності, під час приватних поїздок. Суд постановив, що зібрана інформація становить персональні дані. Суд також підкреслив, що працівники не мали повноважень відключати систему GPS, тому вона залишалася активною цілодобово, сім днів на тиждень, в результаті чого спостереження було постійним і систематичним, що явно втручалось в приватне життя заявника¹.

ii. Фінансові дані

39. Інформація, отримана з банківських документів фізичної особи, становить персональні дані, незалежно від того, чи це конфіденційна приватна інформація, чи інформація про професійну діяльність суб'єкта даних («М.Н. та інші проти Сан-Маріно» (*M.N. and Others v. San Marino*), 2015, § 51; «Г.С.Б. проти Швейцарії» (*G.S.B. v. Switzerland*), 2015, § 51). Копіювання банківських даних і подальше зберігання органами влади таких даних, дії, які підпадають під поняття як «приватне життя», так і «кореспонденція», становлять втручання для цілей статті 8 («М.Н. та інші проти Сан-Маріно» (*M.N. and Others v. San Marino*), 2015, § 55).

¹ Див. також «Дані про місцезнаходження за допомогою GPS» нижче.

40. Суд розглядав питання збору, обробки та розголошення фінансових даних у контексті: кримінального розслідування (*«М.Н. та інші проти Сан-Маріно» (M.N. and Others v. San Marino)*, 2015, §§ 7-9, 53-55); широкої публікації в пресі фінансових даних з метою обговорення питання, що становить загальний інтерес (*«Сатакуннан Марккінапорссі Ой та Сатамедіа Ой проти Фінляндії» (Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland)* [ВП], 2017, §§ 172-173); обов'язку адвоката розкривати дані, що становлять професійну таємницю, при повідомленні про підозри щодо протиправної діяльності з боку клієнтів, наприклад, відмивання грошей (*«Мішод проти Франції» (Michaud v. France)*, 2012, §§ 91-92); передачі фінансових даних органам влади іншої Держави, яка не є стороною Конвенції (*«Г.С.Б. проти Швейцарії» (G.S.B. v. Switzerland)*, 2015, § 50); і, нарешті, відхилення позову щодо розголошення інформації про податковий ідентифікаційний номер та податкову декларацію заявниці під час телевізійного репортажу про кримінальну справу проти її чоловіка (*«Самойлова проти Росії» (Samoylova v. Russia)*, 2021, §§ 83 і 90-93).

41. Існування суспільного інтересу в наданні доступу до великих обсягів податкових даних і дозволу на їх збір не обов'язково або автоматично означає, що існує також суспільний інтерес у масовому поширенні таких необроблених даних у незміненому вигляді без будь-якого аналітичного втручання (*«Сатакуннан Марккінапорссі Ой та Сатамедіа Ой проти Фінляндії» (Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland)* [ВП], 2017, §§ 172-178, 198).

42. Попри те, що в податкових питаннях свобода розсуду Держави є ширшою, коли йдеться про захист суто фінансових даних, які не включають жодних даних, що мають особистий характер або тісно пов'язані з особою суб'єкта даних (*«Г.С.Б. проти Швейцарії» (G.S.B. v. Switzerland)*, 2015, § 93), міркування приватного життя вступають у гру в ситуаціях, коли податкові дані були зібрані про конкретну особу або коли вони були оприлюднені у спосіб або в обсязі, що виходить за межі того, що суб'єкт даних міг розумно передбачити (*«М.Н. та інші проти Сан-Маріно» (M.N. and Others v. San Marino)*, 2015, §§ 52-53; *«Сатакуннан Марккінапорссі Ой та Сатамедіа Ой проти Фінляндії» (Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland)* [ВП], 2017, § 136).

iii. Дані трафіку

43. Дані про трафік включають дані, отримані від телефонних операторів, які ідентифікують особу, якій або від якої здійснюється комунікація, а також дату, час і тривалість комунікації, але не стосуються її змісту (*«Мелоун проти Сполученого Королівства» (Malone v. the United Kingdom)*, 1984, §§ 83-84; *«Копленд проти Сполученого Королівства» (Copland v. the United Kingdom)*, 2007, § 43). У контексті кримінального розслідування процес, відомий як «облік», що передбачає використання пристрою (принтер перевірки контрольного пристрою), який реєструє номери, набрані на певний телефон, а також час і тривалість кожного дзвінка, без моніторингу або перехоплення комунікацій, є втручанням у приватне життя суб'єкта даних (*«Мелоун проти Сполученого Королівства» (Malone v. the United Kingdom)*, 1984, §§ 83-84). Використання таких даних і, зокрема, набраних номерів може викликати питання за статтею 8, оскільки така інформація є «невід'ємним елементом телефонних комунікацій» (*«Мелоун проти Сполученого Королівства» (Malone v. the United Kingdom)*, 1984, § 84; *«Копленд проти Сполученого Королівства» (Copland v. the United Kingdom)*, 2007, § 43). На думку Суду, передача цієї інформації поліції без згоди абонента також становить втручання у право, гарантоване статтею 8 (*«Мелоун проти Сполученого Королівства» (Malone v. the United Kingdom)*, 1984, § 84).

44. Практику «обліку», яка не порушуватиме статтю 8, якщо вона здійснюється, наприклад, постачальником телефонних послуг для забезпечення правильності нарахування абоненту плати, слід відрізнати за своєю природою від перехоплення дзвінків (*«Мелоун проти Сполученого Королівства» (Malone v. the United Kingdom)*, 1984, §§ 83-84; *«П.Г. і Дж.Г. проти Сполученого Королівства» (P.G. and J.H. v. the United Kingdom)*, 2001, § 42). Судовий наказ,

надісланий телефонній компанії для отримання даних про дзвінки, здійснені на різні мобільні телефони особи та з різних мобільних телефонів, а також для збору даних про місцезнаходження мобільного телефону для подальшого відстеження його пересування, не обов'язково був несумісним зі статтею 8, оскільки він був санкціонований законом і забезпечував достатні гарантії проти свавілля (*«Бен Файза проти Франції» (Ben Faiza v. France)*, 2018, §§ 56, 59, 69). Суд не знайшов порушення статті 8 у справі, де такі накази мали бути попередньо санкціоновані прокурором під загрозою їх недійсності та могли бути оскаржені в суді, а отримані дані могли бути виключені з доказів у разі їх незаконності (*там само*, §§ 79, 73).

45. Персональні дані користувачів передплатених SIM-карт, такі як імена, адреси та номери телефонів абонентів мобільного зв'язку, зібрані постачальниками послуг, не можуть вважатися «несуттєвими» (*«Бреєр проти Німеччини» (Breyer v. Germany)*, 2020, §§ 92-95). Саме лише зберігання постачальниками послуг зв'язку таких абонентських даних є втручанням у приватне життя суб'єкта даних, незалежно від будь-якого подальшого використання (*там само*, § 92). Таке втручання має досить обмежений характер (*там само*, § 95), а національні органи влади користуються певною свободою розсуду в цій сфері за відсутності будь-якого європейського консенсусу (*там само*, § 90). Відсутність повідомлення про процедуру вилучення не буде несумісною зі статтею 8, якщо існує нагляд з боку незалежного органу, який уповноважений перевіряти, якщо це буде визнано обґрунтованим, чи є прийнятним передача даних органу, що запитує їх, а також можливість оскарження будь-ким, хто вважає, що його або її права були порушені в результаті процедури вилучення або запиту даних (*там само*, §§ 103-107).

46. Що стосується даних про інтернет-з'єднання, то вони можуть дозволити ідентифікувати користувача, наприклад, його або її IP-адресу та адресу електронної пошти, адресата (адресатів) комунікації, інформацію про використані матеріали комунікації та будь-які додаткові послуги, які були запитані або використані, а також їхнього постачальника (*«Бенедік проти Словенії» (Benedik v. Slovenia)*, 2018, § 96). На думку Суду, інформація про абонента, пов'язана з конкретними динамічними IP-адресами, присвоєними в певний час, становить персональні дані. Вона не є загальнодоступною і тому не може порівнюватися з інформацією, що міститься в традиційному телефонному довіднику або публічній базі даних реєстраційних номерів транспортних засобів (*там само*, § 108).

47. Отримання пов'язаних даних про комунікації в контексті масового перехоплення не обов'язково є менш інтрузивним, ніж отримання змісту комунікацій (*«Центр правосуддя проти Швеції» (Centrum för rättvisa v. Sweden)* [ВП], 2021, 277, і *«Біг Бразер Вотч та інші проти Сполученого Королівства» (Big Brother Watch and Others v. the United Kingdom)* [ВП], 2021, § 363). Перехоплення, зберігання та пошук пов'язаних з ними комунікаційних даних слід аналізувати з урахуванням тих самих гарантій, які застосовуються до змісту. При цьому, зважаючи на різний характер пов'язаних комунікаційних даних та різні способи їх використання спецслужбами, доки існують вищезазначені гарантії, правові положення, що регулюють поводження з ними, не обов'язково повинні бути в усіх відношеннях ідентичними положенням, що регулюють поводження зі змістом (*«Центр правосуддя проти Швеції» Centrum för rättvisa v. Sweden* [ВП], 2021, § 278; та *«Біг Бразер Вотч та інші проти Сполученого Королівства» (Big Brother Watch and Others v. the United Kingdom)* [ВП], 2021, § 364).

50. Переважна вимога конфіденційності даних про з'єднання може за певних обставин виявитися несумісною зі статтею 8, якщо вона перешкоджає ефективному кримінальному розслідуванню з метою виявлення та притягнення до відповідальності особи, яка вчинила злочин через інтернет (*«К.У. проти Фінляндії» (K.U. v. Finland)*, 2008, § 49). Гарантія абонентам телекомунікацій та інтернету на повагу до їхнього приватного життя повинна в окремих випадках поступатися іншим законним імперативам, таким як запобігання заворушенням чи злочинам або захист прав і свобод інших осіб (*там само*, § 49).

iv. Зразки голосу

48. Операції з «прослуховування» спрямовані на перехоплення розмов особи шляхом встановлення пристроїв прослуховування на приватній власності («*Vetter проти Франції*» (*Vetter v. France*), 2005, §§ 10, 20) або в громадських місцях («*П.Г. і Дж.Г. проти Сполученого Королівства*» (*P.G. and J.H. v. the United Kingdom*), 2001, §§ 38, 63; «*Еллен проти Сполученого Королівства*» (*Allan v. the United Kingdom*), 2002, § 35; «*Доєрга проти Нідерландів*» (*Doerga v. the Netherlands*), 2004, § 43; «*Віссе проти Франції*» (*Wisse v. France*), 2005, § 29).

49. Приховане прослуховування голосу особи та зберігання постійного запису, який підлягає аналізу і має безпосереднє відношення до ідентифікації цієї особи в контексті інших персональних даних, становить обробку персональних даних, яка втручається в право суб'єкта даних на повагу до його приватного життя («*П.Г. і Дж.Г. проти Сполученого Королівства*» (*P.G. and J.H. v. the United Kingdom*), 2001, §§ 59-60). У справі, де не було національного законодавства, що регулює використання пристроїв для прихованого прослуховування, встановлених поліцією у власних приміщеннях або на приватних територіях, Суд встановив порушення статті 8 (*там само*, §§ 38, 63).

50. Прослуховування розмов за допомогою пристроїв прослуховування, як і перехоплення телефонних дзвінків, є серйозним втручанням у право суб'єкта даних на повагу до його приватного життя («*Vetter проти Франції*» (*Vetter v. France*), 2005, § 26). Тому воно повинно ґрунтуватися на особливо точному «законі». І в цій сфері видається необхідним існування чітких і детальних правил, особливо з огляду на те, що відповідні технічні процеси постійно вдосконалюються (*там само*, § 26). На думку Суду, «закон» повинен надавати громадянам «відповідні гарантії» проти такого ж роду зловживань, яких можна було б побоюватися у випадку з прослуховуванням телефонних розмов (*там само*, § 26). Таким чином, зокрема, необхідно визначити категорії осіб, до яких може бути застосований такий захід, а також види правопорушень, які можуть бути підставою для його застосування; суд повинен буде встановити часові рамки для застосування такого заходу. Необхідно також визначити умови складання протоколів про перехоплені розмови, запобіжні заходи, яких необхідно вжити для передачі записів у непошкодженому й повному вигляді для можливого перегляду суддею і захистом, а також обставини, за яких плівки повинні бути видалені або знищені, особливо після прийняття рішення про закриття справи або виправдувального вироку (*там само*, § 26, з посиланням на критерії перехоплення доказів, викладені у справі «*Круслін проти Франції*» (*Kruslin v. France*), 1990, § 35).

51. Якщо голос особи був записаний без мінімального рівня захисту, що вимагається верховенством права в демократичному суспільстві, це буде порушенням статті 8 («*Віссе проти Франції*» (*Wisse v. France*), 2005, § 34 про запис і подальше використання розмов у кімнаті для побачень у в'язниці; «*Еллен проти Сполученого Королівства*» (*Allan v. the United Kingdom*), 2002, § 36, про встановлення прослуховувального пристрою в тюремній камері).

v. Дані про місцезнаходження за допомогою GPS

52. Дані, зібрані за допомогою GPS-пристрою, є персональними даними, оскільки вони можуть вказувати на місцезнаходження особи та її публічні пересування («*Узун проти Німеччини*» (*Uzun v. Germany*), 2010, §§ 51-52; «*Флоріндо де Альмейда Васконселос Грамаксо проти Португалії*» (*Florindo de Almeida Vasconcelos Gramaxo v. Portugal*), 2022, § 95). Обробка та використання таких даних можуть розглядатися як втручання в право суб'єкта даних на повагу до приватного життя («*Узун проти Німеччини*» (*Uzun v. Germany*), 2010, §§ 51-52; «*Флоріндо де Альмейда Васконселос Грамаксо проти Португалії*» (*Florindo de Almeida Vasconcelos Gramaxo v. Portugal*), 2022, § 96). GPS-спостереження за своєю природою слід відрізняти від інших методів візуального або акустичного спостереження, які, як правило, більш схильні до втручання в право особи на повагу до приватного життя, оскільки вони розкривають більше

інформації про поведінку, думки або почуття особи (*«Узун проти Німеччини» (Uzun v. Germany)*, 2010, § 52).

53. Оскільки цей вид заходів слід вважати менш інвазивним для приватного життя суб'єкта даних, ніж прослуховування його телефонних розмов, суворі стандарти, встановлені й застосовані в контексті телефонних прослуховувань, не можуть бути автоматично застосовані до спостереження за пересуванням особи за допомогою GPS (*там само*, § 66). Щоб визначити, чи було надано в конкретній справі особі, яка піддавалася геолокаційним заходам за допомогою GPS, належний захист від свавільного втручання в її права за статтею 8, Суд застосовує загальні принципи перевірки передбачуваності закону (*там само*, § 66 і посилання, наведені в § 63). Видача ордера незалежним органом не завжди необхідна, а подальший судовий контроль за GPS-спостереженням може забезпечити достатній захист від свавілля (*там само*, § 72).

54. Встановлення пристрою геолокації в режимі реального часу на транспортному засобі особи в рамках кримінального розслідування незаконного обігу наркотиків було визнано порушенням статті 8 у випадку, коли національне законодавство (ні законодавчі акти, ні судова практика) на відповідний момент не регулювало достатньо чітко порядок і межі використання владою дискреційних повноважень у цій сфері (*«Бен Файза проти Франції» (Ben Faiza v. France)*, 2018, §§ 58-61).

55. Однак в іншій справі, де Суд розглядав питання щодо персональних даних, зібраних за допомогою геолокації, і їхнє використання у кримінальному провадженні, він не знайшов порушення статті 8 (*«Узун проти Німеччини» (Uzun v. Germany)*, 2010, §§ 60-74). Судовий контроль і можливість виключення доказів, отриманих за допомогою незаконного GPS-спостереження — це важлива гарантія, що запобігає використанню слідчими органами незаконних методів збору доказів (*там само*, § 72). При перевірці пропорційності втручання враховувалися такі обставини: що національне законодавство висувало дуже жорсткі вимоги для отримання дозволу на проведення оскаржуваного заходу спостереження; що GPS-спостереження дозволялося лише після того, як інші менш інвазивні методи розслідування виявилися неефективними; і що воно тривало відносно короткий період часу (*там само*, §§ 77-81).

56. У справі *«Флоріндо де Альмейда Васконселос Грамаксо проти Португалії» (Florindo de Almeida Vasconcelos Gramaxo v. Portugal)*, 2022, §§ 95-96 і 105-125, роботодавець заявника встановив систему GPS у службовому автомобілі заявника для моніторингу відстаней, подоланих під час його професійної діяльності й, за потреби, під час приватних поїздок. Суд зазначив, що система дозволяла відстежувати переміщення транспортного засобу в режимі реального часу, що дозволяло географічно визначити місцезнаходження особи, яка користувалася ним. На думку Суду ця інформація вважається персональними даними. Суд також підкреслив, що працівники не мали повноважень відключати систему GPS, тому вона залишалася активною цілодобово, сім днів на тиждень, в результаті чого спостереження було постійним і систематичним, що явно втручалася в приватне життя заявника. Водночас Суд зазначив, що національні суди ретельно збалансували право заявника на приватне життя з правом роботодавця забезпечувати ефективну роботу компанії, враховуючи законну мету контролю за витратами, яку ставила перед собою компанія. Тому Суд не встановив порушення положень статті 8 Конвенції.

vi. Фотографії

60. Право на захист свого зображення — одна з найважливіших складових особистого розвитку і передбачає право контролювати використання цього зображення (*«Реклос і Давурліс проти Греції» (Reklos and Davourlis v. Greece)*, 2009, §§ 40-43; *«Маргарі проти Греції» (Margari v. Greece)*, 2023, § 28; *«Глухін проти Росії» (Glukhin v. Russia)*, 2023, § 66). Окрім

випадків, коли особа свідомо або випадково дозволила себе сфотографувати в контексті діяльності, яка, ймовірно, буде публічно висвітлена або записана, ефективний захист зображення передбачає отримання згоди особи під час фотографування, а не тільки тоді, коли фотографію буде опубліковано (*«Реклос і Давурліс проти Греції» (Reklos and Davourlis v. Greece)*, 2009, §§ 37, 40). Однак цей принцип не абсолютний. Статус публічної особи або фігури, що має суспільний інтерес, за певних обставин може виправдовувати фіксацію зображення без згоди особи та його поширення².

57. У випадку заарештованих або обвинувачених осіб об'єктивна корисність фотографій, зроблених владою після затримання підозрюваного, може виправдовувати збереження таких фотографій «необхідним у демократичному суспільстві» для цілей боротьби зі злочинністю (*«Супруненко проти Росії» (Suprunenko v. Russia)* (ухв.), 2018, §§ 63-65). Сам факт фотографування підозрюваного та внесення його до бази даних не обов'язково тягне за собою клеймо підозри або провини (*там само*, § 64). У справі *«Мюррей проти Сполученого Королівства» (Murray v. the United Kingdom)* [ВП], 1994, §§ 92-93, фотографування і зберігання без згоди особи, підозрюваної у вчиненні терористичного злочину, не було визнане непропорційним законній меті запобігання тероризму, яка є законною метою в демократичному суспільстві. Компетентні органи не виходять за рамки законного процесу розслідування терористичних злочинів, коли записують і зберігають основні особисті дані заарештованої особи або навіть інших осіб, присутніх під час і в місці арешту (*там само*, § 93). Суд також визнав явно необґрунтованою скаргу щодо збереження в комп'ютерній системі Міністерства внутрішніх справ фотографії заявника, зробленої під час його затримання за підозрою у вчиненні злочину (*«Супруненко проти Росії» (Suprunenko v. Russia)* (ухв.), 2018, § 65). Навіть якщо зібрана таким чином і збережена на комп'ютері поліції інформація мала особистий характер, вона не може вважатися інтимною або конфіденційною (*там само*, § 64).

58. Суд, однак, встановив порушення статті 8 у випадках, коли поліція надавала пресі фотографії осіб, які були заарештовані або обвинувачені, без їхньої попередньої згоди (*«Сціацца проти Італії» (Sciacca v. Italy)*, 2005, §§ 29-31; *«Хужин та інші проти Росії» (Khuzhin and Others v. Russia)*, 2008, §§ 115-118; *«Маргарі проти Греції» (Margari v. Greece)*, 2023, §§ 54-60), коли поліція запрошувала телевізійну групу для незаконної зйомки заявника у відділенні поліції та трансляції відзнятого матеріалу (*«Тома проти Румунії» (Toma v. Romania)*, 2009, §§ 90-93; *«Хмель проти Росії» (Khmel v. Russia)*, 2013, § 41), коли Міністерство внутрішніх справ опублікувало на своєму вебсайті фотографії заявників, зроблені під час їхнього перебування під вартою в поліції, на яких їхня особа не була прихована (*«Д.Г. та інші проти Північної Македонії» (D.H. and Others v. North Macedonia)*, 2023, §§ 63-65), коли розміщення фотографії заявника на дошці оголошень розшукуваних осіб не відповідало закону (*«Гуїоргуї Ніколаїшвілі проти Грузії» (Giorgui Nikolaïshvili v. Georgia)*, 2009, §§ 129-131), або коли існуючі правила та процедури не відповідали вимогам «якості закону» (*«Негру проти Республіки Молдова» (Negru v. the Republic of Moldova)*, 2023, §§ 29-35).

59. На думку Суду, зберігання протягом необмеженого строку фотографії особи, підозрюваної у вчиненні правопорушення, яка не була визнана винною, несе більший ризик стигматизації, ніж зберігання даних про осіб, які були засуджені за вчинення правопорушення (*«С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom)* [ВП], 2008, § 122; *«Гоґран проти Сполученого Королівства» (Gaughran v. the United Kingdom)*, 2020, §§ 82-84). Тривалість періоду зберігання не обов'язково відіграє вирішальну роль при оцінці того, чи вийшла Держава за межі допустимої свободи розсуду при встановленні відповідного режиму

² Див. також [Посібник до статті 10 Конвенції \(свобода вираження поглядів\)](#) про публікацію фотографій у журналістських цілях.

зберігання персональних даних, радше цю функцію виконують наявність і функціонування певних гарантій (*там само*, § 88).

60. Технології розпізнавання та відображення обличчя, які сьогодні можуть застосовуватися до фотографій, стають усе більш складними, і національні суди повинні враховувати це при розгляді необхідності будь-якого втручання в право на повагу до приватного життя особи, фотографія якої була зроблена органами влади (*там само*, §§ 67-70; див. також використання поліцією технології розпізнавання обличчя для ідентифікації заявника за фотографіями, опублікованими на публічному каналі Telegram, «Глухін проти Росії» (*Glukhin v. Russia*), 2023, §§ 64-91).

61. У справі «Горран проти Сполученого Королівства» (*Gaughran v. the United Kingdom*), 2020, §§ 97-98, де органи влади прийняли рішення про безстрокове зберігання фотографії особи, засудженої за водіння в стані алкогольного сп'яніння, на додаток до його профілю ДНК і відбитків пальців, Суд встановив порушення статті 8. Приймаючи рішення про збереження персональних даних без урахування тяжкості правопорушення та за відсутності реальної можливості їх перегляду, органи влади не забезпечили справедливого балансу між конкуруючими публічними та приватними інтересами. Попри те, що Державі було надано дещо ширшу свободу розсуду щодо зберігання фотографій порівняно зі зберіганням профілів ДНК (*там само*, §§ 84, 96), цієї свободи розсуду було недостатньо для того, щоб зберігання таких даних було пропорційним за будь-яких обставин, зокрема, якщо не було відповідних гарантій або реальної можливості їх перегляду (*там само*, § 96).

62. У справі «П.Н. проти Німеччини» (*P.N. v. Germany*), 2020, §§ 76-91, Суд не встановив порушення статті 8 щодо збору поліцією, після відкриття нового кримінального провадження проти особи, яка була раніше засуджена, інформації, що ідентифікує особу, зокрема фотографій обличчя та тіла, особливо будь-яких татувань, разом з відбитками пальців і долонь. З огляду на відносно обмежену інтрузивність і тривалість збору ідентифікаційних даних, обмежений вплив зберігання даних на повсякденне життя заявника, видалення даних через п'ять років, а також той факт, що дані зберігалися в поліцейській базі даних, яка підлягала гарантіям та індивідуальному перегляду, оскаржуваний захід становив пропорційне втручання у право заявника на повагу до його приватного життя.

63. В іншому контексті, у справі «Реклос і Давурліс проти Греції» (*Reklos and Davourlis v. Greece*), 2009, §§ 41-43, Суд встановив порушення статті 8 на тій підставі, що фотографування новонародженої дитини в клініці та збереження фотографом фотографій у формі, що дозволяє ідентифікувати особу, з можливістю подальшого використання, відбулося проти волі батьків. Аналогічне порушення було встановлено у справах «Гайовський проти Словаччини» (*Hájovský v. Slovakia*), 2021, §§ 46-49, щодо публікації в пресі нерозмитих зображень заявниці, зроблених таємно під різними приводами, та «Володіна проти Росії» (*№ 2*) (*Volodina v. Russia (no. 2)*), 2021, § 68, яка стосувалася неспроможності влади захистити жінку від неодноразового кібернасилства з боку її чоловіка, який створив фальшиві профілі на її ім'я та опублікував її інтимні фотографії.

64. У справі «Вучина проти Хорватії» (*Vučina v. Croatia*) (ухв.), 2019, §§ 34-51, сам факт того, що ім'я, яке не належало заявниці, не маючи жодного негативного відтінку, було помилково вказано в підписі до фотографії в жіночому журналі, не може розглядатися як особливо істотне втручання в право суб'єкта даних на повагу до приватного життя такого суб'єкта.

65. У справі «Фон Ганновер проти Німеччини» (*№ 2*) (*Von Hannover v. Germany (no. 2)*) [ВП], 2012, §§ 114-126, відмова національних судів заборонити публікацію фотографії відомої пари, зробленої без їхнього відома, не становила порушення статті 8, оскільки національні суди ретельно урівноважили право видавничої компанії на свободу вираження поглядів, з одного боку, і право заявників на повагу до їхнього приватного життя, з іншого. При цьому вони надали принципового значення питанню, чи сприяли фотографії, розглянуті у світлі

супровідних статей, дебатам, що становлять загальний інтерес. Вони також розглянули обставини, за яких були зроблені фотографії.

70. У справі *«Кан проти Німеччини» (Kahn v. Germany)*, 2016, §§ 63-76, Суд не знайшов порушення статті 8, коли видавництво не зобов'язало сплатити жодної суми за порушення заборони на публікацію фотографій двох дітей колишнього воротаря німецької національної футбольної збірної. Суд роз'яснив, що зі статті 8 Конвенції неможливо вивести принцип, згідно з яким для ефективного захисту приватного життя особи наказ, що зобов'язує видавця виплатити певну суму за невиконання судової заборони на публікацію, буде достатнім лише в тому випадку, якщо ця сума буде виплачена потерпілій особі. Це справедливо за умови, що держава, користуючись своєю свободою розсуду, надає потерпілим сторонам інші потенційно ефективні засоби правового захисту, про які не можна сказати, що вони непропорційно обмежують можливості отримання відшкодування за передбачувані порушення (*там само*, § 75).

В. Два аспекти (негативний і позитивний) захисту даних

66. Хоча основною метою статті 8 Конвенції є захист осіб від свавільного втручання органів державної влади або приватних органів, яким держава делегувала відповідні повноваження, у їхнє право на повагу до приватного і сімейного життя, житла та кореспонденції, вона також може накладати на державу певні позитивні зобов'язання щодо забезпечення ефективного дотримання цих прав (*«Барбулеску проти Румунії» (Bărbulescu v. Romania)* [ВП], 2017, § 108).

67. Якщо захід, що втручається у захист персональних даних, вживається фізичною або юридичною особою виключно в приватному секторі, Суд розглядає справу з точки зору позитивних зобов'язань держави (*«Краксі проти Італії» (№ 2) (Craxi v. Italy (no. 2))*, 2003, §§ 68-76; *«Кьопке проти Німеччини» (Körpke v. Germany)* (ухв.), 2010; *«Алкая проти Туреччини» (Alkaya v. Turkey)*, 2012, § 32; *«Сьодерман проти Швеції» (Söderman v. Sweden)* [ВП], 2013, § 89; *«Барбулеску проти Румунії» (Bărbulescu v. Romania)* [ВП], 2017, § 111; *«Лопез Рібалда та інші проти Іспанії» (López Ribalda and Others v. Spain)* [ВП], 2019, § 111; *«Бутуруга проти Румунії» (Buturugă v. Romania)*, 2020, §§ 60-63; *«Володіна проти Росії» (№ 2) (Volodina v. Russia (no. 2))*, 2021, §§ 58-68; *«Флоріндо де Альмейда Васконселос Грамаксо проти Португалії» (Florindo de Almeida Vasconcelos Gramaxo v. Portugal)*, 2022, § 111; *«Тена Аррегуї проти Іспанії» (Tena Arregui v. Spain)*, 2024, § 35). Однак, якщо захід було вжито державним органом (*«Копленд проти Сполученого Королівства» (Copland v. the United Kingdom)*, 2007, § 39; *«Лібєрт проти Франції» (Libert v. France)*, 2018, § 41; *«Дрелон проти Франції» (Drelon v. France)*, 2022, § 85; *«Шєрр'єр проти Франції» (Cherrier v. France)*, 2024, § 57), приватним органом, якому держава делегувала свої зобов'язання (*«Вукота-Боїч проти Швейцарії» (Vukota-Bojić v. Switzerland)*, 2016, § 47), або приватним органом, що діє відповідно до вимог закону (*«Подчасов проти Росії» (Podchasov v. Russia)*, 2024, § 52), Суд розглядатиме справу з точки зору негативного зобов'язання держави. Суд повинен буде перевірити, чи відповідає втручання вимогам пункту 2 статті 8, а саме, чи було воно здійснене відповідно до закону, переслідувало законну мету і було необхідним у демократичному суспільстві. Це питання буде розглянуто детальніше в частині цього посібника, присвяченій триступеневому тесту захисту даних.

68. У справі *«Вукота-Боїч проти Швейцарії» (Vukota-Bojić v. Switzerland)*, 2016, § 47, Суд наголосив, що держава не може звільнити себе від відповідальності за Конвенцією, делегуючи свої зобов'язання приватним органам або особам. З огляду на те, що приватна страхова компанія, яка збирала та зберігала персональні дані, керувала державною системою страхування і розглядалася національним режимом як орган державної влади, компанія повинна була розглядатися як державний орган, а її дії повинні були бути поставлені в провину державі-відповідачу (*там само*, § 47).

69. У справі *«Лібєрт проти Франції» (Libert v. France)*, 2018, §§ 37-41, Суд відхилив заперечення уряду про те, що Національна залізнична компанія (SNCF), роботодавець заявника, якого звинуватили у відкритті особистих файлів на робочому комп'ютері, не може розглядатися як орган державної влади для цілей статті 8. Хоча співробітники працювали в приватних компаніях, компанія була юридичною особою публічного права, перебувала під наглядом Держави і мала призначених Державою директорів, а отже, користувалася непрямыми державними гарантіями.

70. У справі, що стосувалася спостереження за телефонними дзвінками, електронною поштою та інтернет-з'єднанням працівника школи, Суд дійшов висновку, що питання, яке підлягало аналізу, стосувалося негативного зобов'язання Держави не втручатися у приватне життя і кореспонденцію заявника, оскільки школа була державним органом, за дії якого для цілей Конвенції був відповідальним уряд (*«Копленд проти Сполученого Королівства» (Copland v. the United Kingdom)*, 2007, § 39).

71. У справі *«Лібшер проти Австрії» (Liebscher v. Austria)*, 2021, заявник скаржився на обов'язок надати весь договір про розлучення (а не його витяг) для того, щоб його частка нерухомості була передана його колишній дружині. Інформація, що містилася в угоді про розлучення, включала імена та місця проживання його неповнолітніх дітей та колишньої дружини, розмір аліментів, угоди про опіку, угоди про поділ майна (окрім нерухомості), а також перелік його доходів та активів. Передача майна, а отже, і всі підтверджувальні документи, включаючи рішення про розірвання шлюбу, були б зареєстровані в земельному кадастрі, відкритому для громадськості, з яким може без обмежень ознайомитися будь-яка третя особа. Суд підійшов до розгляду справи з точки зору позитивного зобов'язання Держави вжити заходів, спрямованих на забезпечення поваги до приватного життя, включаючи як створення нормативно-правової бази, так і здійснення, у разі необхідності, конкретних заходів (*там само*, §§ 60-61).

72. Хоча межі між позитивними та негативними зобов'язаннями Держави за Конвенцією не піддаються точному визначенню, застосовні принципи все ж схожі. В обох контекстах слід звернути увагу, зокрема на справедливий баланс, який має бути досягнутий між конкурентними інтересами окремої особи та спільноти в цілому, у будь-якому разі підпорядковуючись свободі розсуду, якою користується Держава (*«Барбулеску проти Румунії» (Bărbulescu v. Romania)* [ВП], 2017, § 112; *«Тена Арреґуї проти Іспанії» (Tena Arregui v. Spain)*, 2024, § 32).

73. У справах, що стосуються захисту персональних даних, Суд встановив, що свобода розсуду Держави є ширшою в таких випадках: коли в Державах-членах Ради Європи немає консенсусу щодо важливості інтересу, про який йдеться, або найкращих засобів його захисту (*«Одієвре проти Франції» (Odièvre v. France)* [ВП], 2003, § 47; *«Бреєр проти Німеччини» (Breyer v. Germany)*, 2020, § 108; *«Говен-Фурні і Сілію проти Франції» (Gauvin-Fournis and Silliau v. France)*, 2023, § 111); коли суто фінансові дані не були тісно пов'язані з особою заявника (*«Г.С.Б. проти Швейцарії» (G.S.B. v. Switzerland)*, 2015, § 93); і, нарешті, у справах, пов'язаних із національною безпекою (*«Леандер проти Швеції» (Leander v. Sweden)*, 1987, § 59). На противагу цьому, свобода розсуду, надана національним органам влади, була визнана вужчою, коли, наприклад, персональні дані, що підлягають автоматизованій обробці, яка значно полегшує доступ до них та їх поширення, можуть завдати шкоди репутації особи та ускладнити її повсякденне життя (*«Хелілі проти Швейцарії» (Khelili v. Switzerland)*, 2011, §§ 64, 70). Це ж міркування особливо актуальне для захисту категорій конфіденційних даних, зокрема інформації про ДНК, яка містить генетичну інформацію про особу і має велике значення як для самої особи, так і для її сім'ї (*«С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom)* [ВП], 2008, §§ 102-103).

74. Невід'ємні позитивні зобов'язання щодо забезпечення ефективного захисту прав і свобод, передбачених Конвенцією, можуть включати, наприклад, зобов'язання забезпечити особі доступ протягом розумного строку до інформації, яка систематично зберігається про неї колишніми державними секретними службами стосовно її далекого минулого («*Гараламбіє проти Румунії*» (*Haralambie v. Romania*), 2009, § 79; «*Йарнеа проти Румунії*» (*Jarneea v. Romania*), 2011, § 50; «*Йоанна Шульц проти Польщі*» (*Joanna Szulc v. Poland*), 2012, § 87); забезпечити «ефективну та доступну процедуру», що дозволяє зацікавленій стороні мати доступ до «всієї відповідної та належної інформації», зібраної та збереженої органами державної влади, з метою отримання інформації, необхідної для знання та розуміння дитинства та раннього розвитку особи («*Гаскін проти Сполученого Королівства*» (*Gaskin v. the United Kingdom*), 1989, § 49), з'ясувати її особу («*Одієвре проти Франції*» (*Odièvre v. France*) [ВП], 2003, § 42; «*Говен-Фурні і Сілію проти Франції*» (*Gauvin-Fournis and Silliau v. France*), 2023, § 110), або виявити будь-які ризики для здоров'я, на які наражалася особа («*Гуерра та інші проти Італії*» (*Guerra and Others v. Italy*), 1998, § 60; «*Мак'їнлі та Еган проти Сполученого Королівства*» (*McGinley and Egan v. the United Kingdom*), 1998, § 101; «*Роше проти Сполученого Королівства*» (*Roche v. the United Kingdom*) [ВП], 2005, § 162).

80. Суд, однак, вважає, що такі позитивні зобов'язання не покладаються на національні органи влади в контексті чутливих розвідувальних даних національної безпеки, зібраних владою про особу («*Леандер проти Швеції*» (*Leander v. Sweden*), 1987, § 51).

75. У справі «*Котілайнен та інші проти Фінляндії*» (*Kotilainen and Others v. Finland*), 2020, § 83, щодо стрілянини в школі, Суд дійшов висновку, що позитивне зобов'язання влади захищати життя родичів заявників не поширюється, відповідно до матеріальної частини статті 2, на зобов'язання поліції отримати перед стріляниною медичну та військову справи правопорушника для перевірки даних про його психічний стан. Доступ поліції до медичних даних особи не може бути рутинним і повинен відповідати конкретним вимогам необхідності та обґрунтованості.

76. За певних обставин, коли постає питання про персональні дані, наприклад, у контексті особливо тяжких злочинів, вчинених між окремими особами, ефективне здійснення прав, передбачених Конвенцією, вимагає від Держави прийняття спеціального законодавства для захисту цих прав. Так у справі «*Сьодерман проти Швеції*» (*Söderman v. Sweden*) [ВП], 2013, §§ 86-117, Суд встановив порушення статті 8 з огляду на відсутність чітких законодавчих положень, що означало, що ізольований акт прихованої або несанкціонованої зйомки / фотографування оголеної дитини залишився безкарним — прогалина в законодавстві, яка на той час не була компенсована іншими положеннями кримінального права, а також з огляду на неефективність засобів цивільного захисту (*там само*, §§ 108-114). Аналогічно у справі «*К.У. проти Фінляндії*» (*K.U. v. Finland*), 2008, §§ 49-50, було встановлено порушення статті 8 через відсутність правової бази, яка б дозволила владі зобов'язати провайдера послуг доступу до інтернету розкрити особу, яка розшукувалася за розміщення непристойного оголошення щодо неповнолітньої особи на сайті знайомств. Законодавча влада повинна забезпечити основу для узгодження різних вимог, які конкурують за захист у цьому контексті. Справа «*Хадіджа Ісмаїлова проти Азербайджану*» (*Khadija Ismayilova v. Azerbaijan*), 2019, §§ 105-132, стосувалася прихованої зйомки журналістки в її будинку та публічного розповсюдження відеозаписів. У цій справі ці дії каралися кримінальним законодавством, і було відкрито кримінальне розслідування. Однак, Суд встановив, що органи влади не виконали свого позитивного зобов'язання щодо забезпечення достатнього захисту приватного життя заявниці шляхом проведення ефективного кримінального розслідування дуже серйозного втручання в її приватне життя (*там само*, §§ 119-131). Справа «*Володіна проти Росії*» (*№ 2*) (*Volodina v. Russia (no. 2)*), 2021, § 68, стосувалася скарги заявниці на те, що органи влади не змогли захистити її від неодноразового кібернасилства з боку її співмешканця, який створив фальшиві профілі від її імені, опублікував її інтимні фотографії, стежив за її пересуваннями та надсилав їй

погрози смерті через соціальні мережі. Суд встановив, зокрема, що, попри наявність правових інструментів для притягнення партнера заявниці до відповідальності, органи влади не провели ефективного розслідування і жодного разу не передбачили вжиття належних заходів для її захисту. Таким чином, вони не виконали свого обов'язку щодо її захисту від серйозного насильства.

77. Що стосується менш серйозних дій між фізичними особами, таких як спостереження за працівниками на робочому місці, Держави можуть вирішувати, чи варто приймати спеціальне законодавство щодо відеоспостереження (*«Лопез Рібалда та інші проти Іспанії» (López Ribalda and Others v. Spain)* [ВП], 2019, § 113; *«Кьопке проти Німеччини» (Körpke v. Germany)* (ухв.), 2010) або моніторингу непрофесійної кореспонденції та комунікацій працівників (*«Барбулеску проти Румунії» (Bărbulescu v. Romania)* [ВП], 2017, § 119). Однак національні суди повинні забезпечити, щоб будь-яке запровадження роботодавцем заходів спостереження, що втручаються в право працівників на повагу до їхнього приватного життя або кореспонденції, було пропорційним і супроводжувалося належними та достатніми гарантіями проти зловживань (*«Кьопке проти Німеччини» (Körpke v. Germany)* (ухв.), 2010; *«Барбулеску проти Румунії» (Bărbulescu v. Romania)* [ВП], 2017, § 120; *«Лопез Рібалда та інші проти Іспанії» (López Ribalda and Others v. Spain)* [ВП], 2019, § 116; див. також у контексті моніторингу електронної кореспонденції політичною партією своїх членів, *«Тена Аррегуї проти Іспанії» (Tena Arregui v. Spain)*, 2024, § 38).

78. В інших справах, що стосуються розголошення персональних даних, Суд встановив, що Держава має позитивний обов'язок розслідувати передбачувані порушення статті 8, незалежно від того, чи були вони вчинені приватними особами або органами державної влади. Так у справі *«Краксі проти Італії» (№ 2) (Craxi v. Italy (no. 2))*, 2003, §§ 68-76, яка стосувалася зачитування в суді та оприлюднення в пресі розшифровок телефонних розмов політика, перехоплених у межах кримінального провадження у справі про корупцію, Суд дійшов висновку, що органи влади мають позитивне зобов'язання запобігати оприлюдненню приватних розмов у публічному просторі. Оскільки розголошення розмов у пресі не було прямим наслідком дій прокурора, а, ймовірно, спричинене збоєм у роботі секретаріату національного суду, Суд встановив порушення статті 8, адже органи влади не вжили необхідних заходів для забезпечення ефективного захисту прав заявника через надання належних гарантій та проведення ефективного розслідування.

79. У справі *«Алкая проти Туреччини» (Alkaya v. Turkey)*, 2012, §§ 30-40, Суд дійшов висновку, що захист, наданий національними органами влади щодо особистої інформації відомої акторки, повна адреса якої була розкрита в газеті, був недостатнім. Не знайшовши жодних доказів, які могли б виправдати з міркувань суспільного інтересу рішення газети розкрити її адресу, Суд зазначив, що національні суди, вочевидь, не взяли до уваги можливі наслідки для життя заявниці через публікацію її домашньої адреси в газеті. Така нездатність національних судів оцінити конкуруючі інтереси не може розглядатися як виконання державою позитивних зобов'язань за статтею 8.

80. У контексті домашнього насильства, у справі *«Бутуруга проти Румунії» (Buturugă v. Romania)*, 2020, §§ 73-78, де колишній чоловік заявниці зловживав її електронними акаунтами, включаючи Facebook, і робив копії її приватних розмов, документів і фотографій, Суд встановив, що органи влади були зобов'язані розслідувати порушення конфіденційності її кореспонденції. Суд визнав, що кібербулінг — один з аспектів насильства щодо жінок і дівчат, і що він може набувати різних форм, включаючи порушення недоторканності приватного життя, злом комп'ютера жертви, викрадення, поширення та маніпулювання даними й зображеннями, включаючи інтимні подробиці. Суд також погодився, що такі дії, як неналежний моніторинг, доступ і збереження кореспонденції подружжя, можуть бути враховані національними органами влади при розслідуванні справ про домашнє насильство. Ствердження про порушення конфіденційності кореспонденції вимагало від органів влади проведення перевірки

по суті, щоб отримати всебічне уявлення про всі можливі форми домашнього насильства (*там само*, §§ 76-77). Оскільки така перевірка не була проведена, було встановлено порушення статті 8 (див. також, у схожому контексті, *«Володіна проти Росії» (№ 2) (Volodina v. Russia (no. 2))*, 2021, §§ 48-68).

С. Триступеневий тест захисту даних

81. Пункт 2 статті 8 визначає умови, за яких може мати місце втручання у користування захищеним правом: таке втручання має здійснюватися «відповідно до закону», переслідувати «законну мету» і бути «необхідним у демократичному суспільстві».

1. Чи було втручання законним

82. У низці справ Суд розглядав питання щодо того, чи була дотримана вимога статті 5 Конвенції 108, яка встановлює, що персональні дані, які піддаються автоматизованій обробці, повинні бути отримані та оброблені справедливим і законним шляхом. У низці справ Суд встановив порушення статті 8 виключно через відсутність правової бази на національному рівні для санкціонування заходів, що втручаються в відповідні права (*«Тейлор-Саборі проти Сполученого Королівства» (Taylor-Sabori v. the United Kingdom)*, 2002, §§ 17-19; *«Раду проти Молдови» (Radu v. Moldova)*, 2014, § 31; *«Моккуте проти Литви» (Mockutė v. Lithuania)*, 2018, §§ 103-104; *«М.Д. та інші проти Іспанії» (M.D. and Others v. Spain)*, 2022, §§ 61-64; *«Качмарек проти Польщі» (Kaczmarek v. Poland)*, 2024, §§ 74-80).

83. Зокрема, у справі *«Моккуте проти Литви» (Mockutė v. Lithuania)*, 2018 (§§ 103-104), Суд зазначив, що ні Уряд, ні національні суди не вказали жодного положення, яке могло б стати правовою підставою для передачі психіатричною лікарнею інформації про стан здоров'я заявниці, яка була повнолітньою, її матері та журналістам. У справі *«Тейлор-Саборі проти Сполученого Королівства» (Taylor-Sabori v. the United Kingdom)*, 2002 (§§ 17-19), де заявник був підданий поліцейському нагляду шляхом «клонування» його пейджера, не існувало законодавчої системи, яка б регулювала перехоплення повідомлень пейджера, переданих через приватну телекомунікаційну систему. У справі *«Раду проти Республіки Молдова» (Radu v. Republic of Moldova)*, 2014 (§ 31), поширення державною лікарнею медичної інформації про вагітність, стан здоров'я та лікування заявниці її роботодавцем не було «відповідним до закону». У справі *«М.Д. та інші проти Іспанії» (M.D. and Others v. Spain)*, 2022 (§§ 61-64) поліція складала протокол стосовно суддів і магістратів, які виконували свої функції в Каталонії та підписали маніфест із юридичною думкою щодо так званого «права вирішувати» каталонців. У протоколі були розкриті особисті дані, фотографії, професійна інформація та політичні погляди деяких з них. Суд зазначив, що складання поліцейського протоколу не було передбачено законом, і оскільки органи державної влади використовували персональні дані з іншою метою, ніж та, яка виправдовувала їх збір, сама наявність поліцейського протоколу щодо осіб, поведінка яких не передбачала жодної злочинної діяльності, становила порушення статті 8 Конвенції. У справі *«Качмарек проти Польщі» (Kaczmarek v. Poland)*, 2024 (§§ 74-80), де запис телефонної розмови заявника було оприлюднено на пресконференції, Суд встановив, що відповідне положення кримінального процесуального закону, яке в основному стосувалося ознайомлення з матеріалами справи та зняття копій під час розслідування, не може розглядатися як правова підстава для такого розголошення.

90. В інших справах Суд встановив порушення статті 8 на тій підставі, що національне законодавство, яке повинно було захищати персональні дані, було недоступним або конфіденційним (*«Василь Васильєв проти Болгарії» (Vasil Vasilev v. Bulgaria)*, 2021, §§ 169-170; *«Нух Узун та інші проти Туреччини» (Nuh Uzun and Others v. Turkey)*, 2022, §§ 80-99) або не було достатньо чітким і передбачуваним (*«Вукота-Боїч проти Швейцарії» (Vukota-Bojić v. Switzerland)*, 2016; *«Бен Файза проти Франції» (Ben Faiza v. France)*, 2018, §§ 58-61; *«Бенедік*

проти Словенії» (Benedik v. Slovenia), 2018; *«Ротару проти Румунії» (Rotaru v. Romania)* [ВП], 2000; *«Золтан Варга проти Словаччини» (Zoltán Varga v. Slovakia)*, 2021, § 162; *«Гашчак проти Словаччини» (Haščák v. Slovakia)*, 2022, §§ 94-95; *«Качмарек проти Польщі» (Kaczmarek v. Poland)*, 2024, §§ 93-96). Так, у справі *«Нух Узун та інші проти Туреччини» (Nuh Uzun and Others v. Turkey)*, 2022, §§ 80-99, кореспонденція ув'язнених була відсканована та завантажена на сервер Національної судової мережі на підставі інструкцій, виданих Міністерством юстиції, які були адресовані прокурорам та адміністрації в'язниць. Ці інструкції не були доступні для громадськості в цілому та для заявників зокрема. У справі *«Вукота-Боїч проти Швейцарії» (Vukota-Bojić v. Switzerland)*, 2016, §§ 71-77, положення, на яких ґрунтувалося негласне спостереження, якому була піддана заявниця після дорожньо-транспортної пригоди страховою компанією, не вказували з достатньою чіткістю на обсяг і спосіб здійснення дискреційних повноважень, наданих страховим компаніям, які діють як органи державної влади в страхових спорах, для проведення негласного спостереження за застрахованими особами. У справі *«Ротару проти Румунії» (Rotaru v. Romania)* [ВП], 2000 (§§ 57-62), що стосувалася особистої інформації, яка зберігалася румунською розвідувальною службою, національне законодавство не визначало тип інформації, яка могла оброблятися, категорії осіб, щодо яких могли вживатися заходи спостереження, і за яких обставин, а також процедуру, якої слід було дотримуватися. У справі *«Бенедік проти Словенії» (Benedik v. Slovenia)*, 2018 (§ 132), певні правові положення, використані поліцією для отримання даних про абонента, пов'язаних з динамічною IP-адресою, були недостатньо чіткими і не забезпечували захисту від свавільного втручання, оскільки не існувало жодних гарантій проти зловживань або незалежного моніторингу відповідних повноважень поліції. Аналогічно у справі *«Качмарек проти Польщі» (Kaczmarek v. Poland)*, 2024 (§§ 93-96) тривале зберігання органами влади матеріалів спостереження за заявницею, зібраних під час операції з гарантування безпеки, суб'єктом якої вона сама не була, ґрунтувалося на законодавчих положеннях, яким бракувало достатньої чіткості і які не передбачали жодних процесуальних гарантій. В результаті цього заявниця не змогла домогтися знищення цих матеріалів.

84. На противагу цьому, в інших справах Суд не встановив порушення статті 8 після того, як з'ясував, що національне законодавство було чітким і передбачуваним, і надавало достатні гарантії проти потенційних зловживань (*«Сатакуннан Марккінапорссі Ой та Сатамедіа Ой проти Фінляндії» (Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland)* [ВП], 2017, § 154; *«Бен Файза проти Франції» (Ben Faiza v. France)*, 2018, § 75). У справі *«Бен Файза проти Франції» (Ben Faiza v. France)*, 2018 (§§ 70-76), рішення суду, використане для отримання від оператора мобільного зв'язку персональної інформації про заявника, яка не стосувалася змісту дзвінків, було ухвалене «відповідно до закону». Такі судові рішення були санкціоновані та регулювалися відповідною законодавчою базою. Також існували гарантії проти свавілля, оскільки такі рішення мали бути попередньо санкціоновані прокурором під загрозою їх недійсності та підлягали судовому контролю, а отримана інформація могла бути виключена з доказів у разі будь-якої незаконності (*там само*, § 73).

85. Аналогічного висновку Суд дійшов у справі *«Сатакуннан Марккінапорссі Ой та Сатамедіа Ой проти Фінляндії» (Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland)* [ВП], 2017 (§ 154), що стосувалася рішення Ради з питань захисту даних, підтриманого судами, яке забороняло широку публікацію податкових даних. Формулювання відповідного законодавства про захист даних і спосіб його застосування відповідно до вказівок, наданих фінським судам Судом справедливості Європейського Союзу (СЕС), були достатньо передбачуваними. Хоча ця справа була першою у своєму роді відповідно до Закону про персональні дані, а Вищий адміністративний суд звернувся до Суду справедливості ЄС за тлумаченням відступу від положень Директиви про захист даних, це не зробило тлумачення та застосування національними судами журналістського відступу від положень свавільним або непередбачуваним (*там само*, § 150). Оскільки компанії-заявники були працівниками засобів масової інформації, вони повинні були усвідомлювати можливість того, що масовий збір даних

та їх масове поширення не можуть розглядатися як обробка «виключно» в журналістських цілях згідно з відповідними положеннями законодавства Фінляндії та права ЄС (*там само*, § 151).

86. Нарешті, в інших справах Суд встановив, що вимога втручання «відповідно до закону» настільки тісно пов'язана з критерієм «необхідності в демократичному суспільстві», що ці дві умови необхідно розглядати разом (*«С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom)* [ВП], 2008, § 99; *«Квасніца проти Словаччини» (Kvasnica v. Slovakia)*, 2009, § 84; *«Кеннеді проти Сполученого Королівства» (Kennedy v. the United Kingdom)*, 2010, § 155; *«Глухін проти Росії» (Glukhin v. Russia)*, 2023, § 78).

87. У конкретному контексті заходів негласного спостереження, таких як перехоплення повідомлень, Суд встановив, що «передбачуваність» не можна розуміти так само, як у багатьох інших сферах. На його думку, це не може означати, що особа повинна мати можливість передбачити, коли органи влади можуть вдатися до таких заходів, щоб вона могла відповідно адаптувати свою поведінку (*«Адомайтіс проти Литви» (Adomaitis v. Lithuania)*, 2022, § 83; див. також *«Сарбу проти Румунії» (Sârbu v. Romania)*, 2023, § 51, де ті ж принципи були застосовані в контексті прихованого відеозапису, зробленого приватною особою). Проте, особливо коли повноваження, покладені на виконавчі органи, здійснюються таємно, очевидним є ризик свавілля. Тому важливо мати чіткі, детальні правила щодо заходів негласного спостереження, особливо з огляду на те, що технології, доступні для використання, постійно стають усе більш досконалими. Національне законодавство має бути достатньо чітким, щоб дати громадянам адекватне уявлення про обставини та умови, за яких органи державної влади мають право вдаватися до будь-яких таких заходів (*«Мелон проти Сполученого Королівства» (Malone v. the United Kingdom)*, 1984, § 67; *«Леандер проти Швеції» (Leander v. Sweden)*, 1987, § 51; *«Валензуела Контрерас проти Іспанії» (Valenzuela Contreras v. Spain)*, 1998, § 46; *«Вебер і Саравія проти Німеччини» (Weber and Saravia v. Germany)* (ухв.), 2006, § 93; *«Асоціація за європейську інтеграцію і права людини та Екімджієв проти Болгарії» (Association for European Integration and Human Rights and Ekimdjiev v. Bulgaria)*, 2007, § 75; *«Роман Захаров проти Росії» (Roman Zakharov v. Russia)* [ВП], 2015, § 229). Крім того, закон повинен визначати обсяг будь-якого такого розсуду, наданого компетентним органам, і спосіб його здійснення з достатньою чіткістю, щоб забезпечити особі належний захист від свавільного втручання (*«Роман Захаров проти Росії» (Roman Zakharov v. Russia)* [ВП], 2015, § 230).

88. У своїй судовій практиці щодо перехоплення повідомлень у контексті кримінальних розслідувань Суд визначив, що для запобігання зловживанню владою закон повинен містити щонайменше шість таких елементів: характер правопорушень, які можуть стати підставою для видачі ордера на перехоплення; визначення категорій осіб, чиї комунікації можуть бути перехоплені; часові рамки здійснення заходу; порядок, якого слід дотримуватися для вивчення, використання та зберігання зібраних даних; запобіжні заходи, яких слід вжити для передачі даних іншим сторонам; обставини, за яких перехоплені дані можуть або повинні бути видалені або знищені (*«Гувіг проти Франції» (Huvig v. France)*, 1990, § 34; *«Валензуела Контрерас проти Іспанії» (Valenzuela Contreras v. Spain)*, 1998, § 46; *«Вебер і Саравія проти Німеччини» (Weber and Saravia v. Germany)* (ухв.), 2006, § 95; *«Асоціація за європейську інтеграцію і права людини та Екімджієв проти Болгарії» (Association for European Integration and Human Rights and Ekimdjiev v. Bulgaria)*, 2007, § 76). У справі *«Роман Захаров проти Росії» (Roman Zakharov v. Russia)* [ВП], 2015 (§ 238), Суд підтвердив, що ці ж мінімальні гарантії застосовуються і у випадках, коли перехоплення було здійснено з міркувань національної безпеки. Однак, щоб визначити, чи несумісне зі статтею 8 оскаржуване законодавство, Суд також взяв до уваги такі фактори: механізми нагляду за здійсненням заходів таємного

спостереження, будь-які механізми повідомлення та засоби правового захисту, передбачені національним законодавством³.

89. У контексті персональних даних, що збираються органами влади та зберігаються в базах даних для цілей, пов'язаних із запобіганням злочинам або покаранням за них, Суд вказав на важливість наявності чітких, детальних правил, що регулюють обсяг і застосування таких заходів, а також мінімальних гарантій, що стосуються, зокрема, тривалості, зберігання, використання, доступу третіх осіб, процедур збереження цілісності та конфіденційності даних і процедур їх знищення, забезпечуючи, таким чином, достатні гарантії від ризику зловживань і свавілля («*C. і Марпер проти Сполученого Королівства*» (*S. and Marper v. the United Kingdom*) [ВП], 2008, §§ 99, 103; «*Нух Узун та інші проти Туреччини*» (*Nuh Uzun and Others v. Turkey*), 2022, § 86). Суд встановив порушення статті 8 у випадках, коли національне законодавство не вказувало з достатньою чіткістю на обсяг і спосіб здійснення дискреційних повноважень, наданих національним органам влади («*Шимоволос проти Росії*» (*Shimovolos v. Russia*), 2011, § 70; «*Дімітров-Казаків проти Болгарії*» (*Dimitrov-Kazakov v. Bulgaria*), 2011, § 33; «*Негру проти Республіки Молдова*» (*Negru v. the Republic of Moldova*), 2023, § 34). У справі «*Шимоволос проти Росії*» (*Shimovolos v. Russia*), 2011 (§ 69), створення і ведення бази даних спостереження, що зберігає персональні дані, в тому числі про пересування правозахисника, а також порядок її функціонування регулювалися міністерським наказом, який ніколи не був опублікований або іншим чином доступний для громадськості. У справі «*Дімітров-Казаків проти Болгарії*» (*Dimitrov-Kazakov v. Bulgaria*), 2011 (§ 33), реєстрація особи як «правопорушника» в поліцейських реєстрах ґрунтувалася на непублічній інструкції, яка на той час мала конфіденційний характер і була призначена, до її подальшого розсекречення, для внутрішнього використання в Міністерстві внутрішніх справ. У справі «*Негру проти Республіки Молдова*» (*Negru v. the Republic of Moldova*), 2023 (§ 24), заявницю було включено до списку розшукуваних осіб, що передбачало обробку її персональних даних у національній інтегрованій автоматизованій інформаційній системі обліку правопорушень, кримінальних справ і правопорушників, а її фотографію було розміщено в громадських приміщеннях поліцейської дільниці на підставі рішення прокурора, яке було прийнято в рамках недостатньо чітких процедур, в результаті чого розсуд прокурора вважався практично необмеженою владою.

90. У справі «*Кетт проти Сполученого Королівства*» (*Catt v. the United Kingdom*), 2019 (§§ 97, 106), Суд підкреслив ризик неоднозначності правової бази, що використовується органами влади для збору та зберігання персональних даних, що впливає з нечітко визначених понять у національному законодавстві.

91. У контексті впровадження технології розпізнавання обличчя Суд зазначив, що для дотримання вимоги «якості закону» необхідно мати детальні правила, що регулюють обсяг і застосування заходів, а також надійні гарантії проти ризику зловживань і свавілля. Потреба в гарантіях буде ще більшою, коли йдеться про використання технології розпізнавання обличчя в реальному часі («*Глухін проти Росії*» (*Glukhin v. Russia*), 2023, § 82). У цій справі Суд вперше звернувся до питання використання такої технології і висловив серйозні сумніви в тому, що положення національного законодавства, які дозволяли обробку біометричних персональних даних, у тому числі за допомогою технології розпізнавання обличчя, «у зв'язку зі здійсненням правосуддя», відповідали вимозі «якості закону», оскільки були сформульовані широко і, як видається, дозволяли обробку таких даних у зв'язку з будь-яким видом судочинства. Національне законодавство не містило жодних обмежень щодо характеру ситуацій, які можуть

³ Див. також [Посібник зі статті 8 Конвенції \(право на повагу до приватного і сімейного життя\)](#) про вимогу передбачуваності закону в питаннях перехоплення повідомлень, прослуховування телефонних розмов і прихованого спостереження.

призвести до використання технології розпізнавання обличчя, цілей, категорій осіб, які можуть бути об'єктом розпізнавання, або щодо обробки конфіденційних персональних даних. Крім того, як видається, не існує жодних процедурних гарантій, що супроводжують використання технології розпізнавання обличчя, таких як процедури авторизації, процедури, яких слід дотримуватися для вивчення, використання та зберігання отриманих даних, механізми наглядового контролю або доступні засоби правового захисту (*там само*, § 83).

2. Чи переслідувало втручання закону мету

92. У низці справ Суд розглядав питання про те, чи була дотримана вимога статті 5 Конвенції 108 про те, що персональні дані, які піддаються автоматизованій обробці, повинні збиратися для чітких, визначених і законних цілей. У цих справах розгляд законних цілей, які можуть виправдати втручання у здійснення прав, передбачених статтею 8, перелічених у пункті 2, є досить стислим. Ці цілі: захист національної безпеки, суспільної безпеки та економічного добробуту Держави, запобігання заворушенням і злочинам, захист здоров'я чи моралі або захист прав і свобод інших осіб. Суд, як правило, підтверджує наявність однієї або декількох з цих законних цілей, на які посилається Уряд.

100. Наприклад, Суд вважав, що зберігання в таємному реєстрі поліції даних про приватне життя осіб, а потім використання цих даних при перевірці кандидатів на посади, важливі для національної безпеки, переслідувало законну мету для цілей статті 8, а саме — захист національної безпеки («*Леандер проти Швеції*» (*Leander v. Sweden*), 1987, § 49). Спостереження за заявником за допомогою GPS, яке було призначене прокурором для розслідування кількох замахів на вбивство, відповідальність за які взяв на себе терористичний рух, і для запобігання подальшим вибухам, на думку Суду, слугувало інтересам національної та громадської безпеки, запобігання злочинам і захисту прав жертв («*Узун проти Німеччини*» (*Uzun v. Germany*), 2010, § 77).

93. Суд також встановив, що передача банківських даних органам влади іншої Держави за двосторонньою угодою переслідувала законну мету, оскільки цей захід слугував захисту економічного добробуту країни («*Г.С.Б. проти Швейцарії*» (*G.S.B. v. Switzerland*), 2015, § 83). З огляду на те, що банківський сектор — важлива галузь економіки для Держави-відповідача, оскаржуваний захід, який був частиною комплексних зусиль уряду Швейцарії, спрямованих на врегулювання конфлікту між банком (описаним як «великий гравець у швейцарській економіці, який працевлаштовує велику кількість людей») і податковими органами США, можна обґрунтовано вважати таким, що сприяє захисту економічного добробуту країни (*там само*, § 83).

94. Посилаючись на міжнародні документи, згідно з якими справедливість і рівність можливостей є основоположними для боротьби з допінгом, Суд встановив, що захист здоров'я і моралі виправдовує обов'язок встановлювати місцезнаходження спортсменів з огляду на необхідність боротьби з допінгом у спорті («*Національна федерація асоціацій і спілок спортсменів та інші проти Франції*» (*National Federation of Sportspersons' Associations and Unions (FNASS) and Others v. France*), 2018, §§ 164-166). На думку Суду, те, що уряд назвав «мораллю» в контексті зусиль, спрямованих на забезпечення рівної та змістовної конкуренції у спорті, також пов'язане із законною метою «захисту прав і свобод інших осіб», оскільки використання допінгових засобів з метою отримання переваги над іншими спортсменами — це небезпечне підбурювання спортсменів-аматорів, зокрема молоді, наслідувати їхній приклад з метою покращення своїх результатів. Також це позбавляє глядачів чесною конкуренції, на яку вони мають право розраховувати (*там само*, § 166).

95. У справі «*Бен Файза проти Франції*» (*Ben Faiza v. France*), 2018 (§ 77), Суд встановив, що судові рішення на отримання від оператора мобільного зв'язку особистої інформації про заявника, яка не стосувалася змісту дзвінків, був спрямований на встановлення істини в

контексті кримінального провадження щодо імпорту наркотиків у складі організованої банди, злочинної змови та відмивання грошей. Таким чином, цей захід переслідував законні цілі запобігання заворушенням чи злочинам або захисту громадського здоров'я.

96. Перехоплення телефонних розмов заявника, директора в'язниці, який підозрювався в корупції, зберігання цієї інформації та її розголошення під час дисциплінарного провадження, що зрештою призвело до його звільнення, було визнано спрямованим на запобігання діям корупційного характеру та гарантування прозорості й відкритості державної служби. Отже, це переслідувало законні цілі запобігання заворушенням чи злочинам, а також захисту прав і свобод інших осіб у справі *«Адомайтіс проти Литви» (Adomaitis v. Lithuania)*, 2022 (§ 84). Аналогічні висновки Суд зробив щодо негласної зйомки розмов, здійсненої приватною особою в професійному контексті, яка згодом була використана владою як доказ для визнання заявника винним у корупції (*«Сарбу проти Румунії» (Sârbu v. Romania)*, 2023, § 54).

97. У справі *«Лопез Рібалда та інші проти Іспанії» (López Ribalda and Others v. Spain)* [ВП], 2019 (§§ 118, 123), законний інтерес роботодавця у вжитті заходів для пошуку та покарання осіб, відповідальних за підозрювані крадіжки, з метою забезпечення захисту майна компанії та її безперебійної роботи, може виправдати заходи, пов'язані з відеоспостереженням за працівниками на робочих місцях.

3. Чи було втручання «необхідним у демократичному суспільстві»

986. Для того, щоб бути необхідним у демократичному суспільстві, будь-який захід, що втручається в захист персональних даних відповідно до статті 8, повинен відповідати «нагальній суспільній потребі» і не бути непропорційним переслідуваним законним цілям (*«Z проти Фінляндії» (Z v. Finland)*, 1997, § 94; *«Хелілі проти Швейцарії» (Khelili v. Switzerland)*, 2011, § 62; *«Вісент Дель Кампо проти Іспанії» (Vicent Del Campo v. Spain)*, 2018, § 46). Причини, на які посилається уряд, повинні бути доречними і достатніми (*«Z проти Фінляндії» (Z v. Finland)*, 1997, § 94). Хоча первинна оцінка всіх цих аспектів належить до компетенції національних органів влади, остаточна оцінка того, чи було втручання необхідним, залишається предметом розгляду Судом на відповідність вимогам Конвенції (*«С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom)* [ВП], 2008, § 101).

99. У контексті особливо серйозних дій між фізичними особами, здатних порушити права за статтею 8, перевірка Судом того, чи відповідали вони вимозі «необхідності в демократичному суспільстві», стосується того, як Держава прийняла спеціальне законодавство для забезпечення захисту цих прав (*«К.У. проти Фінляндії» (K.U. v. Finland)*, 2008, §§ 43-50; *«Сьодерман проти Швеції» (Söderman v. Sweden)* [ВП], 2013, §§ 80-83). Що стосується менш серйозних дій між фізичними особами, таких як відеоспостереження за працівниками на робочому місці, перевірка Судом того, чи був цей захід «необхідним у демократичному суспільстві», стосуватиметься того, яким чином національні суди взяли до уваги критерії, встановлені Судом у своїй практиці, показуючи, чи були зважені конкуруючі інтереси (*«Лопез Рібалда та інші проти Іспанії» (López Ribalda and Others v. Spain)* [ВП], 2019, §§ 116-117, § 122). При перегляді цих критеріїв, якщо буде встановлено, що одного з них бракує, гарантії, що впливають з інших, можуть достатньою мірою компенсувати цей недолік (*там само*, § 131).

100. Загалом, щоб встановити, чи відповідає захід, що втручається в захист персональних даних за статтею 8, умові «необхідності в демократичному суспільстві», Суд дослідив, чи відповідає він вимогам, переліченим у статті 5 [Конвенції 108](#), а саме, зокрема, вимозі мінімізувати обсяг зібраних даних, забезпечити, щоб вони були точними, адекватними, релевантними та не надмірними щодо цілей, для яких вони обробляються, обмежити тривалість їх зберігання, використовувати їх для цілей, для яких вони були зібрані, та забезпечити прозорість їхньої обробки.

а. Вимога мінімізації обсягу зібраних або записаних даних

101. У низці справ Суд розглядав питання про те, чи були персональні дані, що піддавалися автоматизованій обробці, адекватними, релевантними і ненадмірними стосовно цілей, для яких вони були зібрані (*«Л.Л. проти Франції» (L.L. v. France)*, 2006, §§ 45-46; *«Вісент Дель Кампо проти Іспанії» (Vicent Del Campo v. Spain)*, 2018, § 51; *«Хадіджа Ісмаїлова проти Азербайджану» (Khadija Ismayilova v. Azerbaijan)*, 2019, § 147; *«Круглов та інші проти Росії» (Kruglov and Others v. Russia)*, 2020, § 132 *наприкінці*; *«Л.Ф. проти Франції» (L.F. v. France)* (ухв.), 2024, § 34).

102. Суд встановив порушення статті 8 у випадках, коли, наприклад, не було дотримано процедури відбору даних під час обшуків, щоб мінімізувати кількість вилучених даних з електронних пристроїв заявників (*«Круглов та інші проти Росії» (Kruglov and Others v. Russia)*, 2020, § 132 *наприкінці*). Іншим прикладом є справа, де судові рішення щодо заявника, який не був стороною провадження, вказувало його ім'я у справі про домагання на робочому місці, хоча суддя міг уникнути стигматизації, використовуючи лише ініціали (*«Вісент Дель Кампо проти Іспанії» (Vicent Del Campo v. Spain)*, 2018, § 51). У ще одній справі персональні дані журналістки, яку знімали без її відома в інтимних обставинах вдома, були надмірно і безпідставно розкриті у звіті про розслідування (*«Хадіджа Ісмаїлова проти Азербайджану» (Khadija Ismayilova v. Azerbaijan)*, 2019, § 147).

103. Суд зазначив, що створення баз даних з метою запобігання та покарання за правопорушення не може ґрунтуватися на надмірному збиранні інформації (*«Б.Б. проти Франції» (B.B. v. France)*, 2009, § 62; *«Гардель проти Франції» (Gardel v. France)*, 2009, § 63; *«М.Б. проти Франції» (M.B. v. France)*, 2009, § 54). Без дотримання необхідної пропорційності відносно законних цілей, покладених на такі механізми, їхні переваги будуть переважені серйозними порушеннями прав і свобод, які Держави повинні гарантувати відповідно до Конвенції особам, що перебувають під їхньою юрисдикцією (*«М.К. проти Франції» (M. K. v. France)*, 2013, § 35; *«Айкагуер проти Франції» (Aycaguer v. France)*, 2017, § 34). У контексті схеми невибіркового та безстрокового зберігання аргумент про те, що «чим більше зберігається даних, тим більше запобігається злочинів», на практиці буде рівнозначний виправданню зберігання інформації про все населення та їхніх померлих родичів, що, безумовно, було б надмірним і нерелевантним (*«Гогран проти Сполученого Королівства» (Gaughran v. the United Kingdom)*, 2020, § 89).

104. У справі *«Кетт проти Сполученого Королівства» (Catt v. the United Kingdom)*, 2019 (§ 122), Суд визнав порушення статті 8 через відсутність ефективних гарантій щодо знищення в базі даних поліції персональної інформації, що розкриває політичні погляди мирного протестувальника, щойно її зберігання стало непропорційним.

105. Натомість обробка персональних даних, які не були «чутливими» у розумінні статті 6 Конвенції 108 і обмежувалися фактичною та об'єктивною інформацією, пов'язаною з судовим провадженням, в якому особа була стороною, у внутрішній базі даних Міністерства юстиції, не порушувала вимог статті 8 (*«Л.Ф. проти Франції» (L.F. v. France)* (ухв.), 2024, §§ 34 і 40).

б. Вимога точності та оновлення даних

106. Суд розглядав випадки зберігання неточних даних або даних, точність яких оскаржувалася суб'єктом (*«Кемалеттин Канлі проти Туреччини» (Cemalettin Canli v. Turkey)*, 2008, §§ 34-37, про неточні поліцейські дос'є у кримінальному провадженні; *«Ротару проти Румунії» (Rotaru v. Romania)* [ВП], 2000, § 36, про нездатність особи оскаржити інформацію, зібрану службами безпеки, про його передбачувану участь у русі «легіонерів» у своєму далекому минулому).

107. Неправдива або неповна інформація, що була зібрана й зберігається органами влади, може ускладнити життя особи (*«Хелілі проти Швейцарії» (Khelili v. Switzerland)*, 2011, § 64), може виявитися наклепницькою (*«Ротару проти Румунії» (Rotaru v. Romania)* [ВП], 2000, § 44) або порушувати процесуальні гарантії захисту прав суб'єкта даних, коли такі дані можуть бути переміщені між різними органами влади (*«Кемалеттін Канлі проти Туреччини» (Cemalettin Canli v. Turkey)*, 2008, §§ 42-43). Суд також підкреслив, що збір персональних даних на підставі лише припущень або презумпцій без будь-якої доведеної фактичної основи — неприйнятний (*«Дрелон проти Франції» (Drelon v. France)*, 2022, § 97).

108. На думку Суду, саме органи влади повинні довести точність даних, які були збережені. У справі *«Хелілі проти Швейцарії» (Khelili v. Switzerland)*, 2011 (§§ 66-70), де невизначеність оточувала нечітке й загальне твердження про незаконну проституцію, зафіксоване органами влади, зберігання слова «повія» в поліцейських файлах протягом багатьох років не було «необхідним у демократичному суспільстві», беручи до уваги суперечливу поведінку органів влади, принцип, згідно з яким саме ці органи влади повинні доводити точність конкретних даних, вузьку свободу розсуду, якою користуються національні органи влади в цій сфері, і серйозність втручання в право заявниці на повагу до її приватного життя за статтею 8. Подібним чином у справі *«Дрелон проти Франції» (Drelon v. France)*, 2022, §§ 95-97, щодо відмови Французької служби донорства крові прийняти заявника як донора крові на підставі його передбачуваної гомосексуальності, Суд зазначив, що збір персональних даних повинен мати точну і достовірну фактичну основу, тоді як у цій справі висновок про сексуальні практики заявника був зроблений лише тому, що він відмовився відповідати на запитання про своє сексуальне життя під час медичної співбесіди, що передувала донорству.

109. У справі *«Анчев проти Болгарії» (Anchev v. Bulgaria)* (ухв.), 2017 (§§ 112-115), де заявник був об'єктом трьох розслідувань і був позначений на підставі архівних матеріалів як співробітник колишніх служб безпеки відповідно до закону про розголошення інформації про державних службовців, які співпрацювали з комуністичним режимом, Суд відхилив скаргу заявника, зазначивши, що він мав можливість ознайомитися з архівами, а потім публічно оскаржити їхню достовірність на конкретній підставі.

110. У справі *«Маргарі проти Греції» (Margari v. Greece)*, 2023, § 59, де інформація, опублікована в пресі про кримінальні правопорушення заявниці, неточно відображала звинувачення, висунуті проти неї, Суд підкреслив, що надзвичайно важливо, щоб дані, опубліковані в контексті відкритого кримінального провадження або в контексті розслідування кримінальних правопорушень, точно відображали ситуацію і звинувачення, висунуті проти обвинуваченої особи, з урахуванням також дотримання презумпції невинуватості.

с. Вимога зберігати дані не довше, ніж це необхідно для досягнення мети, з якою вони були зафіксовані⁴

111. Питання необхідності обмеження строку зберігання персональних даних розглядалося Судом у низці справ (*«С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom)* [ВП], 2008; *«Б.Б. проти Франції» (B.B. v. France)*, 2009; *«Гардель проти Франції» (Gardel v. France)*, 2009; *«М.Б. проти Франції» (M.B. v. France)*, 2009; *«М.К. проти Франції» (M.K. v. France)*, 2013; *«Дж.П.Д. проти Франції» (J.P.D. v. France)* (ухв.), 2014; *«Перуззо і Мартенс проти Німеччини» (Peruzzo and Martens v. Germany)* (ухв.), 2013; *«В. проти Нідерландів» (W. v. the Netherlands)* (ухв.), 2009; *«Брунет проти Франції» (Brunet v. France)*, 2014; *«Дрелон проти Франції» (Drelon v. France)*, 2022, § 98). Максимальний тридцятирічний термін зберігання в національній судовій базі даних осіб, які вчинили сексуальні злочини, з моменту закінчення тюремного ув'язнення тривалістю від п'яти до п'ятнадцяти років за

⁴ Див. також частину цього посібника, присвячену Строк зберігання даних.

згвалтування, вчинене щодо неповнолітньої особи, не був визнаний непропорційним законній меті, яку переслідувало зберігання даних, а саме запобігання заворушенням або злочинам («*Б.Б. проти Франції*» (*B.B. v. France*), 2009, §§ 67-68; «*Гардель проти Франції*» (*Gardel v. France*), 2009, §§ 68-69; «*М.Б. проти Франції*» (*M.B. v. France*), 2009, §§ 59-60).

112. Однак постійне зберігання в національній базі даних відбитків пальців, клітинних зразків і профілів ДНК осіб, підозрюваних, але не засуджених у вчиненні злочинів, незалежно від характеру або тяжкості злочину, в якому особа спочатку підозрювалася, і незалежно від віку, було визнано порушенням статті 8 («*С. і Марпер проти Сполученого Королівства*» (*S. and Marper v. the United Kingdom*) [ВП], 2008, §§ 125-126). Постійне зберігання даних незасудженої особи може бути особливо шкідливим у випадку неповнолітніх, зважаючи на їхнє особливе становище та важливість їхнього розвитку й інтеграції в суспільство (*там само*, § 124).

113. Відсутність максимального строку зберігання персональних даних не обов'язково несумісна зі статтею 8 («*Гоґран проти Сполученого Королівства*» (*Gaughran v. the United Kingdom*), 2020, § 88; «*Перуззо і Мартенс проти Німеччини*» (*Peruzzo and Martens v. Germany*) (ухв.), 2013, § 46), але процесуальні гарантії будуть тим більш необхідними, коли зберігання даних повністю залежить від старанності органів влади у забезпеченні пропорційності його тривалості (*там само*, § 46; «*Айсаґуер проти Франції*» (*Aysaquer v. France*), 2017, §§ 44-46).

d. Вимога обмеження використання даних метою, для якої вони були зафіксовані

114. Суд вважає, що важливо обмежити використання даних метою, для якої вони були зафіксовані. Так у справі «*Карабейоглу проти Туреччини*» (*Karabeyoğlu v. Turkey*), 2016 (§§ 112-123) використання в дисциплінарному розслідуванні даних, отриманих в результаті прослуховування телефонних розмов під час кримінального розслідування, а отже, з іншою метою, ніж та, яка виправдовувала їхнє збирання, було визнано порушенням статті 8.

123. У справі «*Суриков проти України*» (*Surikov v. Ukraine*), 2017 (§§ 83-95) тривале зберігання даних про психічне здоров'я особи, а також їх поширення та використання з метою, не пов'язаною з причинами, які спочатку виправдовували їхнє збирання, становило непропорційне втручання у право суб'єкта даних на повагу до його приватного життя.

115. Питання про ризик неналежного використання персональної інформації також виникло у справі «*К.Г. та інші проти Словаччини*» (*K.H. and Others v. Slovakia*), 2009 (§§ 45-57), де заявниці, вісім етнічних ромок, підозрюваних у стерилізації під час перебування в лікарні, скаржилися на те, що вони не змогли отримати копії своїх медичних карток. Суд встановив порушення статті 8, зазначивши, що ризику зловживання, про який стверджував Уряд, можна було б запобігти за допомогою таких засобів, як включення до національного законодавства відповідних гарантій з метою суворого обмеження обставин, за яких такі дані можуть бути розкриті, і кола осіб, які мають право на доступ до цих файлів (*там само*, § 56).

116. Щоб визначити межу інтимності приватного життя, гарантовану статтею 8, Суд провів розмежування між спостереженням за діями особи в громадському місці з метою гарантування безпеки та записом таких дій, які використовуються в інших цілях, що виходять за межі очікувань відповідної особи («*Пек проти Сполученого Королівства*» (*Peck v. the United Kingdom*), 2003, §§ 59-62, щодо зйомки заявника в громадському місці з міркувань безпеки, коли відзнятий матеріал був переданий ЗМІ; «*Перрі проти Сполученого Королівства*» (*Perry v. the United Kingdom*), 2003, §§ 41-42, щодо хитрощів, використаних поліцією для ідентифікації заявника за допомогою відеозапису, що виходив за межі звичайного або передбачуваного використання відеокамер; «*Глухін проти Росії*» (*Glukhin v. Russia*), 2023, §§ 65-73, щодо використання технології розпізнавання обличчя у контексті публічного спостереження за допомогою камер відеоспостереження).

е. Вимога прозорості процедур обробки даних⁵

117. У низці справ, що стосувалися персональних даних, зібраних і збережених органами державної влади, Суд встановив, що органи влади мають позитивне зобов'язання забезпечити зацікавлених осіб «ефективною та доступною процедурою», яка дозволить їм мати доступ до «всієї відповідної та належної інформації», необхідної, наприклад, для того, щоб знати й розуміти своє дитинство та ранній розвиток («*Гаскін проти Сполученого Королівства*» (*Gaskin v. the United Kingdom*), 1989, § 49), встановити ідентичність («*Одієвре проти Франції*» (*Odièvre v. France*) [ВП], 2003, §§ 41-49), або виявити будь-які ризики для здоров'я, на які вони наражались («*Роше проти Сполученого Королівства*» (*Roche v. The United Kingdom*) [ВП], 2005, § 162; «*Гуерра та інші проти Італії*» (*Guerra and Others v. Italy*), 1998, § 60; «*Макгінлі та Еган проти Сполученого Королівства*» (*McGinley and Egan v. the United Kingdom*), 1998, § 101), або щоб відстежити свою особисту історію за часів колишнього тоталітарного режиму («*Гараламбіє проти Румунії*» (*Haralambie v. Romania*), 2009, § 93).

118. Ця вимога прозорості менш сувора в контексті інформації, що стосується національної безпеки («*Леандр проти Швеції*» (*Leander v. Sweden*), 1987, § 51; «*Зегершtedт-Віберг та інші проти Швеції*» (*Segerstedt-Wiberg and Others v. Sweden*), 2006, § 102; «*Далеа проти Франції*» (*Dalea v. France*) (ухв.), 2010).

II. Захист даних та право на повагу до приватного життя (стаття 8 Конвенції)

Стаття 8 Конвенції

«1. Кожен має право на повагу до свого приватного та сімейного життя, до свого житла та кореспонденції.

2. Органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб».

119. На сьогодні Суд розглянув велику кількість операцій з персональними даними, здійснених органами влади або різними приватними установами, оцінюючи, чи було порушено «приватне життя», «житло» та/або «кореспонденцію» суб'єкта даних у спосіб, несумісний зі статтею 8 Конвенції. У різних контекстах Суд визначив обсяг прав, на які можуть покладатися юридичні та фізичні особи для захисту своїх персональних даних.

⁵ Див. також частину цього посібника, присвячену Праву на доступ до власних даних.

А. Операції з даними, що можуть порушувати право на повагу до приватного життя

120. З розвитком технологій збирання, зберігання та розголошення даних набувають різноманітних форм. У кількох справах Суд розглядав питання про те, чи призвели одна або кілька таких операцій до невинного втручання у право суб'єкта даних на повагу до його приватного життя.

1. Збирання персональних даних

121. Суд розглядав операції зі збирання персональних даних у різних контекстах: у боротьбі з організованою злочинністю і тероризмом за допомогою різних таємних систем спостереження, створених органами влади; у судовому контексті щодо персональних даних, зібраних органами влади для використання як доказів; у сфері охорони здоров'я; у контексті даних, зібраних на робочому місці, як державними, так і приватними роботодавцями; і, нарешті, у контексті правових зобов'язань державних або приватних органів щодо передачі персональних даних органам влади з метою захисту громадських інтересів.

а. Збирання даних органами влади за допомогою прихованого спостереження⁶

122. Суд розглянув значну кількість справ щодо збору персональних даних за допомогою різних методів таємного спостереження. Незалежно від того, яку систему спостереження використовують органи влади, важлива наявність адекватних і достатніх гарантій проти зловживань. Суд вважає, що повноваження таємного спостереження за громадянами допустимі лише тією мірою, якою вони суворо необхідні для захисту демократичних інститутів (*«Класс та інші проти Німеччини» (Klass and Others v. Germany)*, 1978, § 42; *«Шабо та Віссу проти Угорщини» (Szabó and Vissy v. Hungary)*, 2016, §§ 72-73). Таке втручання повинне бути обґрунтованим відповідними й достатніми причинами та пропорційним законній меті або цілям, що переслідуються (*«Зеєрштедт-Віберг та інші проти Швеції» (Segerstedt-Wiberg and Others v. Sweden)*, § 88). Національне законодавство повинно передбачати достатньо точні, ефективні та всеосяжні гарантії щодо замовлення та виконання заходів спостереження, а також щодо забезпечення потенційного відшкодування (*«Шабо та Віссу проти Угорщини» (Szabó and Vissy v. Hungary)*, 2016, § 89).

і. Прослуховування та реєстрація телефонних дзвінків

123. У судовій практиці Суд встановив порушення статті 8 у таких сферах: прослуховування телефонних розмов і передача записів реєстрації телефонних розмов до поліції (список телефонних номерів) (*«Мелон проти Сполученого Королівства» Malone v. the United Kingdom*, 1984, §§ 63-89); моніторинг і розшифровка всіх комерційних і приватних телефонних дзвінків заявників (*«Гувіг проти Франції» (Huvig v. France)*, 1990, §§ 24-35); моніторинг і розшифровка декількох телефонних розмов заявників шляхом прослуховування телефонних ліній третіх осіб (*«Круслін проти Франції» (Kruslin v. France)*, 1990, §§ 25-36); моніторинг і запис телефонних розмов заявника шляхом прослуховування телефонної лінії третьої особи (*«Ламберт проти Франції» (Lambert v. France)*, 1998, §§ 21-41); моніторинг і запис прокурором телефонного дзвінка, отриманого особою у власному кабінеті від іншої особи в радянському посольстві в Берні (*«Аманн проти Швейцарії» (Amann v. Switzerland)* [ВП], 2000, §§ 45-62); прослуховування телефонних розмов в рамках попереднього розслідування (*«Прадо Бугалло проти Іспанії»*

⁶ Див. також [Посібник зі статті 8 Конвенції \(Право на повагу до приватного і сімейного життя\)](#).

(*Prado Bugallo v. Spain*), 2003, §§ 28-33); прослуховування телефонних розмов в контексті кримінального переслідування, які згодом були опубліковані в пресі («*Краксі проти Італії*» (*Craxi v. Italy (no. 2)*), 2003, §§ 57-84); включення до матеріалів справи заявника розшифровки прослуховування телефону, здійсненого в рамках провадження, в якому він не брав участь («*Матерон проти Франції*» (*Matheron v. France*), 2005, §§ 27-44); моніторинг телефонних дзвінків органами влади за відсутності дозволу прокурора та відсутності законодавства, що забезпечує достатні гарантії проти свавілля («*Думітру Попеску проти Румунії*» (*Dumitru Popescu v. Romania (no. 2)*), 2007, §§ 61-86); прослуховування телефонних дзвінків, здійснених адвокатом у межах кримінального розслідування («*Квасніца проти Словаччини*» (*Kvasnica v. Slovakia*), 2009, §§ 80-89); недостатні гарантії проти свавілля у національних положеннях про прослуховування телефонних розмов («*Драгоєвіч проти Хорватії*» (*Dragojević v. Croatia*), 2015, §§ 85-102; «*Ліблік та інші проти Естонії*» (*Liblik and Others v. Estonia*), 2019, §§ 132-143); відсутність належних судових гарантій («*Москальов проти Росії*» (*Moskalev v. Russia*), 2017, §§ 35-45); відсутність ефективного нагляду за перехопленням телефонних розмов у кримінальних провадженнях («*Прутеану проти Румунії*» (*Pruteanu v. Romania*), 2015, §§ 41-58); моніторинг мобільних телефонних розмов («*Шантаре та Лабазніковс проти Латвії*» (*Šantare and Labazņikovs v. Latvia*), 2016, §§ 56-63); необґрунтоване ненадання *ex post* повідомлення про тимчасовий захід з реєстрації дзвінків з мобільного телефону («*Кеват Озель проти Туреччини*» (*Cevat Özel v. Turkey*), 2016, §§ 29-37); і превентивний моніторинг телефонних розмов («*Мустафа Сезгін Танрікулу проти Туреччини*» (*Mustafa Sezgin Tanrikulu v. Turkey*), 2017, §§ 45-66); практично необмежені повноваження спецслужб у здійсненні спостереження за особою та зустрічами, що проводилися у квартирі, без достатніх правових гарантій («*Золтан Варга проти Словаччини*» (*Zoltán Varga v. Slovakia*), 2021, §§ 170-171), що також випадковим чином вплинуло на іншу особу без захисту, передбаченого національним законодавством для такої особи («*Хашчак проти Словаччини*» (*Haščák v. Slovakia*), 2022, § 95); перехоплення, фіксація і розшифровка телефонної розмови між адвокатом і клієнтом, колишнім міністром оборони, який перебував під таємним наглядом у зв'язку з кримінальним розслідуванням («*Василь Васильєв проти Болгарії*» (*Vasil Vasilev v. Bulgaria*), 2021, §§ 167-181).

124. Суд не виявив порушення статті 8 щодо прослуховування телефонних розмов, дозволеного судовим рішенням, коли необхідність цього заходу була належним чином оцінена судом («*Ірфан Гюзель проти Туреччини*» (*İrfan Güzel v. Turkey*), 2017, §§ 78-89).

125. Суд також не знайшов порушення статті 8 у таких справах: реєстрація поліцією телефонних номерів, на які телефонувала особа, за допомогою обліку її приватного телефону («*П.Г. і Дж.Г. проти Сполученого Королівства*» (*P.G. and J.H. v. the United Kingdom*), 2001, §§ 42-51); прослуховування телефонних ліній судді в рамках кримінального розслідування щодо незаконної організації, адже підозрювалося, що він її член або прихильник («*Карабейоглу проти Туреччини*» (*Karabeyoğlu v. Turkey*), 2016, §§ 74-111); перехоплення телефонних переговорів директора в'язниці в рамках кримінального розслідування підозри в корупційній діяльності, хоча в кінцевому підсумку це розслідування було припинено через відсутність обвинувальних доказів («*Адомайтіс проти Литви*» (*Adomaitis v. Lithuania*), 2022, §§ 81-90).

126. Кілька заяв були визнані неприйнятними як явно необґрунтовані, зокрема: прослуховування телефонів у рамках превентивних розвідувальних заходів поліції («*Девечі проти Туреччини*» (*Devenci v. Türkiye*) (ухв.), 2022); прослуховування телефонів у рамках досудового розслідування («*Гройтер проти Нідерландів*» (*Greuter v. the Netherlands*) (ухв.), 2002); прослуховування телефонів у рамках кримінального розслідування як одного з основних методів, що допоміг довести причетність до великої мережі торгівлі наркотиками («*Кобан проти Іспанії*» (*Coban v. Spain*) (ухв.), 2006); моніторинг телефонних переговорів члена Європейського парламенту, обвинуваченого в незаконному привласненні корпоративних

активів, і незастосування спеціального режиму, що надається національним депутатам (*«Маркіані проти Франції» (Marchiani v. France)* (ухв.), 2008).

127. У контексті в'язниці незаконний запис і зберігання тюремною адміністрацією телефонних розмов ув'язненого, а також їх подальше використання як доказів для засудження його за наступний злочин порушили статтю 8 у справі *«Доєрга проти Нідерландів» (Doerga v. the Netherlands)*, 2004 (§§ 43-54).

128. Суд також встановив порушення статті 8 у низці інших сфер: автоматична система моніторингу всієї кореспонденції та телефонних дзвінків неповнолітніх у виправній школі-інтернаті, що виключала будь-яку конфіденційність (*«Д.Л. проти Болгарії» (D.L. v. Bulgaria)*, 2006, §§ 100-116); санкціоноване перехоплення Міністерством оборони вихідних повідомлень організацій, що працюють у сфері громадянських свобод (*«Ліберті та інші проти Сполученого Королівства» Liberty and Others v. the United Kingdom*, 2008, §§ 56-70); саме існування законодавства, що дозволяло моніторинг телекомунікацій молдавської неурядової організації, яка спеціалізується на представництві заявників у Суді (*«Лордачі та інші проти Молдови» (Iordachi and Others v. Moldova)*, 2009, §§ 29-54); витік у ЗМІ та трансляція приватної розмови, записаної з дозволу влади на телефонній лінії політика, який перебував під слідством (*«Дракшас проти Литви» (Drakšas v. Lithuania)*, 2012, § 62); недоліки правової бази, що регулює таємний моніторинг мобільних телефонних дзвінків, здійснюваний операторами мобільного зв'язку, що дозволяє Федеральній службі безпеки перехоплювати будь-які телефонні розмови без попереднього судового дозволу (*«Роман Захаров проти Росії» (Roman Zakharov v. Russia)* [ВП], 2015, §§ 163-305); використання в дисциплінарному провадженні даних прослуховування телефонних розмов у рамках кримінального розслідування (*«Карабейоглу проти Туреччини» (Karabeyoğlu v. Turkey)*, 2016, §§ 112-121); використання в дисциплінарному провадженні проти адвоката запису розмови з одним із її клієнтів, телефон якого прослуховувався (*«Версіні-Кампінчі та Краснянські проти Франції» (Versini-Campinchi and Crasnianski v. France)*, 2016, §§ 49-84). Навпаки, використання в дисциплінарному провадженні проти директора в'язниці інформації, отриманої в результаті прослуховування його телефону в рамках кримінального розслідування підозри в корупції, було визнано пропорційним (*«Адомаїміс проти Литви» (Adomaitis v. Lithuania)*, 2022, § 87).

ii. Перехоплення повідомлень пейджера

129. У справі *«Тейлор-Саборі проти Сполученого Королівства» (Taylor-Sabori v. the United Kingdom)*, 2002, §§ 18-19, у рамках судового провадження, перехоплення поліцією повідомлень пейджера заявника та подальше посилання на них як підставу для засудження було визнано таким, що суперечить статті 8, через відсутність будь-яких правових норм щодо такого перехоплення.

iii. Аудіо- та відеоспостереження

130. Суд встановив порушення статті 8 у справі, де запис розмови за допомогою радіопередавального пристрою в рамках таємної поліцейської операції не супроводжувався належними процесуальними гарантіями (*«Буков проти Росії» (Bykov v. Russia)* [ВП], 2009, §§ 81, 83; *«Олейнік проти Росії» (Oleynik v. Russia)*, 2016, §§ 75-79).

131. Суд розрізнив спостереження за діями особи в громадському місці для гарантування безпеки та запис цих дій для інших цілей, що виходять за межі того, що особа могла передбачити (*«Пек проти Сполученого Королівства» (Peck v. the United Kingdom)*, 2003, §§ 59-62; *«Перрі проти Сполученого Королівства» (Perry v. the United Kingdom)*, 2003, §§ 41-42), для встановлення чіткої межі приватного життя, захищеного статтею 8, у сфері таємних заходів спостереження та перехоплення повідомлень державними органами. Суд також підкреслив надзвичайно інтрузивний характер технології розпізнавання обличчя, зокрема, використання

цієї технології в режимі реального часу на камерах відеоспостереження, що контролюють громадські місця. Це дозволило поліції знайти та заарештувати заявника, коли він їхав метрополітенном, через його участь в одиночній демонстрації без попереднього повідомлення. Суд наголосив на високому рівні обґрунтування, який вимагається для того, щоб такі заходи вважалися «необхідними в демократичному суспільстві», причому найвищий рівень обґрунтування вимагається для використання технології розпізнавання обличчя у реальному часі (*«Глухін проти Росії» (Glukhin v. Russia)*, 2023, § 86).

132. У своїй практиці Суд встановив порушення статті 8 у таких справах: запис голосів заявників під час пред'явлення їм звинувачень і під час їхнього утримання в камерах у відділенні поліції (*«П.Г. і Дж.Г. проти Сполученого Королівства» (P.G. and J.H. v. the United Kingdom)*, 2001, §§ 56-63); зйомка з метою ідентифікації підозрюваного у відділенні поліції за допомогою прихованої камери відеоспостереження (*«Перрі проти Сполученого Королівства» (Perry v. the United Kingdom)*, 2003, §§ 36-49); запис, зроблений поліцією за допомогою пристрою для прослуховування, встановленого в будинку третьої особи, яку відвідував заявник, спонтанної розмови, під час якої заявник зізнався, що брав участь у ввезенні наркотиків (*«Кхан проти Сполученого Королівства» (Khan v. the United Kingdom)*, 2000, §§ 25-28); прослуховування поліцією приватних приміщень у рамках судового розслідування (*«Веттер проти Франції» (Vetter v. France)*, 2005, §§ 20-27); запис розмови за допомогою пристрою підслуховування, встановленого на особу органами поліції, і подальше використання цього запису в суді, хоча і не як єдиного обвинувального доказу (*«Хеглас проти Чеської Республіки» (Heglas v. Czech Republic)*, 2007, §§ 71-76); запис повідомлень особи в контексті офіційного розслідування чи для такого розслідування, як кримінального, так і будь-якого іншого, за участю та технічною допомогою державних слідчих органів (*«Ван Вондель проти Нідерландів» (Van Vondel v. the Netherlands)*, 2007, §§ 47-55). Навпаки, не було встановлено порушення у справі щодо використання у кримінальному провадженні відеозаписів розмов заявника з приватною особою у професійному контексті, зроблених цією особою на приховану камеру, і виявлених органами влади під час огляду комп'ютера іншої особи, де зберігалися ці записи (*«Сарбу проти Румунії» (Sârbu v. Romania)*, 2023, §§ 48-59).

133. У контекст в'язниці Суд встановив порушення статті 8 у таких справах: використання владою відео- та аудіозаписувальних пристроїв, приховано встановлених у камері заявника і в зоні для побачень, а також на особі співкамерника, що сприяло запису неспонтанних, спровокованих заяв заявника (*«Еллен проти Сполученого Королівства» (Allan v. the United Kingdom)*, 2002, §§ 35-36); запис розмов між ув'язненими та їхніми родичами в кімнатах для побачень (*«Віссе проти Франції» (Wisse v. France)*, 2005, §§ 28-34); таємне спостереження за консультаціями ув'язненого з його адвокатом (*«Р.Е. проти Сполученого Королівства» (R.E. v. the United Kingdom)*, 2015, §§ 115-143); цілодобове відеоспостереження за ув'язненими в їхніх камерах за допомогою прихованих камер відеоспостереження (*«Горлов та інші проти Росії» (Gorlov and Others v. Russia)*, 2019, §§ 83-100).

134. Суд не встановив порушення статті 8 щодо прихованого спостереження за консультаціями ув'язненого з особою, призначеною для надання йому допомоги як вразливій особі після арешту (*«Р.Е. проти Сполученого Королівства» (R.E. v. the United Kingdom)*, 2015, §§ 154-168). Положення, що стосуються спрямованого спостереження, в частині, яка стосується можливого спостереження за консультаціями між ув'язненими та відповідними дорослими, супроводжувалися належними гарантіями проти зловживань.

135. У різних контекстах, коли дані були зібрані за допомогою прихованих камер, Суд встановив порушення статті 8 щодо: передачі засобам масової інформації відеозапису з прихованої камери відеоспостереження, на якому була зафіксована особа, що намагалася вчинити самогубство в громадському місці (*«Пек проти Сполученого Королівства» (Peck v. the United Kingdom)*, 2003, §§ 57-87); трансляції по телебаченню непікселізованого та нерозмитого зображення особи, знятої прихованою камерою (*«Бремнер проти Туреччини» (Bremner*

v. Turkey), 2015, §§ 71-85); прихованої відеозйомки журналістки вдома та публічної трансляції цих відеозаписів («*Хадіджа Ісмаїлова проти Азербайджану*» (*Khadija Ismayilova v. Azerbaijan*), 2019, §§ 108-132).

iv. Геолокація транспортного засобу за допомогою GPS⁷

136. У справі «*Узун проти Німеччини*» (*Uzun v. Germany*), 2010 (§§ 49-81) GPS-спостереження за особою, підозрюваною в тероризмі, не було визнано порушенням статті 8. Навпаки у справі «*Бен Файза проти Франції*» (*Ben Faiza v. France*), 2018 (§§ 53-61), встановлення геолокаційного пристрою в транспортному засобі та використання отриманих даних, які дозволили слідчим відстежувати пересування заявника в режимі реального часу і затримати його, було визнано порушенням статті 8.

v. Стеження приватними детективами

137. У справі «*Вукота-Боїч проти Швейцарії*» (*Vukota-Bojić v. Switzerland*), 2016 (§§ 52-78) Суд встановив порушення статті 8 у зв'язку з незаконним стеженням приватними детективами за особою, яка отримувала спірні соціальні виплати. Національне законодавство не визначало з достатньою чіткістю обсяг і спосіб реалізації дискреційних повноважень, наданих страховим компаніям, що виступали як державні органи у спорах щодо страхових виплат, зокрема щодо проведення таємного спостереження за застрахованими особами.

vi. Моніторинг кореспонденції

138. У контексті в'язниць Суд встановив порушення статті 8 у таких справах: перехоплення та відкриття кореспонденції ув'язненого («*Лавенц проти Латвії*» (*Lavents v. Latvia*), 2002, §§ 136-137); відкриття кореспонденції ув'язненого, навіть у випадку несправності поштової служби у в'язниці («*Деміртепе проти Франції*» (*Demirtepe v. France*), 1999, §§ 26-28; «*Валашінас проти Литви*» (*Valašinas v. Lithuania*), 2001, §§ 128-130); перехоплення та цензурування кореспонденції ув'язненого («*Сілвер та інші проти Сполученого Королівства*» (*Silver and Others v. the United Kingdom*), 1983, §§ 84-105; «*Лабіта проти Італії*» (*Labita v. Italy*) [ВП], 2000, §§ 176-184; «*Недбала проти Польщі*» (*Niedbala v. Poland*), 2000, §§ 78-84; «*Мессіна проти Італії*» (*№ 2*) (*Messina v. Italy (no. 2)*), 2000, §§ 78-83); перехоплення листів ув'язненого до адвоката («*Екінчі та Акалін проти Туреччини*» (*Ekinçi and Akalin v. Turkey*), 2007, §§ 37-48); перехоплення листування ув'язненого з адвокатами та Європейською комісією з прав людини («*Кемпбел проти Сполученого Королівства*» (*Campbell v. the United Kingdom*), 1992, §§ 32-54; «*А.Б. проти Нідерландів*» (*A.B. v. the Netherlands*), 2002, §§ 81-94); відкриття листа, надісланого ув'язненому Європейською комісією («*Піерс проти Греції*» (*Peers v. Greece*), 2001, §§ 81-84); моніторинг листування ув'язненого з його радником («*Жулук проти Сполученого Королівства*» (*Szuluk v. the United Kingdom*), 2009, §§ 47-55); практика сканування та завантаження приватної кореспонденції ув'язнених, як вхідної, так і вихідної, на сервер Національної судової мережі («*Нух Узун та інші проти Туреччини*» (*Nuh Uzun and Others v. Turkey*), 2022, §§ 80-99). Навпаки, у справі «*Ердем проти Німеччини*» (*Erdem v. Germany*), 2001 (§§ 53-70), не було виявлено порушення статті 8 щодо перехоплення листування між ув'язненим, підозрюваним у тероризмі, і його адвокатом.

139. В іншому контексті порушення статті 8 було встановлено у справі, коли арбітражний керуючий відкрив і скопіював до справи кореспонденцію банкрута («*Фокслі проти Сполученого Королівства*» (*Foxley v. the United Kingdom*), 2000, §§ 27-47).

⁷ Див. також вище розділ Посібника про Дані про місцезнаходження за допомогою GPS.

vii. Негласне спостереження, шпигунство і операції з масового спостереження

140. У справі *«Роман Захаров проти Росії» (Roman Zakharov v. Russia)* [ВП], 2015 (§§ 171-172) Суд постановив, що заявник може стверджувати, що він є жертвою порушення, спричиненого самим фактом існування таємних заходів спостереження або законодавства, що дозволяє такі заходи, якщо дотримані певні умови, і що підхід, прийнятий у справі *«Кеннеді проти Сполученого Королівства» (Kennedy v. the United Kingdom)*, 2010 (§ 124), якнайкраще відповідає потребі гарантувати, що таємність заходів спостереження не призводить до того, що вони фактично не підлягають оскарженню і залишаються за межами нагляду з боку національних органів правосуддя і суду. У справі *«Екімджієв та інші проти Болгарії» (Ekimdzhiiev and Others v. Bulgaria)*, 2022 (§ 262-277 і 371-384) Суд прийняв, на основі принципів, розроблених у справі *«Роман Захаров проти Росії» (Roman Zakharov v. Russia)* [ВП], 2015 (§ 171), що заявники, два адвокати та дві пов'язані з ними неурядові організації, можуть стверджувати, що вони є жертвами втручання в їхні права за статтею 8 через саме існування національного законодавства або практики, що дозволяють таємне спостереження, а також законів, що регулюють доступ органів влади до збережених даних про комунікації (див. також аналогічний підхід щодо законодавчої вимоги до постачальників послуг інтернет-зв'язку зберігати зміст інтернет-комунікацій та пов'язані з ними комунікаційні дані, надавати доступ правоохоронним органам і службам безпеки до цих даних на їхню вимогу та розшифровувати електронні повідомлення, якщо вони були зашифровані, *«Подчасов проти Росії» (Podchasov v. Russia)*, 2024, §§ 54-55).

141. Суд встановив порушення статті 8 у таких справах: коли асоціація-заявник могла бути піддана заходам спостереження в будь-який час без повідомлення відповідно до Закону про спеціальні засоби спостереження (*«Асоціація за європейську інтеграцію і права людини та Екімджієв проти Болгарії» (Association for European Integration and Human Rights and Ekimdzhiiev v. Bulgaria)*, 2007, §§ 69-94); прослуховування і запис розмови за допомогою радіопередавального пристрою в рамках таємної операції поліції без процесуальних гарантій (*«Биков проти Росії» (Bykov v. Russia)* [ВП], 2009, §§ 72-83); запис розмов в рамках «оперативного експерименту», проведеного за ініціативою Федеральної служби безпеки у спосіб, що не «відповідає закону» (*«Олейнік проти Росії» (Oleynik v. Russia)*, 2016, §§ 74-79); санкціоноване перехоплення Міністерством оборони вихідних повідомлень організацій, що працюють у сфері громадянських свобод (*«Ліберті та інші проти Сполученого Королівства» (Liberty and Others v. the United Kingdom)*, 2008, §§ 55-70); зберігання записів і поліцейський нагляд за заявником через його членство в правозахисній організації (*«Шимоволос проти Росії» (Shimovolos v. Russia)*, 2011, §§ 64-71); законодавство про таємне спостереження, що передбачає створення спеціальної антитерористичної оперативної групи без належних гарантій проти зловживань (*«Шабо і Віссу проти Угорщини» (Szabó and Vissy v. Hungary)*, 2016, §§ 52-89); зберігання інформації, зібраної за допомогою таємного спостереження (*«Ротару проти Румунії» (Rotaru v. Romania)* [ВП], 2000, §§ 45-63; *«Асоціація «21 грудня 1989» та інші проти Румунії» (Association «21 December 1989» and Others v. Romania)*, 2011, §§ 169-177); різні недоліки національної правової бази, що регулює таємне спостереження за мобільним зв'язком (*«Роман Захаров проти Росії» (Roman Zakharov v. Russia)* [ВП], 2015, §§ 163-305); і режим масового перехоплення комунікацій, який не містив достатніх «наскрізних» запобіжних заходів для забезпечення адекватних та ефективних гарантій проти свавілля та ризику зловживань, навіть попри те, що певні надійні запобіжні заходи були визначені (*«Центр правосуддя проти Швеції» (Centrum för rättvisa v. Sweden)* [ВП], 2021, §§ 365-374, та *«Біг Бразер Вотч та інші проти Сполученого Королівства» (Big Brother Watch and Others v. the United Kingdom)* [ВП], 2021, §§ 424-427). Суд також визнав порушення статті 8 у справ *«Екімджієв та інші проти Болгарії» (Ekimdzhiiev and Others v. Bulgaria)*, 2022 (§§ 356-359 і 419-421), зазначивши, зокрема, що, хоча закони, які регулюють таємне спостереження, були значно вдосконалені після їх розгляду у справі *«Асоціація за європейську інтеграцію і права людини*

та Екімджиев проти Болгарії» (Association for European Integration and Human Rights and Ekimdzhiiev v. Bulgaria), 2007, закони, що регулюють таємне спостереження, в тому вигляді, в якому вони застосовуються на практиці, все ще не відповідають мінімальним гарантіям від свавілля та зловживань у низці аспектів. Аналогічний висновок був зроблений і щодо законів, які регулюють зберігання даних про комунікації та подальший доступ до них органів влади. Так само у справі *«Пьотржак і Бичавська-Синярска та інші проти Польщі» (Pietrzak and Bychawska-Siniarska and Others v. Poland)*, 2024 (§§ 195-278), Суд встановив, що два польські закони, які дозволяють таємне спостереження, зберігання та обробку комунікаційних даних, не мають достатніх гарантій проти свавілля.

142. Суд не знайшов порушення статті 8 у таких справах: використання агента під прикриттям у поєднанні з прослуховуванням телефонної лінії заявника, який був звинувачений у торгівлі наркотиками (*«Люді проти Швейцарії» (Lüdi v. Switzerland)*, 1992, §§ 38-41); система, що дозволяє таємне спостереження за листуванням, поштою і телефонними розмовами громадян (*«Класс та інші проти Німеччини» (Klass and Others v. Germany)*, 1978, §§ 39-60); законодавча база, що дозволяє перехоплення внутрішніх комунікацій з метою боротьби з тероризмом і серйозними злочинами (*«Кеннеді проти Сполученого Королівства» (Kennedy v. the United Kingdom)*, 2010, §§ 151-170).

143. Суд визнав явно необґрунтованою заяву *«Вебер і Саравія проти Німеччини» (Weber and Saravia v. Germany)* (ухв.), 2006 (§§ 143-153) щодо стратегічного спостереження за телекомунікаціями, яка є продовженням справи *«Класс та інші проти Німеччини» (Klass and Others v. Germany)*, 1978.

б. Збирання даних роботодавцями на робочому місці

144. Суд оцінив за статтею 8 питання збирання персональних даних на робочому місці роботодавцями державного сектору (*«Гелфорд проти Сполученого Королівства» (Halford v. the United Kingdom)*, 1997, §§ 49, 45; *«Антовіч і Мірковіч проти Чорногорії» (Antović and Mirković v. Montenegro)*, 2017, § 58; *«Ліберт проти Франції» (Libert v. France)*, 2018, § 41) чи приватного сектору (*«Кьопке проти Німеччини» (Körke v. Germany)* (ухв.), 2010; *«Барбулеску проти Румунії» (Bărbulescu v. Romania)* [ВП], 2017, § 109; та *«Лопез Рібалда та інші проти Іспанії» (López Ribalda and Others v. Spain)* [ВП], 2019, § 109). У деяких випадках операція зі збору даних проводилася без відома суб'єктів даних через спостереження, яке трималося в таємниці, або повністю (*«Гелфорд проти Сполученого Королівства» (Halford v. the United Kingdom)*, 1997, § 49; *«Копленд проти Сполученого Королівства» (Copland v. the United Kingdom)*, 2007, § 45; *«Барбулеску проти Румунії» (Bărbulescu v. Romania)* [ВП], 2017, § 78), або частково (*«Лопез Рібалда та інші проти Іспанії» (López Ribalda and Others v. Spain)* [ВП], 2019, § 93), тоді як в інших випадках дані збиралися з повного відома відповідних працівників (*«Антовіч і Мірковіч проти Чорногорії» (Antović and Mirković v. Montenegro)*, 2017, § 44).

145. Персональні дані, які підлягали збору, виникали в результаті: спостереження за непрофесійними телефонними дзвінками з професійних приміщень (*«Гелфорд проти Сполученого Королівства» (Halford v. the United Kingdom)*, 1997, § 44); моніторингу використання телефону, електронної пошти та інтернету на роботі (*«Копленд проти Сполученого Королівства» (Copland v. the United Kingdom)*, 2007, §§ 44-49); моніторингу використання Інтернету та миттєвих повідомлень (Yahoo) (*«Барбулеску проти Румунії» (Bărbulescu v. Romania)* [ВП], 2017, § 74); відкриття файлів, що зберігаються працівником на комп'ютері, наданому роботодавцем у робочих цілях (*«Ліберт проти Франції» (Libert v. France)*, 2018, § 25); відеозаписів поведінки ідентифікованого працівника або працівника, якого можна ідентифікувати, на робочому місці (*«Кьопке проти Німеччини» (Körke v. Germany)* (ухв.), 2010; *«Антовіч і Мірковіч проти Чорногорії» (Antović and Mirković v. Montenegro)*, 2017, § 44; *«Лопез Рібалда та інші проти Іспанії» (López Ribalda and Others v. Spain)* [ВП], 2019, § 92); або моніторингу за допомогою системи GPS відстаней, подоланих працівником на службовому

транспортному засобі в ході його професійної діяльності та, у відповідних випадках, під час приватних поїздок (*«Флоріндо де Альмейда Васконселос Грамаксо проти Португалії» (Florindo de Almeida Vasconcelos Gramacho v. Portugal)*, 2022, §§ 94-96).

146. У перших двох рішеннях, винесених у цій сфері (*«Гелфорд проти Сполученого Королівства» (Halford v. the United Kingdom)*, 1997, § 44, і *«Копленд проти Сполученого Королівства» (Copland v. the United Kingdom)*, 2007, § 41), Суд постановив, що неробочі телефонні дзвінки з офісних приміщень на перший погляд охоплюються поняттями «приватне життя» і «кореспонденція» для цілей статті 8. Він також постановив, що електронні листи, надіслані з роботи, мають бути так само захищені статтею 8, як і інформація, отримана в результаті моніторингу особистого користування інтернетом (*«Копленд проти Сполученого Королівства» (Copland v. the United Kingdom)*, 2007, § 41). Згодом Суд також уточнив, що дані, які чітко визначені як приватні і зберігаються працівником на комп'ютері, наданому йому роботодавцем для робочих цілей, також можуть охоплюватися поняттям «приватне життя» (*«Ліберт проти Франції» (Libert v. France)*, 2018, § 25). Крім того, прихований відеозапис, що показує поведінку працівника на робочому місці без його повідомлення, також впливає на його «приватне життя» (*«Кьопке проти Німеччини» (Köpke v. Germany)* (ухв.), 2010). Згодом Суд не побачив причин відступати від цього висновку незалежно від того, чи було відеоспостереження за працівниками на їхньому робочому місці таємним чи відкритим (*«Антовіч і Мірковіч проти Чорногорії» (Antović and Mirković v. Montenegro)*, 2017, § 44; *«Лопез Рібалда та інші проти Іспанії» (López Ribalda and Others v. Spain)* [ВП], 2019, § 93).

147. У справах *«Гелфорд проти Сполученого Королівства» (Halford v. the United Kingdom)*, 1997 (§§ 50-51) та *«Копленд проти Сполученого Королівства» (Copland v. the United Kingdom)*, 2007 (§ 48), Суд постановив, що за відсутності на той час національного законодавства, яке дозволяло б збирати персональні дані з неробочих телефонних дзвінків працівників та електронних повідомлень, надісланих з робочого місця, відповідно, втручання в їхнє право на повагу до приватного життя не відбувалося «відповідно до закону». У справі *«Кьопке проти Німеччини» (Köpke v. Germany)* (ухв.), 2010, Суд визнав явно необґрунтованою скаргу на роботодавця, який за допомогою приватного детективного агентства зібрав дані про касира супермаркету, підозрюваного в крадіжці, використовуючи приховане відеоспостереження. Хоча на той час умови, за яких роботодавець може вдаватися до відеоспостереження за працівником, ще не були законодавчо закріплені, судова практика Федерального суду з питань праці встановила основні гарантії проти свавільного втручання у право працівників на повагу до їхнього приватного життя.

148. Існування обґрунтованої підозри у вчиненні серйозного проступку та розмір збитків, виявлених у цій справі, можуть бути вагомим обґрунтуванням для роботодавців здійснювати збір персональних даних на робочому місці (*«Лопез Рібалда та інші проти Іспанії» (López Ribalda and Others v. Spain)* [ВП], 2019, § 134). І навпаки, прості підозри у привласненні або будь-якому іншому правопорушенні з боку працівників не можуть виправдати встановлення роботодавцем негласного відеоспостереження (*там само*, § 134).

149. У справі *«Барбулеску проти Румунії» (Bărbulescu v. Romania)* [ВП], 2017 (§ 121) Суд визначив низку критеріїв, яким мають відповідати заходи, спрямовані на нагляд за кореспонденцією та спілкуванням працівників на робочому місці, щоб вони не порушували статтю 8. У цьому контексті національні органи влади повинні відповісти на такі питання: чи був працівник повідомлений про можливість того, що роботодавець може вжити заходів для контролю за кореспонденцією та іншими повідомленнями, а також про здійснення таких заходів? Який був ступінь моніторингу з боку роботодавця та ступінь втручання в приватне життя працівника? Чи надав роботодавець законні підстави для моніторингу комунікацій працівника? Чи можна було б створити систему моніторингу, засновану на менш інтрузивних методах і заходах, ніж безпосередній доступ до вмісту повідомлень працівника? Якими були наслідки моніторингу для працівника, щодо якого здійснювався моніторинг? Чи було надано

працівнику адекватні гарантії, особливо коли операції моніторингу роботодавця мали інтрузивний характер? Нарешті, національні органи влади повинні забезпечити, щоб працівник, комунікації якого відстежувалися, мав доступ до засобу правового захисту в судовому органі, який має відповідну юрисдикцію, щоб визначити, принаймні по суті, як було дотримано критеріїв, викладених вище, і чи були оскаржувані заходи законними (*там само*, § 122).

150. Згодом, у справі *«Лопез Рібалда та інші проти Іспанії» (López Ribalda and Others v. Spain)* [ВП], 2019 (§ 116), Суд вказав, що ці критерії можуть бути застосовані до заходів відеоспостереження, що здійснюються роботодавцем на робочому місці. У справі *«Флоріндо де Альмейда Васконселос Грамаксо проти Португалії» (Florindo de Almeida Vasconcelos Gramaxo v. Portugal)*, 2022 (§ 115), Суд також застосував зазначені критерії в контексті моніторингу роботодавцем за допомогою системи GPS відстаней, подоланих працівником на службовому автомобілі.

151. Суд встановлював порушення статті 8 у випадках, коли національні суди не змогли забезпечити, щоб застосування роботодавцем заходів нагляду було пропорційним і супроводжувалося належними та достатніми гарантіями. У справі *«Барбулеску проти Румунії» (Bărbulescu v. Romania)* [ВП], 2017 (§§ 108-141), національні суди не змогли визначити конкретні причини, що виправдовують застосування заходів спостереження, чи міг працівник вдатися до менш інтрузивних заходів щодо приватного життя та кореспонденції працівника, або чи був працівник заздалегідь повідомлений роботодавцем про можливий моніторинг його комунікацій. Навпаки у справі *«Ліберт проти Франції» (Libert v. France)*, 2018 (§§ 37-53) Суд не знайшов порушення статті 8 щодо відкриття особистих файлів, що зберігалися на робочому комп'ютері, порнографічний зміст яких став підставою для звільнення працівника. Він зазначив, що національне законодавство, як його тлумачив і застосовував національний суд, містило адекватні гарантії проти свавілля, включаючи той факт, що роботодавцю було дозволено відкривати файли з позначкою «особисте» лише у присутності працівника.

152. На думку Суду, лише переважна вимога, пов'язана із захистом значних суспільних або приватних інтересів, може виправдати ненадання роботодавцем працівникам попередньої інформації про заходи, які можуть порушити захист персональних даних працівників (*«Лопез Рібалда та інші проти Іспанії» (López Ribalda and Others v. Spain)* [ВП], 2019, § 133). Перед здійсненням заходів зі збору їхніх даних роботодавці повинні інформувати відповідних працівників про існування та умови такого збору даних, хоча б у загальних рисах (*там само*, § 131). Вимога прозорості та пов'язане з нею право на інформацію фундаментальні, особливо в контексті трудових відносин, де роботодавець має значні повноваження щодо працівників, і слід уникати будь-яких зловживань цими повноваженнями. Однак надання інформації особі, за якою здійснюється моніторинг, та її обсяг є лише одним із критеріїв, які слід брати до уваги для оцінки пропорційності такого заходу в конкретному випадку. Однак, якщо така інформація відсутня, гарантії, що впливають з інших критеріїв, будуть ще більш важливими (*там само*, § 131).

153. Якщо попередня інформація не була надана, важливо з'ясувати, чи мали працівники, за якими велося спостереження, у своєму розпорядженні національні засоби правового захисту, спеціально призначені для забезпечення ефективного захисту права на повагу до приватного життя. У рамках заходів, що застосовуються до працівників на робочому місці, такий захист може бути забезпечений різними засобами, які можуть належати до трудового права, а також до цивільного, адміністративного або кримінального права (*там само*, § 136).

154. Що стосується більш конкретно відеоспостереження за працівниками, то у справі *«Лопез Рібалда та інші проти Іспанії» (López Ribalda and Others v. Spain)* [ВП], 2019 (§ 125) Суд зазначив, що при аналізі пропорційності заходів відеоспостереження необхідно розрізняти різні місця, в яких здійснювався моніторинг, у світлі захисту приватного життя, на який

працівник міг би обґрунтовано очікувати. Ці очікування дуже високі в місцях, які є приватними за своєю природою, таких як туалети або гардеробні, де виправдані посилені захист або навіть повна заборона відеоспостереження (*там само*, §§ 125, 61, 65, з посиланням на відповідні міжнародні документи). Він залишається високим у закритих робочих приміщеннях, таких як кабінети, і значно нижчим у місцях, які є видимими або доступними для колег або широкої громадськості (*там само*, § 125).

155. У зв'язку з цим, у справі *«Кьорке проти Німеччини» (Körke v. Germany)* (ухв.), 2010, Суд визнав неприйнятною як явно необґрунтовану скаргу заявниці, касирки супермаркету, щодо прихованого відеоспостереження, яке здійснювалося її роботодавцем за допомогою приватного детективного агентства. Суд зазначив, зокрема, що оскаржуваний захід був обмежений у часі (два тижні) і охоплював лише загальнодоступну зону навколо каси, що отримані відеодані оброблялися обмеженою кількістю осіб, які працювали в детективному агентстві, і співробітниками роботодавця, і що вони використовувалися виключно в рамках процедури звільнення заявниці та розгляду справи в суді з трудових спорів.

156. І навпаки, у рішенні у справі *«Антовіч і Мірковіч проти Чорногорії» (Antović and Mirković v. Montenegro)*, 2017 (§§ 55-60), Суд встановив порушення статті 8 на тій підставі, що передбачуване втручання в приватне життя заявників, двох професорів університету, в результаті встановлення системи відеоспостереження в університетських аудиторіях, де вони проводили заняття, не було передбачено законом.

157. У справі *«Лопез Рібалда та інші проти Іспанії» (López Ribalda and Others v. Spain)* [ВП], 2019 (§ 137), Суд не встановив порушення статті 8 щодо частково відкритого та прихованого відеоспостереження за касирами та продавцями в супермаркеті, беручи до уваги, серед іншого, суттєві гарантії, передбачені іспанським законодавством, включаючи засоби правового захисту, якими заявники не скористалися.

158. Аналогічно справа *«Флоріндо де Альмейда Васконселос Грамаксо проти Португалії» (Florindo de Almeida Vasconcelos Gramaxo v. Portugal)*, 2022 (§§ 105-125) стосувалося звільнення заявника на підставі даних про пробіг, зафіксованих за допомогою системи GPS, встановленої роботодавцем на його службовому автомобілі. Суд не встановив порушення статті 8, зазначивши, що національні суди ретельно збалансували право заявника на приватне життя з правом роботодавця забезпечувати ефективну роботу компанії, враховуючи законну мету контролю за витратами, яку ставила перед собою компанія.

159. Подібні принципи також застосовуються в інших контекстах, зокрема, щодо моніторингу політичною партією електронних комунікацій своїх членів, навіть незважаючи на те, що внутрішні організаційні структури політичних партій відрізняються від структур приватних компаній і що правові зв'язки, які існують між роботодавцем і працівником та між політичною партією та її членами, принципово відрізняються (*«Тена Арреґуї проти Іспанії» (Tena Arregui v. Spain)*, 2024, §§ 38 і 41).

с. Збирання даних для використання як доказів у судових справах

160. Збір реальних доказів у рамках судових справ піднімає питання, пов'язані із захистом персональних даних фізичних осіб, незалежно від їхнього статусу в провадженні, як сторін, свідків або третіх осіб.

і. Обшуки та вилучення

161. У кількох справах Суд підкреслив, що Договірні Держави могли вважати за необхідне вдатися до таких заходів, як обшуки та вилучення, з метою отримання речових доказів певних правопорушень (*«Васильчук проти України» (Vasylchuk v. Ukraine)*, 2013, § 79; *«К.С. та М.С. проти Німеччини» (K.S. and M.S. v. Germany)*, 2016, § 43). У таких випадках перевірка заходів

буде спрямована на релевантність і достатність причин, наведених для їх виправдання, а також на дотримання принципу їх пропорційності переслідуваній меті («Смірнов проти Росії» (*Smirnov v. Russia*), 2007, § 44). Серйозність правопорушення, яке стало підставою для проведення обшуку та вилучення, обставини, за яких було видано постанову, зокрема, чи були на той момент наявні додаткові докази, зміст та обсяг постанови, з особливою увагою до характеру обшукуваного приміщення та гарантій, вжитих з метою обмеження впливу цього заходу до розумних меж, спосіб проведення обшуку та ступінь можливих наслідків для поваги до приватного життя відповідної особи, є важливими критеріями, які мають бути враховані при збалансуванні різних конкуруючих інтересів (*там само*, § 44; «Модесту проти Греції» (*Modestou v. Greece*), 2017, § 42 та посилання в ньому). Суд також вимагає, щоб національне законодавство забезпечувало належні та достатні гарантії проти свавілля («Вінчі Констракшен та ДжіТіЕм Жені Сівіл енд Сервісіс проти Франції» (*Vinci Construction and GTM Génie Civil and Services v. France*), 2015, § 66; «Модесту проти Греції» (*Modestou v. Greece*), 2017, § 43). Такі гарантії включають наявність «ефективного контролю» заходів, що порушують статтю 8 (*там само*, § 42).

162. У справі «Трабайо Рueda проти Іспанії» (*Trabajo Rueda v. Spain*), 2017 (§§ 44-47), вилучення персонального комп'ютера заявника, яке дозволило поліції отримати доступ до всіх особистих файлів, що зберігалися в комп'ютері, на підставі того, що він містив матеріали дитячої порнографії, було визнано таким, що суперечить статті 8. Суд не був переконаний у невідкладності ситуації, що вимагала від поліції вилучити файли з персонального комп'ютера заявника й отримати доступ до всіх даних, що зберігалися, без отримання попереднього судового дозволу, який зазвичай вимагається, навіть якщо такий дозвіл можна було отримати досить швидко.

163. У справі «К.С. та М.С. проти Німеччини» (*K.S. and M.S. v. Germany*), 2016 (§§ 32-58), Суд не знайшов порушення статті 8 щодо обшуку житла заявників за ордером, виданим на підставі інформації, яка містила персональні дані, незаконно скопійовані співробітником банку, а потім продані спецслужбам, про їхні активи в банку за кордоном. Німецьке законодавство та практика надавали адекватні та ефективні гарантії проти зловживань. Крім того, національні суди не вийшли за межі своєї свободи розсуду, обґрунтовуючи ордер на обшук даними, що походять з-за кордону. Зокрема, Суд надав особливої ваги тому факту, що на момент видачі ордеру на обшук німецькими органами влади було придбано дуже мало відповідних наборів даних, якщо вони взагалі були придбані, окрім того, про який йде мова (*там само*, § 51). Той факт, що не існує абсолютного правила, згідно з яким докази, отримані з порушенням процесуальних норм, не можуть бути використані в кримінальному провадженні, також не означає, що органи влади навмисно отримали дані з порушенням міжнародного або національного законодавства (*там само*, § 51). Більше того, носій даних містив інформацію про фінансовий стан заявників, яку вони були зобов'язані подавати до національних податкових органів, але не містив даних, тісно пов'язаних з їхньою особою (*там само*, § 53; порівняйте «Г.С.Б. проти Швейцарії» (*G.S.B. v. Switzerland*), 2015, § 93, щодо передачі банківських реквізитів податковим органам іншої Держави відповідно до двосторонньої угоди).

164. Обшуки, що проводяться в офісних приміщеннях з метою збору реальних доказів, піднімають питання щодо захисту їхніх даних під кутом зору права на повагу до «кореспонденції» та «житла», що гарантується статтею 8. Наприклад, у справі «Берн Ларсен Голдинг АС та інші проти Норвегії» (*Bernh Larsen Holding AS and Others v. Norway*), 2013 (§§ 104-175) Суд не знайшов порушення статті 8 щодо рішення, яке зобов'язувало компанію надати резервну копію всіх даних на комп'ютерному сервері, який вона використовувала спільно з іншими компаніями. Хоча вимога попереднього судового дозволу не застосовувалася, Суд взяв до уваги ефективні та адекватні гарантії проти зловживань, інтереси компаній та їхніх працівників, а також суспільний інтерес в ефективній податковій перевірці

(там само, §§ 172-175). З іншого боку, у справі «ДЕЛЬТА ПЕКАРНИ а.с. проти Чеської Республіки» (*DELTA PEKÁRNY a.s. v. Czech Republic*), 2014 (§§ 92-93), Суд констатував порушення статті 8, що стосувалося огляду офісних приміщень з метою отримання доказів існування незаконної угоди про ціни, що порушує правила конкуренції. Суд послався на відсутність попереднього дозволу судді, ефективного *post hoc* перегляду необхідності цього заходу та правил щодо можливого знищення отриманих даних.

165. У справі «Бук проти Німеччини» (*Buck v. Germany*), 2005 (§§ 30-53), обшук офісних і житлових приміщень заявника у зв'язку з порушенням правил дорожнього руху, вчиненим третьою особою, становив порушення статті 8. Беручи до уваги особливі обставини цієї справи, зокрема той факт, що обшук і вилучення, про які йдеться, були призначені у зв'язку з незначним порушенням нормативно-правового акта, яке нібито було вчинено третьою особою, і стосувалися приватного житла заявника, Суд дійшов висновку, що втручання не може вважатися пропорційним переслідуванню законним цілям (там само, § 52).

166. Що стосується обшуків професійних приміщень, будинків і приватних транспортних засобів журналістів (у деяких випадках), а також масових вилучень з метою виявлення джерел інформації, Суд встановив порушення статті 8 у справі «Ернст та інші проти Бельгії» (*Ernst and Others v. Belgium*), 2003 (§§ 110-117). У зв'язку з боротьбою з порушенням таємниці судового слідства, законодавство і практика Договірних Держав, які можуть передбачати обшуки житла і вилучення, повинні надавати адекватні та достатні гарантії проти зловживань. У цій справі ситуація не була такою, оскільки проти заявників не було висунуто жодних обвинувачень, а різні ордери на обшук були сформульовані широко, не надаючи жодної інформації про оскаржуване розслідування, конкретні приміщення, які підлягали обшуку, або предмети, що підлягали вилученню, таким чином, залишаючи слідчим широке поле для маневру. Крім того, заявники не були поінформовані про фактичні причини обшуків (див. також пункт **Error! Reference source not found.** нижче щодо порушення статті 10 у цій справі).

167. Що стосується вилучень, які здійснюються в юридичній практиці, вони завжди повинні супроводжуватися спеціальними процесуальними гарантіями, такими як захист конфіденційності даних, що лежать в основі довірчих відносин між адвокатом і клієнтом⁸. У справі «Кірдьок та інші проти Туреччини» (*Kirdök and Others v. Turkey*), 2019 (§§ 52-58), виїмка електронних даних кількох адвокатів судовими органами для цілей кримінального провадження проти іншого адвоката, який ділив з ними офіс, і відмова повернути ці дані або знищити їх становили порушення статті 8. Суд надав значення тому факту, що під час обшуку не було дотримано жодної процедури фільтрації електронних документів або даних, що становлять професійну таємницю. Крім того, відмова повернути вилучені дані на тій підставі, що, оскільки вони ще не були розшифровані, не було можливості встановити, кому вони належать, не була чітко прописана в законі й суперечила самій суті професійної таємниці, яка передбачає конфіденційність цих даних.

168. У справі «Круглов та інші проти Росії» (*Kruglov and Others v. Russia*), 2020 (§§ 123-138), Суд постановив, що вилучення комп'ютерів і жорстких дисків, які містили особисту інформацію та документи, що становлять професійну таємницю заявників, які були адвокатами за професією, або їхніх клієнтів, під час обшуків, проведених поліцією в їхніх будинках та офісах, без будь-якої фільтрації вилучених даних, суперечило статті 8. Зокрема, існування попереднього судового дозволу має обмежений вплив, оскільки національні суди ніколи не намагалися збалансувати зобов'язання захищати конфіденційність даних з потребами

⁸ Див. також [Посібник зі статті 8 Конвенції \(право на повагу до приватного і сімейного життя\)](#), щоб отримати більш детальну інформацію про процесуальні гарантії, що застосовуються до вилучень, які здійснюються в юридичній практиці.

кримінального розслідування, наприклад, розглядаючи можливість отримання інформації з інших джерел (*там само*, §§ 126-129).

169. Суд також встановив порушення статті 8 у справі «Смірнов проти Росії» (*Smirnov v. Russia*), 2007 (§§ 36-49), щодо обшуку та вилучення великої кількості документів і блоку комп'ютера адвоката в його будинку без обґрунтування та гарантій; у справі «Візер енд Бікос Бетейлігунген ГмбХ проти Австрії» (*Wieser and Bicos Beteiligungen GmbH v. Austria*), 2007 (§§ 42-68), щодо обшуків та вилучення електронних даних адвоката з порушенням процесуальних гарантій, передбачених законом; у справі «Робатін проти Австрії» (*Robathin v. Austria*), 2012 (§ 52), щодо недостатньо обґрунтованого дозволу на обшук та вилучення всіх електронних даних, що зберігаються в юридичній практиці; та у справі «Серґава проти Естонії» (*Särgava v. Estonia*), 2021 (§§ 107-108), щодо процесуальних гарантій, які були визнані недостатніми для захисту даних, що становлять професійну таємницю, після вилучення та подальшого дослідження комп'ютера та мобільного телефону адвоката.

170. У справі «Вінчі Констракшен та ДжіТіЕм Жені Сівіл енд Сервісіс проти Франції» (*Vinci Construction and GTM Génie Civil and Services v. France*), 2015 (§§ 69-81), Суд визнав порушення статті 8 щодо обшуку та вилучення комп'ютерних даних, що належать компаніям, включаючи електронні повідомлення, які підпадають під конфіденційність відносин між адвокатом і клієнтом. Суд першої інстанції, визнавши наявність листування адвоката серед вилучених слідчими документів, обмежився лише оцінкою законності формальних підстав для оскаржуваних вилучень без проведення необхідної детальної експертизи.

171. У справі «Андре та інші проти Франції» (*André and Others v. France*), 2008 (§§ 37-49), «домашній» обшук і вилучення документів в юридичній практиці податківцями з метою отримання доказів проти однієї з компаній-клієнтів становило порушення статті 8. Метою обшуку, про який йде мова, було виявлення в приміщеннях заявників, виключно в їхній ролі адвокатів компанії, підозрюваної в шахрайстві, документів, здатних встановити наявність такого шахрайства з боку компанії, і використання таких документів як доказів проти неї. На жодному етапі заявники не були звинувачені або підозрювалися у вчиненні злочину або причетності до шахрайства, вчиненого компанією-клієнтом (*там само*, § 46).

172. Друге вилучення, здійснене через п'ять хвилин після повернення незаконно конфіскованих матеріалів, становило порушення статті 8 у справі «Вісі проти Словаччини» (*Visy v. Slovakia*), 2018 (§§ 33-47). Заявник був позбавлений будь-яких ефективних гарантій проти свавілля та зловживань щодо другого вилучення.

173. У справі «Шер та інші проти Сполученого Королівства» (*Sher and Others v. the United Kingdom*), 2015 (§§ 171-176), справі про тероризм, Суду довелося розглянути питання про ордер на обшук, який можна було продовжити у випадках підозри в терористичній діяльності. Суд постановив, що складність, притаманна таким справам, може виправдати проведення обшуку на більш широких підставах, ніж це було б допустимо в іншому випадку. Встановлення відповідно до статті 8 вимоги, щоб в ордері на обшук детально визначався точний характер предметів, які шукаються і підлягають вилученню, може серйозно поставити під загрозу ефективність розслідування, коли під загрозою може опинитися життя багатьох людей. У таких випадках поліція повинна мати певну свободу дій, щоб на основі виявлених під час обшуку предметів визначити, які з них можуть бути пов'язані з терористичною діяльністю, і вилучити їх для подальшого вивчення (*там само*, § 74).

174. У справі «Івашченко проти Росії» (*Ivashchenko v. Russia*), 2018 (§§ 59-95), повноваження митних органів зазирати у та копіювати електронні дані фізичних осіб становили порушення статті 8 за відсутності обґрунтованих підозр у вчиненні правопорушень. Копіювання особистих і професійних даних заявника з подальшою передачею їх для проведення спеціалізованої експертизи, а також зберігання його даних протягом близько двох років виходило за рамки того, що можна вважати ненав'язливими «рутинними» процедурами, на які зазвичай дається

згода. Заявник не мав можливості обирати, чи бажає він представити себе та свої речі митниці та пройти митний огляд. (Див. також *«Гіллан і Кінтон проти Сполученого Королівства»* (*Gillan and Quinton v. the United Kingdom*), 2010, §§ 61-67, щодо повноважень зупиняти й обшукувати осіб без будь-яких правдоподібних підстав підозрювати їх у вчиненні правопорушення, що становило порушення статті 8. Суд зазначив, що публічний характер обшуку, під час якого особа відчуває збентеження через те, що її особиста інформація стає доступною іншим особам, може навіть у певних випадках посилювати серйозність втручання у приватне життя особи через елемент приниження та збентеження. Розсуд, яким користуються працівники міліції, викликає занепокоєння: вони не тільки не зобов'язані демонструвати наявність будь-якої обґрунтованої підозри, але й не повинні навіть суб'єктивно підозрювати щось про особу, яку зупиняють і обшуковують).

ii. Примусові медичні дії для отримання клітинних зразків

175. Загалом, використання різних примусових медичних заходів для взяття клітинних зразків, таких як аналізи крові та мазки з ротової порожнини, не заборонено як таке в контексті збору доказів у цивільному або кримінальному провадженні (*«Яллох проти Німеччини»* (*Jalloh v. Germany*) [ВП], 2006, § 70; *«Каруана проти Мальти»* (*Caruana v. Malta*) (ухв.), 2018, § 41; *«Д.Г. та інші проти Північної Македонії»* (*D.H. and Others v. North Macedonia*), 2023, § 52).

176. Зокрема, у справі *«Д.Г. та інші проти Північної Македонії»* (*D.H. and Others v. North Macedonia*), 2023 (§§ 52-53) Суд дійшов висновку, що взяття зразків крові у заявників, усіх секс-працівників, за підозрою у злочині, пов'язаному з поширенням хвороб, що передаються статевим шляхом, не порушувало вимог статті 8, оскільки ця медична дія була призначена суддею, проведена лікарем у клініці, і заявники ніколи не стверджували, що ця дія була пов'язана з надмірним застосуванням сили або завдала шкоди їхньому здоров'ю. Таким чином, відповідну скаргу було відхилено як явно необґрунтовану.

177. У справі *«Мікуліч проти Хорватії»* (*Mikulić v. Croatia*), 2002 (§ 64), Суд постановив, що відсутність будь-якого процесуального заходу для примусу передбачуваного батька до проходження тесту ДНК відповідає принципу пропорційності лише в тому випадку, якщо були забезпечені альтернативні засоби для визначення батьківства. Суд встановив порушення статті 8, оскільки національне законодавство не передбачало таких засобів, прирікаючи заявницю на подальшу тривалу невизначеність щодо її особистої ідентичності через відмову передбачуваного батька пройти ДНК-тестування (*там само*, §§ 65-66).

178. У справі *«Міфсуд проти Мальти»* (*Mifsud v. Malta*), 2019 (§§ 61-78), судовий наказ, виданий заявнику для проходження генетичного тестування проти його волі в рамках провадження щодо батьківства відповідно до законодавства Мальти, не суперечив статті 8. Перш ніж зобов'язати заявника пройти ДНК-тестування, національні суди провели необхідну процедуру збалансування конкуруючих інтересів у справі в рамках судового розгляду, в якому заявник брав участь, будучи представленим захисником за власним вибором, і де його процесуальні права було дотримано нарівні з протилежною стороною. Таким чином, національні суди встановили справедливий баланс між інтересом передбачуваної дочки заявника у встановленні батьківства та інтересом заявника не проходити ДНК-тест (*там само*, § 77). Загалом, процес прийняття рішення був справедливим і належним чином захистив інтереси заявника, гарантовані статтею 8.

179. У справі *«Болевіч проти Сербії»* (*Boljević v. Serbia*), 2020 (§§ 50-56), Суд постановив, що відхилення національними судами заяви про перегляд остаточного рішення, винесеного сорок один рік тому, яке дозволяло чоловікові оскаржити батьківство, в той час, коли тестування ДНК ще не існувало, суперечило статті 8. Суд дійшов висновку, що збереження правової визначеності не може бути достатньою підставою для позбавлення заявника права знати правду про важливий аспект його особистої ідентичності без збалансування конкуруючих

інтересів у справі. Національне законодавство щодо строків поновлення провадження у справі не дозволило органам влади здійснити таке врівноваження, враховуючи дуже специфічні обставини справи заявника, а саме те, що заявник дізнався про остаточне рішення щодо батьківства свого передбачуваного батька лише після смерті останнього. Суд постановив, що на приватне життя померлої особи, у якої має бути взятий зразок ДНК, не може негативно вплинути прохання про це, зроблене після її смерті. Раніше Суд ухвалив аналогічне рішення у справах *«Сексешен Крестен Фільтенборг Мортесен проти Данії» (Succession Kresten Filtenborg Mortensen v. Denmark)* (ухв.), 2006, щодо ексгумації трупа для проведення генетичного тестування, та *«Йеггі проти Швейцарії» (Jäggi v. Switzerland)*, 2006 (§ 42), де відмова судів надати дозвіл на проведення ДНК-тестування померлої особи на вимогу передбачуваного сина останньої з метою встановлення особи його справжнього батька становила порушення статті 8 (*там само*, §§ 34-44).

180. У справі *«Каруана проти Мальти» (Caruana v. Malta)* (ухв.), 2018 (§§ 28-42), Суд визнав явно необґрунтованою скаргу, що стосувалася зобов'язання дружини ймовірного вбивці здати зразки з внутрішньої поверхні щік. Суд постановив, що булакальний мазок — це незначне втручання, яке рідко спричиняє тілесні ушкодження або фізичні чи моральні страждання. Вбивство було серйозним кримінальним злочином, тому було розумним і необхідним зібрати якомога більше доказів (*там само*, § 41). Крім того, Суд провів різницю між становищем свідка й обвинуваченого, відмова якого від такого заходу в рамках кримінального провадження може вплинути на остаточне визнання вини та пов'язані з цим санкції (*там само*, § 40).

181. У справ *«Драган Петровіч проти Сербії» (Dragan Petrović v. Serbia)*, 2020 (§§ 79-84), взяття булакального мазка в рамках розслідування вбивства було визнано порушенням статті 8 через відсутність відповідних правових положень. Той факт, що заявник погодився надати зразок своєї слини співробітникам міліції, не мав значення для того, чи відбулося втручання в його приватне життя, оскільки він зробив це лише під загрозою того, що, в іншому випадку, зразок слини або крові буде взятий у нього силою (*там само*, § 79).

182. Суд також встановив порушення статті 8 у справі про збір медичних даних у Свідків Єгови, які відмовилися від переливання крові (*«Авілкіна та інші проти Росії» (Avilkina and Others v. Russia)*, 2013); див. також п. 188 вище.

183. Порушення статті 8 також було встановлено у справі про вилучення органів з тіла померлих осіб з метою трансплантації без відома або згоди їхніх близьких родичів (*«Петрова проти Латвії» (Petrova v. Latvia)*, 2014, §§ 87-98), а також у ситуації з неясністю національного законодавства щодо згоди близького родича на вилучення тканин з тіла померлої особи (*«Ельберте проти Латвії» (Elberte v. Latvia)*, 2015, §§ 105-117).

d. Збір персональних даних у медичному контексті

184. Суд розглядав питання збору чутливих даних у медичній сфері. У справі *«Л.Г. проти Латвії» (L.H. v. Latvia)*, 2014 (§§ 47-60), збір медичних даних про пацієнта в державній лікарні державним органом, відповідальним за контроль якості медичної допомоги, було визнано таким, що не відповідає статті 8 через відсутність чітко сформульованого законодавства, яке б забезпечувало належний правовий захист від свавілля. Агентство збирало дані протягом семи років безсистемно, без будь-якої попередньої оцінки того, чи будуть зібрані дані «потенційно вирішальними», «релевантними» або «важливими» для досягнення мети розслідування. Воно також не було зобов'язане запитувати й отримувати згоду заявника на збір його даних (*там само*, § 53). Обсяг приватних даних, які могли бути зібрані, не був жодним чином обмежений (*там само*, § 57). Більше того, доречність і достатність підстав для збирання інформації, як видається, не розглядалися на жодному етапі національної процедури (*там само*, § 57). У цьому контексті Суд вважав менш важливим те, чи мав орган юридичний обов'язок зберігати конфіденційність персональних даних (*там само*, § 58).

185. У справі *«Суріков проти України» (Surikov v. Ukraine)*, 2017 (§§ 75-95), збирання та зберігання персональних даних про психічне здоров'я особи протягом тривалого періоду, а також передача та використання цих даних з метою, не пов'язаною з початковими причинами їх збору, становили непропорційне втручання у право суб'єкта даних на повагу до його приватного життя, що порушує статтю 8. Хоча роботодавці можуть мати законний інтерес до інформації про психічне й фізичне здоров'я своїх працівників, особливо в контексті призначення їм певних робочих функцій, пов'язаних із конкретними навичками або обов'язками, збирання і обробка відповідної інформації повинні бути законними й забезпечувати справедливий баланс між інтересами роботодавця і правом кандидата на захист приватного життя (*там само*, § 91).

186. У справі *«Z проти Фінляндії» (Z v. Finland)*, 1997 (§§ 106-110), Суд не знайшов порушення статті 8 щодо вилучення медичної документації та її включення до матеріалів слідства без попередньої згоди пацієнтки в рамках кримінального провадження проти її чоловіка. Не було жодних порушень у процесі прийняття рішення, і були доступні засоби правового захисту для оскарження вилучення та скасування строку, встановленого в постанові про конфіденційність.

187. Справа *«Дрелон проти Франції» (Drelon v. France)*, 2022 (§§ 79-100) стосувалася спроби заявника здати кров у пункті збору французької Служби донорства крові та відмови прийняти його як донора крові на підставі його передбачуваної гомосексуальності. Хоча заявник відмовився відповідати на питання про своє статеве життя під час медичної бесіди перед донацією, дані включали протипоказання до здачі крові, характерні для чоловіків, які мали статеві стосунки з іншими чоловіками. Відзначивши чутливий характер зазначених даних, Суд визнав, що їх збирання і зберігання ґрунтувалися на відповідних і достатніх підставах, зокрема, на охороні здоров'я і важливості забезпечення безпеки крові. Водночас він зазначив, що зібрані дані ґрунтувалися лише на припущеннях без будь-якого доведеного фактичного підґрунтя. Він також звернув увагу на надмірну тривалість зберігання даних, що уможливило їх повторне використання проти заявника, що призвело до його автоматичного виключення з числа донорів крові. З огляду на ці елементи, Суд встановив порушення статті 8 Конвенції.

е. Примусова передача персональних даних

188. Суд неодноразово оцінював зобов'язання операторів мобільного зв'язку, інтернет-провайдерів, банків, елітних спортсменів і лікарень надавати органам влади персональні дані, якими вони володіють, відповідно до закону або наказу, виданого державними органами.

189. Що стосується боротьби з організованою злочинністю та тероризмом, Суд визнав, що методи розслідування повинні бути адаптовані до сучасних комунікаційних технологій. У справі *«Бреєр проти Німеччини» (Breyer v. Germany)*, 2020 (§§ 81-110), юридичний обов'язок операторів мобільного зв'язку записувати персональні дані користувачів передплачених SIM-карт і надавати їх органам влади відповідно до Закону про телекомунікації, який уповноважував різні державні органи вимагати отримання та передачу таких даних без необхідності судового рішення або повідомлення зацікавлених осіб, не був визнаний таким, що суперечить статті 8. Зберігався лише обмежений набір даних, і не зберігалися дані, що стосувалися окремих комунікаційних подій; отже, втручання було досить незначним (*там само*, §§ 92-95). Існувала також низка запобіжних заходів: страхування технічної безпеки, обмежений період зберігання, дані, обмежені необхідною інформацією для чіткої ідентифікації відповідного абонента; врегульовані можливості для майбутніх консультацій та використання збережених даних; нагляд з боку незалежного органу; та можливості оскарження для будь-кого, хто вважає, що його права були порушені, хоча рівень перевірки та нагляду не був вирішальним елементом в оцінці пропорційності збирання та зберігання такого обмеженого набору даних (*там само*, §§ 96-107).

190. І навпаки, Суд постановив, що покладення юридичного обов'язку на інтернет-провайдерів отримати збережені дані про з'єднання або одного зі своїх абонентів і передати їх поліції становило порушення статті 8, оскільки правові положення, на які спиралася поліція, були нечіткими і не забезпечували захисту від свавільного втручання, особливо за відсутності незалежного нагляду за відповідними повноваженнями поліції (*«Бенедік проти Словенії» (Benedik v. Slovenia)*, 2018, §§ 132-134).

200. У справі *«Зоммер проти Німеччини» (Sommer v. Germany)*, 2017 (§ 63), перевірка банківського рахунку адвоката становила порушення статті 8 з огляду на низький поріг для перевірки банківського рахунку заявника, широкий обсяг запитів на інформацію, подальше розголошення та подальше зберігання особистої інформації заявника, а також недостатність процесуальних гарантій.

191. У справі *«Авілікіна та інші проти Росії» (Avilkina and Others v. Russia)*, 2013 (§ 54), щодо збирання медичних даних про Свідків Єгови, які відмовилися від переливання крові, Суд постановив, що збирання прокуратурою даних про заявників у медичному закладі, де їх лікували, без інформування суб'єктів даних або надання їм можливості заперечити, був несумісний зі статтею 8. У прокуратури були інші можливості для перевірки скарг на відповідну релігійну організацію, зокрема, шляхом допиту відповідних осіб або отримання їхньої згоди (*там само*, § 48).

192. У справі *«Національна федерація асоціацій і спілок спортсменів та інші проти Франції» (National Federation of Sportspersons' Associations and Unions (FNASS) and Others v. France)*, 2018 (§§ 155-191), вимога щодо інформування про місцезнаходження, накладена на «пул тестування» елітних спортсменів з метою проведення раптових допінг-тестів в рамках антидопінгової кампанії, що передбачає великі штрафи після третього невиконання протягом вісімнадцяти місяців поспіль, не була визнана такою, що суперечить статті 8. Не применшуючи вплив вимог щодо місцезнаходження на приватне життя заявників, Суд постановив, що зменшення або скасування цих вимог могло б підвищити небезпеку допінгу для здоров'я як самих спортсменів, так і всієї спортивної спільноти, а також суперечило б європейському та міжнародному консенсусу щодо необхідності тестування без попередження (*там само*, § 191).

193. У справі *«Айкагуер проти Франції» (Aycaguer v. France)*, 2017 (§§ 45-47), Суд встановив порушення статті 8 на тій підставі, що кримінальне засудження заявника за відмову пройти обов'язковий біологічний тест для внесення його ДНК-профілю до національної комп'ютеризованої бази даних засуджених осіб не може розглядатися як захід, необхідний у демократичному суспільстві. Заявник вчинив дії (які призвели до наказу примусового проходження ДНК-тестування) у політичному / профспілковому контексті, що стосувалися ударів парасолькою по жандармах, яких навіть не було ідентифіковано, за що його засудили до двох місяців умовного позбавлення волі. Однак національна комп'ютеризована база даних ДНК не передбачала жодної диференціації залежно від характеру та тяжкості вчиненого злочину, що відображає значну різницю у можливих ситуаціях, як це показує випадок заявника (*там само*, § 43). Заявник також не мав доступу до процедури видалення збережених даних (така процедура передбачена лише для підозрюваних у злочинах, а не для засуджених осіб) (*там само*, § 43).

2. Зберігання персональних даних

194. Зберігання державними органами інформації, що стосується приватного життя особи, незалежно від способу її отримання, становить втручання у право на повагу до приватного життя суб'єкта даних у розумінні статті 8, навіть якщо ці дані згодом не використовуються (*«Амман проти Швейцарії» (Amman v. Switzerland)* [ВП], 2000, § 69; *«Ротару проти Румунії» (Rotaru v. Romania)* [ВП], 2000, § 46; *«С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom)* [ВП], 2008, § 67; *«М.К. проти Франції» (M.K. v. France)*, 2013, § 29;

«Айкагуер проти Франції» (Aysaquer v. France), 2017, § 33). Приватний характер цієї інформації вимагає від Суду ретельної перевірки будь-яких державних заходів, які дозволяють органам влади зберігати та використовувати її без згоди відповідної особи (*«С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom)* [ВП], 2008, § 104).

а. Зберігання персональних даних з метою боротьби зі злочинністю

195. Інтереси суб'єктів даних і суспільства загалом у захисті персональних даних, включно з інформацією про відбитки пальців і ДНК, можуть переважати над законним інтересом у запобіганні злочинам (*«С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom)* [ВП], 2008, § 104). Для належного захисту свого населення національні органи влади можуть законно створювати бази даних як ефективний засіб для покарання та запобігання певним правопорушенням, у тому числі найтяжчим злочинам, таким як сексуальні злочини (*«Б.Б. проти Франції» (B.B. v. France)*, 2009, § 62; *«Гардель проти Франції» (Gardel v. France)*, 2009, § 63; *«М.Б. проти Франції» (M.B. v. France)*, 2009, § 54; *«Н.Ф. та інші проти Росії» (N.F. and Others v. Russia)*, 2023, § 44). Первинне отримання цієї інформації має на меті пов'язати конкретну особу з конкретним злочином, у якому вона підозрюється, тоді як її зберігання має ширшу мету — допомогти у виявленні майбутніх правопорушників (*«С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom)* [ВП], 2008, § 100). Суд не ставить під сумнів превентивну мету таких реєстрів (*«Гардель проти Франції» (Gardel v. France)*, 2009, § 63; *«Б.Б. проти Франції» (B.B. v. France)*, 2009, § 62; *«М.Б. проти Франції» (M.B. v. France)*, 2009, § 54). Боротьба зі злочинністю, зокрема з організованою злочинністю і тероризмом, яка є одним із викликів для сучасних європейських суспільств, значною мірою залежить від використання сучасних наукових методів розслідування та ідентифікації (*«С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom)* [ВП], 2008, § 105). Водночас, оскільки захист персональних даних має основоположне значення для здійснення особою права на повагу до приватного і сімейного життя, гарантованого статтею 8 Конвенції, національне законодавство повинно передбачати відповідні гарантії для запобігання будь-якому такому використанню персональних даних, яке може бути несумісним з гарантіями цієї статті (*там само*, § 103; *«Глухін проти Росії» (Glukhin v. Russia)*, 2023, § 75).

196. Суд розглянув низку справ, пов'язаних із внесенням до баз даних, призначених для покарання та запобігання злочинам, осіб, засуджених за незначні правопорушення (*«М.К. проти Франції» (M.K. v. France)*, 2013, §§ 6, 8, 41; *«Айкагуер проти Франції» (Aysaquer v. France)*, 2017, §§ 8, 43), серйозні злочини (*«Б.Б. проти Франції» (B.B. v. France)*, 2009, §§ 6, 62; *«Гардель проти Франції» (Gardel v. France)*, 2009, §§ 8, 9, 63; *«М.Б. проти Франції» (M.B. v. France)*, 2009, §§ 6, 54; *«Перуззо і Мартенс проти Німеччини» (Peruzzo and Martens v. Germany)* (ухв.), 2013, §§ 6, 12, 37-38; *«Трайковські та Чіповські проти Північної Македонії» (Trajkovski and Chipovski v. North Macedonia)*, 2020, §§ 6, 12), або за низку правопорушень, які не були ні незначними, ні особливо серйозними (*«П.Н. проти Німеччини» (P.N. v. Germany)*, 2020, §§ 6, 81). Інші справи стосувалися зберігання в базах даних, призначених для покарання та запобігання злочинам, персональних даних осіб, які підозрювалися у вчиненні злочинів, але в кінцевому підсумку звинувачення були зняті (*«С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom)* [ВП], 2007, §§ 10, 11, 113; *«М.К. проти Франції» (M.K. v. France)*, 2013, §§ 7, 9, 42; *«Брунет проти Франції» (Brunet v. France)*, 2014, §§ 6, 7, 40), такі особи були виправдані (*«С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom)* [ВП], 2008, §§ 10, 113), або такі особи були просто попереджені після розгляду справи, без засудження (*«М.М. проти Сполученого Королівства» (M.M. v. the United Kingdom)*, 2012, §§ 7-9). В одній справі персональні дані заявників були зібрані й збережені в базі даних Міністерства внутрішніх справ лише на тій підставі, що в різний час вони піддавалися кримінальному переслідуванню. Існуюча система реєстрації охоплювала не лише судимості (і це незалежно від характеру та тяжкості відповідних правопорушень, і навіть від того, коли ці

судимості були зняті або погашені), але й ситуації, коли особа була притягнута до кримінальної відповідальності, а кримінальне провадження було згодом закрито з «нереабілітуючих підстав» («*Н.Ф. та інші проти Росії*» (*N.F. and Others v. Russia*), 2023, § 49). Нарешті інші справи стосувалися превентивних заходів, пов'язаних зі зберіганням персональних даних у поліцейських файлах на підставі лише підозр («*Шумоволос проти Росії*» (*Shimovolos v. Russia*), 2011, § 16; «*Хелілі проти Швейцарії*» (*Khelili v. Switzerland*), 2011, §§ 8, 9, 59; «*Кетт проти Сполученого Королівства*» (*Catt v. the United Kingdom*), 2019, §§ 6, 14, 119).

197. Наведені нижче фактори важливі при розгляді питання про необхідність зберігання персональних даних для цілей поліції.

і. Безсистемний і недиференційований характер збережених даних

198. У кількох справах Суд поставив під сумнів широке застосування системи зберігання даних, запровадженої органами влади, яка не робила розмежувань відповідно до характеру або ступеня тяжкості правопорушення, що призвело до засудження («*М.К. проти Франції*» (*M.K. v. France*), 2013, § 41; «*Айкагер проти Франції*» (*Ayscaguer v. France*), 2017, § 43; «*Горран проти Сполученого Королівства*» (*Gaughran v. the United Kingdom*), 2020, § 94; «*Н.Ф. та інші проти Росії*» (*N.F. and Others v. Russia*), 2023, § 49), або залежно від того, чи був суб'єкт даних засуджений, виправданий, звільнений чи лише попереджений про підозру у вчиненні правопорушення («*С. і Марпер проти Сполученого Королівства*» (*S. and Marper v. the United Kingdom*) [ВП], 2008, § 119; «*М.М. проти Сполученого Королівства*» (*M.M. v. the United Kingdom*), 2012, § 198; «*М.К. проти Франції*» (*M.K. v. France*), 2013, § 42; «*Брунет проти Франції*» (*Brunet v. France*), 2014, § 41; «*Н.Ф. та інші проти Росії*» (*N.F. and Others v. Russia*), 2023, § 49). Суд вважає, що засоби, створені органами влади для допомоги в покаранні та запобіганні певним правопорушенням, не можуть використовуватися з метою зловживань, спрямованих на максимізацію кількості інформації, що зберігається в них. Власне, без дотримання необхідної пропорційності відносно законних цілей, покладених на такі механізми, їхні переваги будуть переважені серйозними порушеннями прав і свобод, які держави повинні гарантувати відповідно до Конвенції особам, що перебувають під їхньою юрисдикцією («*М.К. проти Франції*» (*M. K. v. France*), 2013, § 35; «*Айкагер проти Франції*» (*Ayscaguer v. France*), 2017, § 34).

199. У справі «*С. і Марпер проти Сполученого Королівства*» (*S. and Marper v. the United Kingdom*) [ВП], 2008 (§§ 119, 125), база даних, у якій можна було збирати й зберігати відбитки пальців, біологічні зразки й профілі ДНК всіх підозрюваних, але не засуджених за кримінальні злочини, незалежно від їхнього віку, характеру й тяжкості злочинів, без обмеження в часі й без будь-якого незалежного розгляду обґрунтованості зберігання даних відповідно до визначених критеріїв, призвела до порушення статті 8. Всеохоплюючий і невибірковий характер такої системи не відображає справедливого балансу між конкуруючими державними й приватними інтересами.

200. Існує ризик стигматизації, коли з особами, які не були засуджені за будь-яке правопорушення і мають право на презумпцію невинуватості, поводяться так само, як із засудженими («*С. і Марпер проти Сполученого Королівства*» (*S. and Marper v. the United Kingdom*) [ВП], 2008, § 122). Хоча зберігання приватних даних про осіб, підозрюваних у вчиненні злочину, але виправданих або звільнених від відповідальності, не можна прирівнювати до висловлення підозри, їхнє відчуття того, що з ними не поводяться як із невинуватими, посилюється тим, що їхні дані зберігаються на невизначений строк, так само як і дані засуджених осіб. У той час як дані тих, хто ніколи не підозрювався у вчиненні злочину, підлягають знищенню (*там само*, § 122). Таким чином, факт, що особа отримала вигоду від звільнення після підозри у вчиненні злочину, виправдовує поведінку з нею інакше, ніж із засудженою особою (*там само*, § 122; див. також з цього приводу «*М.К. проти Франції*» (*M.K. v. France*), 2013, § 42; «*Брунет проти Франції*» (*Brunet v. France*), 2014, § 40). У справі «*Брунет*

проти Франції» (Brunet v. France), 2014 (§ 40), де заявник отримав вигоду від рішення про закриття справи після медіації, Суд поставив під сумнів невивірковий характер персональних даних, зафіксованих у файлах органів влади, що не роблять різниці між засудженими особами й особами, чії справи були закриті. У справі *«Айсагуер проти Франції» (Aysaquer v. France)*, 2017 (§§ 42-43), де персональні дані були зібрані й збережені після засудження за не найтяжчі злочини, Суд поставив під сумнів широкий обсяг збору персональних даних органами влади, які не робили різниці відповідно до рівня тяжкості злочину, що призвів до засудження, незважаючи на широкий спектр ситуацій, які можуть виникнути в рамках застосування закону. На думку Суду, дії, що призвели до засудження заявника, а саме удари парасолькою, спрямовані на жандармів у політичному / профспілковому контексті, не можна порівнювати з діями, які класифікуються як особливо тяжкі злочини, такі як сексуальні злочини, тероризм, злочини проти людяності або торгівля людьми.

201. У справі *«М.М. проти Сполученого Королівства» M.M. v. the United Kingdom*, 2012 (§§ 187-207), довічне зберігання запису про застереження в поліцейських протоколах особи після того, як вона зникла на день зі своїм онуком, немовлям, намагаючись запобігти його від'їзду до Австралії після розпаду шлюбу її сина, призвело до визнання порушення статті 8. Суд поставив під сумнів надзвичайно широкий обсяг системи зберігання даних, яка охоплювала не лише обвинувальні вироки, але й рішення, що не стосувалися засудження, такі як попередження, застереження та догани, а також велику кількість додаткових даних, записаних поліцією на підставі загальної настанови про те, що дані повинні зберігатися до досягнення суб'єктом даних 100-річного віку (*там само*, § 202). Суд вважав, що чим більший обсяг системи запису, а отже, чим більший обсяг і чутливість даних, що зберігаються й доступні для розголошення, тим важливішими є гарантії, які повинні застосовуватися на різних вирішальних етапах подальшої обробки даних (*там само*, § 200). Те саме стосується справи *«Гоґран проти Сполученого Королівства» (Gaughran v. the United Kingdom)*, 2020 (§§ 94-97), щодо безстрокового зберігання біометричних даних і фотографій заявника, який був засуджений за керування автомобілем у стані алкогольного сп'яніння, що становило порушення статті 8.

202. Справа *«Н.Ф. та інші проти Росії» (N.F. and Others v. Russia)*, 2023 (§§ 49-55), стосувалася системи зберігання даних, в якій інформація про кримінальне провадження автоматично збиралася і зберігалася після того, як особа піддавалася кримінальному переслідуванню. Ця система охоплювала інформацію про всі судимості, незалежно від характеру й тяжкості вчиненого злочину і незалежно від того, чи були ці судимості погашені, а також інформацію про кримінальні провадження, які були закриті на «підставах непридатності до реабілітації». Суд визнав обсяг і застосування цієї системи надмірними. Ба більше, він наголосив, що постійна обробка даних була особливо втручанням у життя тих осіб, які не були засуджені за вчинення кримінальних злочинів. Що стосується засуджених осіб, то рівень втручання в їхнє приватне життя також буде інтрузивним після того, як їхні судимості будуть погашені або зняті судом. За відсутності достатніх гарантій проти зловживань і можливості перегляду, така обробка даних була визнана непропорційною.

203. Зберігання даних незасуджених осіб може бути особливо шкідливим у випадку неповнолітніх, враховуючи їхнє особливе становище та важливість їхнього розвитку та інтеграції в суспільство. Особливу увагу слід приділяти захисту неповнолітніх від будь-якої шкоди такого типу (*«С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom)* [ВП], 2008, § 124).

ii. Строк зберігання даних

204. Тривалість періоду, протягом якого органи влади вирішують зберігати персональні дані особи, важливий, хоч і не вирішальний аспект, який слід враховувати при оцінці того, чи

збереження персональних даних у файлі або базі даних для поліцейських цілей пропорційне переслідуваній законній меті. Суд встановив порушення положень статті 8 у справах щодо:

- безстрокового зберігання відбитків пальців і даних ДНК осіб, які підозрювалися у вчиненні злочину, але провадження у справі яких закінчилося рішенням про закриття справи або виправданням (*«С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom) [GC], 2008*);
- безстрокового зберігання профілів ДНК, відбитків пальців і фотографій особи, визнаної винною у вчиненні злочину, навіть після того, як її судимість була вилучена з поліцейського досьє у зв'язку із закінченням встановленого законом строку (*«Гогран проти Сполученого Королівства» (Gaughran v. the United Kingdom), 2020*);
- довічного зберігання в поліцейському досьє всіх обвинувальних, виправдувальних вироків, застережень, попереджень та доган, що стосуються однієї особи (*«М.М. проти Сполученого Королівства» (M.M. v. the United Kingdom), 2012*);
- безстрокового зберігання профілів ДНК осіб, засуджених за крадіжку за обтяжуючих обставин (*«Трайковські та Чіповські проти Північної Македонії» (Trajkovski and Chipovski v. Macédoine du Nord), 2020*);
- зберігання протягом максимум сорока років персональних даних особи, засудженої за досить незначне правопорушення (*«Айсагуер проти Франції» (Aysaquer v. France), 2017*);
- зберігання протягом максимум двадцяти років відбитків пальців особи, підозрюваної, але не засудженої за крадіжку книг (*«М.К. проти Франції» (M. K. v. France), 2013*);
- зберігання протягом максимум двадцяти років персональних даних особи, яка подала скаргу на насильство щодо свого партнера, справу було закрито після медіації (*«Брунет проти Франції» (Brunet v. France), 2014*);
- безстрокове зберігання даних про заміну заявникові адміністративного стягнення (*«Тончев проти Болгарії» (Tonchev v. Bulgaria), 2024*).

205. І навпаки, Суд не знайшов порушення статті 8 у кількох справах щодо зберігання персональних даних осіб, засуджених за сексуальне насильство, протягом максимум тридцяти років, після чого ці дані автоматично видалялися, оскільки були запроваджені процедури, які дозволяли видаляти дані, як тільки вони втрачали свою актуальність (*«Б.Б. проти Франції» (B.B. v. France), 2009, § 67*; *«Гардель проти Франції» (Gardel v. France), 2009, § 69*; *«М.Б. проти Франції» (M.B. v. France), 2009, § 59*). Суд також визнав явно необґрунтованою справу про безстрокове зберігання персональних даних осіб, засуджених за тяжкі злочини, що супроводжувалося переглядом через регулярні проміжки часу, що не перевищують десяти років, з метою визначення того, чи зберігання даних все ще необхідне (*«Перуззо і Мартенс проти Німеччини» (Peruzzo and Martens v. Germany) (ухв.), 2013, §§ 44-49*). У справі *«П.Н. проти Німеччини» (P.N. v. Germany), 2020 (§§ 87-90)*, Суд не знайшов порушення статті 8 щодо зберігання протягом п'яти років, за умови дотримання гарантій та індивідуального перегляду, персональних даних рецидивіста з метою його ідентифікації після відкриття проти нього нового кримінального провадження.

206. Що стосується режимів зберігання біометричних даних засуджених осіб, то тривалість періоду зберігання не обов'язково вирішальна при оцінці того, чи перевищила Держава допустиму свободу розсуду при встановленні відповідного режиму. Вирішальне значення має наявність і функціонування певних гарантій (*«Гогран проти Сполученого Королівства» (Gaughran v. the United Kingdom), 2020, § 88*). Коли Держави самі встановлюють межі зберігання біометричних даних засуджених осіб або навіть вирішують, що зберігання даних має бути безстроковим, вони ставлять себе на межу своєї свободи розсуду і повинні забезпечити наявність певних ефективних гарантій (*там само, § 88*). Наявність або відсутність незалежної перевірки обґрунтованості зберігання інформації відповідно до визначених

критеріїв, таких як тяжкість злочину, обґрунтованість підозри проти особи, попередні судимості та будь-які інші особливі обставини, становить основну гарантію забезпечення пропорційності строків зберігання даних (*там само*, § 94; «*С. і Марпер проти Сполученого Королівства*» (*S. and Marper v. the United Kingdom*) [ВП], 2008, § 119; «*Б.Б. проти Франції*» (*B.B. v. France*), 2009, § 68; «*Гардель проти Франції*» (*Gardel v. France*), 2009, § 69; «*М.Б. проти Франції*» (*M.B. v. France*), 2009, § 60).

207. Відсутність максимального строку зберігання персональних даних не обов'язково є несумісною зі статтею 8 («*Перуззо і Мартенс проти Німеччини*» (*Peruzzo and Martens v. Germany*) (ухв.), 2013, § 46; «*Ґоґран проти Сполученого Королівства*» (*Gaughran v. the United Kingdom*), 2020, § 88), але процесуальні гарантії особливо необхідні, коли зберігання даних повністю залежить від того, наскільки ретельно органи влади забезпечують пропорційність періоду зберігання («*Перуззо і Мартенс проти Німеччини*» (*Peruzzo and Martens v. Germany*) (ухв.), 2013, § 46; «*Айкаґуер проти Франції*» (*Auqaguer v. France*), 2017, § 38).

208. У справі «*Перуззо і Мартенс проти Німеччини*» (*Peruzzo and Martens v. Germany*) (ухв.), 2013 (§ 44) щодо безстрокового зберігання біометричних даних осіб, засуджених за тяжкі злочини, які можуть призвести до рецидиву, Суд, із задоволенням, відзначив, що національне законодавство вимагає від Федерального кримінального відомства перевіряти через регулярні проміжки часу, що не перевищують 10 років, чи зберігання даних все ще необхідне, або чи можна ці дані видалити, беручи до уваги мету їх зберігання, а також природу і серйозність обставин кожної справи, в якій персональні дані було зафіксовано (*там само*, § 46). Суд постановив, що тривалість інтервалів не була необґрунтованою, враховуючи, що профілі ДНК можуть бути отримані тільки від осіб, засуджених за злочини певного ступеня тяжкості (*там само*, §§ 48-49).

209. У справі «*Ґоґран проти Сполученого Королівства*» (*Gaughran v. the United Kingdom*), 2020 (§ 96), безстроковий характер зберігання відбитків пальців, профілів ДНК і фотографії особи, визнаної винною у керуванні в стані алкогольного сп'яніння, призвів до встановлення порушення статті 8. Органи влади не врахували серйозність правопорушення або постійну необхідність зберігання цих даних протягом невизначеного строку, а також не надали реальних можливостей для перегляду їх зберігання (*там само*, § 96).

210. Максимальний строк зберігання персональних даних, встановлений національним законодавством, на практиці може більше нагадувати норму, ніж реальний максимум, якщо шанси на задоволення вимоги про видалення даних до закінчення встановленого законом строку лише гіпотетичні («*М.К. проти Франції*» (*M. K. v. France*), 2013, §§ 44-47; «*Брунет проти Франції*» (*Brunet v. France*), 2014, §§ 41-45; «*Айкаґуер проти Франції*» (*Auqaguer v. France*), 2017, §§ 44-46). Суд встановив порушення статті 8 у кількох справах, де національна система передбачала максимальний строк зберігання даних — двадцять або двадцять п'ять років для правопорушень, провадження у яких було припинено («*М.К. проти Франції*» (*M. K. v. France*), 2013, §§ 44-47; «*Брунет проти Франції*» (*Brunet v. France*), 2014, §§ 41-45), або навіть сорокарічний строк для правопорушення, яке не було особливо тяжким, але призвело до обвинувального вироку («*Айкаґуер проти Франції*» (*Auqaguer v. France*), 2017, § 42).

211. У справі «*Кетт проти Сполученого Королівства*» (*Catt v. the United Kingdom*), 2019 (§ 120), зберігання персональних даних заявника в базі даних національної поліції з питань екстремізму протягом щонайменше шести років, після чого дані підлягали плановому перегляду, призвело до встановлення порушення статті 8. Заявник повністю залежав від ретельності органів влади у виконанні надто гнучких гарантій, викладених у відповідному кодексі практики, для забезпечення пропорційності строку зберігання даних. Відсутність гарантій, що полегшують видалення даних, як тільки період їх зберігання стає непропорційним, викликає особливе занепокоєння, коли дані, що розкривають політичні погляди (які

потребують підвищеного рівня захисту), зберігаються на невизначений строк (*там само*, §§ 122-123).

212. Справа «*М.М. проти Сполученого Королівства*» (*M.M. v. the United Kingdom*), 2012 стосувалася наслідків зміни політики щодо строку зберігання даних про судимість з огляду на перспективи працевлаштування суб'єкта даних (§ 204). Суд вважає, що невибірковий і безстроковий збір даних про судимість навряд чи відповідатиме вимогам статті 8 за відсутності чітких і детальних законодавчих положень, що роз'яснюють застосовні гарантії та встановлюють правила щодо тривалості зберігання таких даних (*там само*, § 199).

213. Див. також, в іншому контексті, десятирічний строк конфіденційності доказів, отриманих під час провадження і таких, що містять медичні дані (наприклад, для встановлення особи та ВІЛ-позитивного статусу), у справі «*Z проти Фінляндії*» (*Z v. Finland*), 1997 (§§ 111-113). У цій справі десятирічний період конфіденційності суперечив бажанням та інтересам сторін провадження, а оприлюднення без згоди заявниці інформації стало серйозним втручанням у її право на повагу до приватного та сімейного життя. Подальше втручання, якого б вона зазнала, якби медична інформація стала доступною для громадськості через десять років, не було підкріплене жодними переконливими причинами.

iii. Гарантії щодо знищення або видалення збережених даних⁹

214. На думку Суду, видалення даних з бази, в якій вони зберігалися для поліцейських цілей, не було особливо обтяжливим («*Кетт проти Сполученого Королівства*» (*Catt v. the United Kingdom*), 2019, § 127). Якби уряд створив базу даних, що не підлягає перегляду або редагуванню, і потім використовував це як виправдання для відмови у видаленні інформації, то така ситуація суперечила б вимозі захисту приватного життя, передбаченій статтею 8, (*там само*, § 127).

215. Наявність на національному рівні судової процедури видалення даних, яка передбачає незалежну перевірку обґрунтованості їх зберігання відповідно до визначених критеріїв, становить важливий фактор у забезпеченні права на повагу до приватного життя («*С. і Марпер проти Сполученого Королівства*» (*S. and Marper v. the United Kingdom*) [ВП], 2008, § 119; «*Гардель проти Франції*» (*Gardel v. France*), 2009, § 69).

216. Суд не встановив порушення статті 8 у випадках, коли, навіть якщо дані зберігалися протягом «тривалих» періодів до тридцяти років («*Б.Б. проти Франції*» (*B.B. v. France*), 2009, §§ 66, 68; «*Гардель проти Франції*» (*Gardel v. France*), 2009, §§ 67, 69; «*М.Б. проти Франції*» (*M.B. v. France*), 2009, §§ 58, 60), або навіть безстроково («*Перуззо і Мартенс проти Німеччини*» (*Peruzzo and Martens v. Germany*) (ухв.), 2013, § 46), суб'єкт даних скористався собі на користь судовою процедурою, яка гарантувала незалежну перевірку обґрунтування зберігання даних за визначеними критеріями, що дозволило йому домогтися видалення даних до закінчення максимального строку, встановленого законом, або, у випадку безстрокового зберігання даних, як тільки таке зберігання втратило актуальність, (див., для порівняння «*С. і Марпер проти Сполученого Королівства*» (*S. and Marper v. the United Kingdom*) [ВП], 2008, § 119).

217. У справах «*Б.Б. проти Франції*» (*B.B. v. France*), 2009 (§ 68), «*Гардель проти Франції*» (*Gardel v. France*), 2009 (§ 69), і «*М.Б. проти Франції*» (*M.B. v. France*), 2009 (§ 60), Суд постановив, що судова процедура видалення даних, яку суб'єкт даних може ініціювати шляхом простого звернення до прокурора, рішення якого можуть бути оскаржені в судовому порядку, забезпечує незалежну перевірку обґрунтованості збереження інформації відповідно до визначених критеріїв та надає адекватні та ефективні гарантії. Див. також п. 204 вище про

⁹ Див. також розділ вище про Право на видалення даних.

справу *«Перуззо і Мартенс проти Німеччини» (Peruzzo and Martens v. Germany)* (ухв.), 2013 (§ 44).

218. У справі *«П.Н. проти Німеччини» (P.N. v. Germany)*, 2020 (§§ 81, 88) яка стосувалася зберігання персональних даних повнолітнього правопорушника, злочини якого не були ні незначними, ні особливо тяжкими, правило про видалення таких даних після п'ятирічного періоду за відсутності нових кримінальних розслідувань щодо суб'єкта даних не було визнано таким, що суперечить статті 8. Поліція мала можливість переглядати необхідність подальшого зберігання даних, за умови судового контролю, що дозволяло заявнику домогтися видалення своїх даних, якщо його поведінка свідчила про те, що ці дані більше не потрібні для поліцейських цілей (*там само*, § 88).

219. Відсутність ефективних гарантій, що дозволяють видаляти персональні дані, які більше не є актуальними для початкових цілей, викликає особливе занепокоєння у випадку чутливих категорій персональних даних, які потребують підвищеного рівня захисту (*«Кетт проти Сполученого Королівства» (Catt v. the United Kingdom)*, 2019, § 123).

220. Можливість видалення даних, передбачена національним законодавством, є «теоретичною та ілюзорною», а не «практичною й ефективною» гарантією, коли право подати запит на таке видалення може конфліктувати з інтересами слідчих служб, які прагнуть мати якомога більше даних, і коли конкуруючі інтереси хоча б частково суперечливі (*«М.К. проти Франції» (M.K. v. France)*, 2013, § 44). Гарантія видалення даних також має обмежений вплив, коли органи влади відмовляються видалити дані на вимогу суб'єкта даних або не надають пояснень щодо їх подальшого зберігання (*«Кетт проти Сполученого Королівства» (Catt v. the United Kingdom)*, 2019, § 122). Те саме стосується випадків, коли запити на видалення дозволяються лише за виняткових обставин або відхиляються, якщо суб'єкт даних визнав, що вчинив правопорушення, а дані є точними (*«М.М. проти Сполученого Королівства» (M.M. v. the United Kingdom)*, 2012, § 202).

221. Суд вважає, що особам, засудженим за вчинення злочину, як і тим, хто був виправданий або звільнений, повинні бути надані реальні можливості для подання запиту на видалення зареєстрованих даних (*«Б.Б. проти Франції» (B.B. v. France)*, 2009, § 68; *«Брунет проти Франції» (Brunet v. France)*, 2014, §§ 41-43; *«Айсагуер проти Франції» (Aysaguer v. France)*, 2017, § 44). У справі *«Айсагуер проти Франції» (Aysaguer v. France)*, 2017 (§ 44), де процедура видалення даних була доступна лише для підозрюваних, але не для засуджених, Суд визнав порушення статті 8. Він зазначив, що через тривалість зберігання ДНК-профілів та відсутність можливості їх видалення правила зберігання ДНК-профілів у національній базі даних не забезпечують справедливого балансу між публічними та приватними інтересами (*там само*, § 45).

222. У справі *«Хелілі проти Швейцарії» (Khelili v. Switzerland)*, 2011 (§§ 68-70) Суд визнав порушення статті 8, підкреслюючи невизначеність і труднощі, з якими зіткнулася заявниця у спробах видалити запис «повія» в розділі «рід занять» поліцейського дос'є, оскільки вона ніколи не була засуджена за незаконну проституцію. Суд зауважив, що не було жодних доказів того, що видалення цього запису було неможливим або складним з технічних причин (*там само*, § 68).

iv. Гарантії, спрямовані на регулювання доступу третіх осіб і захист цілісності та конфіденційності даних

223. Суд неодноразово розглядав питання про те, чи містить застосовне національне законодавство гарантії, здатні ефективно захистити персональні дані, що зберігаються в офіційних базах даних, від неправомірного використання і зловживань (*«С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom)* [ВП], 2008, § 103; *«Б.Б. проти Франції» (B.B. v. France)*, 2009, § 61; *«Гардель проти Франції» (Gardel v. France)*, 2009, § 62;

«*М.М. проти Сполученого Королівства*» (*M.M. v. the United Kingdom*), 2012, § 195; «*М.К. проти Франції*» (*M.K. v. France*), 2013, § 35; «*Брунет проти Франції*» (*Brunet v. France*), 2014, § 35; «*Айсагуер проти Франції*» (*Auçaguer v. France*), 2017, § 38). Суд зазначив, що такі гарантії існують, наприклад, коли:

- доступ до зареєстрованих даних мають лише органи, зобов'язані зберігати конфіденційність («*Б.Б. проти Франції*» (*B.B. v. France*), 2009, § 69; «*Перуззо і Мартенс проти Німеччини*» (*Peruzzo and Martens v. Germany*) (ухв.), 2013, § 47);
- зареєстровані дані підлягали достатньо чітко визначеним процедурам щодо ознайомлення з ними, що стосуються осіб, уповноважених ознайомлюватися з базою даних («*М.К. проти Франції*» (*M.K. v. France*), 2013, § 37; див. для порівняння «*Хелілі проти Швейцарії*» *Khelili v. Switzerland*, 2011, § 64);
- особа людини, у якої було взято зразок ДНК, не була розкрита експертам, відповідальним за ДНК-профілювання; останні також були зобов'язані вжити належних заходів для запобігання будь-якому несанкціонованому використанню досліджуваного клітинного матеріалу («*Перуззо і Мартенс проти Німеччини*» (*Peruzzo and Martens v. Germany*) (ухв.), 2013, § 45); сам клітинний матеріал повинен бути негайно знищений, як тільки він більше не був потрібен для встановлення ДНК-профілю, а в базі даних Федерального відомства кримінальної поліції могли зберігатися лише ДНК-профілі, витягнуті з такого клітинного матеріалу (*там само*, § 45); ба більше, збережені профілі ДНК можуть бути розкриті відповідним органам влади лише для цілей кримінального провадження, превентивного відвернення небезпеки та для надання міжнародної правової допомоги у зв'язку з цим (*там само*, § 47).

224. У справі «*Гардель проти Франції*» (*Gardel v. France*), 2009 (§ 70), де правила використання реєстру та коло органів державної влади, які мають доступ до нього, неодноразово розширювалися і вже не обмежувалися лише судовою владою та поліцією, а й включали адміністративні органи, Суд із задоволенням відзначив, що доступ до реєстру можуть мати лише органи, які зобов'язані зберігати конфіденційність, і за чітко визначених обставин.

225. У справі «*П.Н. проти Німеччини*» (*P.N. v. Germany*), 2020 (§ 89), ніщо не вказувало на те, що ідентифікаційні дані, отримані від повнолітнього правопорушника і які зберігаються поліцією протягом максимум п'яти років, були недостатньо захищені від таких зловживань, як несанкціонований доступ або розповсюдження.

226. Навпаки у справі «*М.М. проти Сполученого Королівства*» (*M.M. v. the United Kingdom*), 2012 (§ 204), що стосувалася довічного зберігання даних про застереження в поліцейському досьє та розголошення цих даних потенційному роботодавцю у контексті пошуку роботи, Суд висловив занепокоєння щодо процедури, що регулює доступ третіх осіб до кримінальних справ шукачів роботи, яка не дозволяє на жодному етапі оцінити релевантність даних, що містяться в центральних реєстрах, для роботи, яку шукають, або потенційний ризик, який може становити суб'єкт даних. Аналогічно у справі «*Н.Ф. та інші проти Росії*» (*N.F. and Others v. Russia*), 2023 (§ 51), що стосувалася бази даних про кримінальні провадження, які або були припинені на «з nereабілітуючих підстав», або завершилися винесенням обвинувальних вироків, Суд відзначив, що наявні нормативні акти не розрізняють мету й інші важливі функції обробки таких даних, що не дозволяє провести адекватний аналіз пропорційності доступу третіх осіб, як цього вимагає стаття 8 Конвенції.

б. Зберігання персональних даних у медичному контексті

227. Суд неодноразово розглядав питання зберігання конфіденційних даних, пов'язаних зі здоров'ям. У справі «*Маланічева проти Росії*» (*Malanicheva v. Russia*) (ухв.), 2016 (§§ 13, 15-18), Суд постановив, що ефективне функціонування закладів охорони здоров'я та процес прийняття

судових рішень вимагають зберігання та обміну відповідними даними. Він відхилив як явно необґрунтовані скарги щодо реєстрації імені заявниці в лікарняному реєстрі осіб із психічними розладами та нібито помилкових посилань на різні аспекти її психічного здоров'я у внутрішньому спілкуванні між медичними закладами та їхніх зауваженнях у судах. Ніщо не вказувало на те, що зареєстрована інформація була доступною для громадськості або використовувалася з іншою метою, окрім як для прийняття рішення про найбільш підходящу медичну допомогу для суб'єкта даних.

228. У справі *«Дрелон проти Франції» (Drelon v. France)*, 2022, (§ 98), де йшлося про зберігання до 2278 року персональних даних заявника про його передбачувану гомосексуальність, зібраних у 2004 році, Суд визнав такий період надмірним.

229. Раніше Комісія визнала явно необґрунтованою заяву та відхилила її щодо запису в психіатричній лікарні даних про примусове утримання пацієнта, яке було визнане незаконним національними судами (*«Івон Шаве, в дівоцтві Жульєн, проти Франції» (Yvonne Chave née Jullien v. France)*, 1991). Комісія зазначила, що запис інформації про психічно хворих слугує не лише законним інтересам забезпечення ефективної роботи державних лікарень, але й захисту прав самих пацієнтів. Це допомагає запобігти ризику свавільного ув'язнення і слугує засобом розслідування для адміністративних або судових органів, які відповідають за нагляд за психіатричними установами. У цій справі персональні дані заявника, внесені до реєстру психіатричної лікарні, були захищені належними правилами конфіденційності.

230. Див. також п. 182 вище про порушення статті 8 у справі *«Суріков проти України» (Surikov v. Ukraine)*, 2017 (§ 75-95).

с. Зберігання персональних даних в інтернеті для журналістських цілей

231. Суд наголосив, що преса відіграє хоч і другорядну, але важливу роль у збереженні архівів раніше переданих новин і наданні доступу до них громадськості. У цьому аспекті інтернет-архіви роблять значний внесок у збереження та поширення новин та інформації, оскільки вони становлять важливе джерело для освіти та історичних досліджень, зокрема через свою легкодоступність та, як правило, безкоштовність (*«Таймз Ньюспейперс Лтд проти Сполученого Королівства» (№№ 1 і 2) (Times Newspapers Ltd v. the United Kingdom) (nos. 1 and 2)*, 2009, §§ 27 і 45; *«Венгжиновський і Смольчевський проти Польщі» (Węgrzynowski and Smolczewski v. Poland)*, 2013, § 59; *«М.Л. та В.В. проти Німеччини» (M.L. and W.W. v. Germany)*, 2018, § 90; див. також справу, розглянуту за статтею 10, *«Гурбейн проти Бельгії» (Hurbain v. Belgium)* [ВП], 2023, § 180).

3. Розголошення персональних даних

232. У кількох справах Суд оцінював заходи, що тягнуть за собою розголошення персональних даних особи обробником даних:

- іншій фізичній або юридичній особі (*«Моккуте проти Литви» (Mockutė v. Lithuania)*, 2018, §§ 99-100, щодо передачі лікарнею інформації про стан здоров'я пацієнтки члену її сім'ї та журналістам; *«Й. проти Туреччини» (Y. v. Turkey)* (ухв.), 2015, §§ 70-72, щодо розголошення бригадою швидкої допомоги персоналу лікарні інформації про ВІЛ-позитивний статус пацієнта; *«Раду проти Республіки Молдова» (Radu v. Republic of Moldova)*, 2014, § 27, щодо розголошення лікарнею медичної інформації про пацієнтку її роботодавцю; *«М.К. проти Сполученого Королівства» (M.C. v. the United Kingdom)*, 2021, § 46, щодо розголошення органами влади інформації про судимість заявниці її потенційному роботодавцю);
- органу державної влади (*«М.С. проти Швеції» (M.S. v. Sweden)*, 1997, § 35, щодо розголошення гінекологічним відділенням медичної інформації про пацієнта фонду

соціального страхування; *«П.Т. проти Республіки Молдова» (P.T. v. Republic of Moldova)*, 2020, §§ 5-6, 29-31, щодо непотрібного включення конфіденційних медичних даних до довідки, яка мала бути видана в різних контекстах);

- громадськості (*«Гайовський проти Словаччини» (Hájovský v. Slovakia)*, 2021, §§ 46-49, щодо публікації в телевізійному випуску новин інформації, яка ідентифікує особу та містить її нерозмитую фотографію, зроблену таємно і під хибним приводом; *«Пек проти Сполученого Королівства» (Peck v. the United Kingdom)*, 2003, § 63, щодо передачі ЗМІ відеозапису, зробленого за допомогою замкненої телевізійної системи, на якому зображена особа, яка намагається вчинити самогубство в публічному місці; *«Бремнер проти Туреччини» (Bremner v. Turkey)*, 2015, §§ 71-85, щодо телевізійної трансляції нерозмитого, непікселізованого зображення особи, знятого прихованою камерою; *«Хадіджа Ісмаїлова проти Азербайджану» (Khadija Ismayilova v. Azerbaijan)*, 2019, §§ 108-132, щодо прихованого відеозапису журналістки в її приватному будинку та публічної трансляції відео; *«Z проти Фінляндії» (Z v. Finland)*, 1997, §§ 70-71, щодо розголошення в судовому рішенні, переданому пресі, особи і стану здоров'я особи; *«Апосту проти Румунії» (Apostu v. Romania)*, 2015, §§ 121-132, щодо розголошення пресі доказів з матеріалів слідства; *«Монтера проти Італії» (Montera v. Italy)* (ухв.), 2002, щодо оприлюднення звіту парламентської комісії про приватне життя та професійну етику судді; *«Фон Ганновер проти Німеччини» (Von Hannover v. Germany)*, 2004, §§ 61-81, щодо публікації в бульварній пресі фотографій, які стосуються приватного життя принцеси; *«Поланко Торрес і Мовілла Поланко проти Іспанії» (Polanco Torres and Movilla Polanco v. Spain)*, 2010, §§ 44-54, щодо статті в пресі, заснованої на заявах колишнього бухгалтера, який звинувачував дружину старшого судді в участі в незаконних операціях із зазначеною компанією; *«Алкая проти Туреччини» (Alkaya v. Turkey)*, 2012, §§ 30-31, щодо розголошення популярною щоденною газетою повної поштової адреси відомої акторки; *«Мітянін і Леонов проти Росії» (Mityanin and Leonov v. Russia)*, 2018, §§ 111-121, щодо поширення в пресі фотографії підозрюваного, яка супроводжувалася заявами, що звинувачують його в різних незначних і серйозних кримінальних злочинах; *«Богомолова проти Росії» (Bogomolova v. Russia)*, 2017, §§ 54-58, щодо публікації фотографії дитини на титульній сторінці брошури під назвою «Дітям потрібна сім'я», виданої Центром психолого-медико-соціальної підтримки; *«Л.Б. проти Угорщини» (L.B. v. Hungary)* [ВП], 2023, щодо обов'язкової публікації податковим органом персональних даних заявника, включаючи його ім'я та домашню адресу, на своєму вебсайті у списку великих податкових боржників).

а. Вплив попередньої згоди

233. Попередня згода суб'єктів даних на передачу, розголошення або публікацію їхніх даних — важливий, хоч і не вирішальний елемент при визначенні в конкретній справі того, чи становлять такі операції втручання в їхнє право на повагу до приватного життя (*«М.С. проти Швеції» (M.S. v. Sweden)*, 1997, §§ 31, 35; *«М.М. проти Сполученого Королівства» (M.M. v. the United Kingdom)*, 2012, §§ 186, 189) або чи можуть вони вважатися такими, що здійснюються «відповідно до закону» у значенні пункту 2 статті 8 (*«Раду проти Республіки Молдова» (Radu v. the Republic of Moldova)*, 2014, § 27; *«Моккуте проти Литви» (Mockutė v. Lithuania)*, 2018, § 101). Суд встановив порушення статті 8 у кількох справах, в яких розголошення персональних даних обробником даних відбулося без згоди суб'єкта даних (*«Раду проти Республіки Молдова» (Radu v. the Republic of Moldova)*, 2014, §§ 30, 32; *«Моккуте проти Литви» (Mockutė v. Lithuania)*, 2018, §§ 103, 106; *«Пек проти Сполученого Королівства» (Peck v. the United Kingdom)*, 2003, §§ 85-87; *«Соро проти Естонії» (Sõro v. Estonia)*, 2015, §§ 17-19, 64).

234. Щоб вважатися дійсною, згода суб'єкта даних повинна бути поінформованою та однозначною («*М.С. проти Швеції*» (*M.S. v. Sweden*), 1997, § 32; «*Коновалова проти Росії*» (*Kononova v. Russia*), 2014, §§ 47-48). У справі про передачу медичної картки особи одним державним органом (гінекологічним відділенням лікарні) іншому (Департаменту соціального забезпечення) без згоди суб'єкта даних, питання полягало в тому, чи відмовився суб'єкт даних, подавши позов про відшкодування збитків, від свого права на конфіденційність даних («*М.С. проти Швеції*» (*M.S. v. Sweden*), 1997, §§ 31-32). Суд постановив, що оскільки розголошення даних залежало не тільки від того, що заявниця подала вимогу про компенсацію, але й від низки факторів, які вона не могла контролювати, з її вимоги про компенсацію не можна було зробити висновок, що вона однозначно відмовилася від свого права на повагу до приватного життя щодо медичної документації. Відповідно застосовувалася стаття 8.

235. Той факт, що персональні дані особи розголошуються на її прохання або за її згодою, не позбавляє її захисту, передбаченого статтею 8, якщо вона не має реального вибору, наприклад, якщо роботодавець наполягає на розголошенні персональних даних, що зберігаються в судимості претендента на роботу («*М.М. проти Сполученого Королівства*» (*M.M. v. the United Kingdom*), 2012, § 189). У пізнішій справі «*М.М. проти Сполученого Королівства*» (*M.M. v. the United Kingdom*), 2012 (§§ 187-207), де заявниця вимагала розголошення потенційному роботодавцю інформації про застереження, зареєстроване в її судимості, Суд встановив порушення статті 8 у зв'язку з відсутністю достатніх гарантій у системі зберігання та розголошення даних про судимість, яка не передбачала оцінку на будь-якому етапі допустимої релевантності даних для роботи, яку шукає особа, або ступеня, до якого суб'єкт даних може сприйматися як потенційно ризиковий (*там само*, § 204). У справі «*М.К. проти Сполученого Королівства*» (*M.C. v. the United Kingdom*), 2021, §§ 47-57, Суд відзначив законодавчі зміни, внесені після рішення у справі «*М.М. проти Сполученого Королівства*» (*M.M. v. the United Kingdom*) і встановив, що новий режим розголошення інформації про судимість сумісний з відповідними вимогами статті 8: він по-різному розрізняє різні типи правопорушень; забезпечує визначеність щодо того, які попередні судимості будуть розголошені в будь-який момент часу; і встановлює чітко визначений, кінцевий термін для розголошення інформації, який може змінюватися в залежності від віку порушника й передбачуваної серйозності правопорушення.

236. Отримання згоди суб'єкта даних не завжди можливе, наприклад, коли записи з камер відеоспостереження, встановлених на вулицях органами влади з метою ідентифікації правопорушників та запобігання злочинам, містять зображення багатьох осіб («*Пек проти Сполученого Королівства*» (*Peck v. the United Kingdom*), 2003, § 81). На думку Суду, система камер відеоспостереження, розголошення зображень з якої ґрунтується на згоді, може на практиці підірвати будь-які дії, спрямовані на підвищення ефективності системи відеоспостереження у виявленні та запобіганні кримінальним правопорушенням, роль якої стає ще більш ефективною завдяки рекламі системи відеоспостереження та її переваг (*там само*, § 81). За таких обставин, або якщо особи, включені до відеозапису, відмовляються давати згоду на поширення їхніх зображень, обробник даних повинен розглянути інші рішення, такі як маскування зображень перед поширенням (*там само*, § 82) або забезпечення того, щоб одержувачі зображень маскували їх самі, у відповідний та адекватний спосіб (*там само*, § 83).

237. У справі «*Пек проти Сполученого Королівства*» (*Peck v. the United Kingdom*), 2003 (§ 87), передача районною радою в пресрелізі для ЗМІ зображень з камер відеоспостереження, що знімали людину, яка намагалася вчинити самогубство в громадському місці, становила порушення статті 8. Суд постановив, що оскільки відеозапис, про який йдеться, чітко зосереджувався на одній особі й стосувався лише однієї особи, оператор системи відеоспостереження, який сповістив поліцію і спостерігав за її втручанням, міг зробити запит до поліції, щоб встановити особу заявника і, таким чином, отримати його згоду на розголошення (*там само*, § 81).

238. У справі *«Бремнер проти Туреччини» (Bremner v. Turkey)*, 2015 (§§ 71-85), трансляція в телевізійному документальному фільмі, знятому прихованою камерою, нерозмитого, непікселізованого зображення особи була визнана такою, що суперечить статті 8. Що стосується, зокрема, того факту, що заявник не був добре відомий, ніщо не вказувало на те, що згадана передача мала якусь інформативну цінність або була використана належним чином і адекватно.

239. Ба більше, беручи до уваги стримувальний ефект, до якого може призвести вимога попереднього повідомлення, значні сумніви щодо ефективності будь-якої вимоги попереднього повідомлення та широку свободу розсуду, якою користуються національні органи влади у цій сфері, Суд у справі *«Мозлі проти Сполученого Королівства» (Mosley v. the United Kingdom)*, 2011 (§ 132), постановив, що стаття 8 не вимагає юридично обов'язкової вимоги щодо повідомлення особи перед публікацією інформації про її приватне життя.

240. У деяких ситуаціях розголошення даних про психічне здоров'я особи без її згоди близькому родичу може становити порушення права на повагу до приватного життя. У справі *«Моккуте проти Литви» (Mockutė v. Lithuania)*, 2018 (§ 100), Суд постановив, що розголошення матері пацієнтки інформації про стан здоров'я її повнолітньої дочки без згоди останньої, зважаючи на напружені стосунки між двома повнолітніми особами, було несумісним з правом, закріпленим у статті 8.

241. Що стосується осіб, які перебувають під арештом або кримінальним переслідуванням, Суд встановив порушення статті 8 у випадках, коли поліцейські служби передали фотографії заявників пресі без їхньої згоди (*«Сціяцца проти Італії» (Sciacca v. Italy)*, 2005, §§ 29-31; *«Хужин та інші проти Росії» (Khuzhin and Others v. Russia)*, 2008, §§ 115-118; *«Маргарі проти Греції» (Margari v. Greece)*, 2023, §§ 54-60), коли вони запросили телевізійну групу знімати заявника в поліцейській дільниці без його згоди з метою трансляції зображень по телебаченню (*«Тома проти Румунії» (Toma v. Romania)*, 2009, §§ 90-93; *«Хмель проти Росії» (Khmel v. Russia)*, 2013, § 41), де Міністерство внутрішніх справ опублікувало на своєму вебсайті фотографії заявників, зроблені під час їхнього перебування під вартою в поліції, на яких не була прихована їхня особистість (*«Д.Г. та інші проти Північної Македонії» (D.H. and Others v. North Macedonia)*, 2023, §§ 63-65), коли розміщення фотографії заявника на дошці оголошень про розшук не було передбачено законом (*«Гуїоргуї Ніколаїшвілі проти Грузії» (Guiorgui Nikolaïchvili v. Georgia)*, 2009, §§ 129-131), або коли існуючі правила і процедури не відповідали вимогам «якості закону» (*«Негру проти Республіки Молдова» (Negru v. the Republic of Moldova)*, 2023, §§ 29-35).

242. Неотримання попередньої згоди суб'єкта даних на передачу, розголошення або публікацію його даних не обов'язково становить порушення статті 8, якщо існують інші законні інтереси, такі як необхідність розслідування кримінальних злочинів і забезпечення публічності судового розгляду (*«Авілкіна та інші проти Росії» (Avilkina and Others v. Russia)*, 2013, § 45; *«Z проти Фінляндії» (Z v. Finland)*, 1997, § 97), необхідність захисту здоров'я людини (*«Й. проти Туреччини» (Y. v. Turkey)* (ухв.), 2015, § 74), національної безпеки (*«Анчев проти Болгарії» (Anchev v. Bulgaria)* (ухв.), 2017, § 100) або економічного добробуту країни (*«М.С. проти Швеції» (M.S. v. Sweden)*, 1997, § 38).

б. Розголошення даних в контексті судового провадження

243. У кількох справах Суд розглядав заходи, вжиті органами влади в контексті судового провадження, які призвели до розголошення персональних даних сторін або третіх осіб, наприклад:

- відтворення судом у рішенні про розлучення витягу з особистої медичної картки (*«Л.Л. проти Франції» (L.L. v. France)*, 2006, § 46), а також постанова, що обмежує

десятьма роками період конфіденційності наданих доказів, що містять медичні дані («*Z проти Фінляндії*» (*Z v. Finland*), 1997, §§ 112-113);

- розголошення конфіденційних психіатричних даних про заявника під час публічного слухання («*Пантелеєнко проти України*» (*Panteleyenko v. Ukraine*), 2006, § 57), і перевірка медичної довідки, наданої на підтримку клопотання про відкладення («*Стоклоса проти Польщі*» (*Stokłosa v. Poland*) (ухв.) 2021, §§ 43-44);
- розголошення особи та ВІЛ-позитивного статусу людини в судовому рішенні, переданому пресі («*Z проти Фінляндії*» (*Z v. Finland*), 1997, § 113);
- розголошення повної інформації про особу третьої сторони в судовому рішенні без попереднього повідомлення останньої («*Вісент Дель Кампо проти Іспанії*» (*Vicent Del Campo v. Spain*), 2018, §§ 47-51);
- використання в судовому рішенні формулювань та аргументів, що розголошують персональні дані жертви, передають стереотипи щодо ролі жінок і можуть перешкоджати ефективному захисту жертв сексуального насильства, незважаючи на задовільну законодавчу базу («*Дж.Л. проти Італії*» (*J.L. v. Italy*), 2021, §§ 136-142);
- публікація фотографій та персональних даних обвинувачених у кримінальному провадженні в пресі («*Маргарі проти Греції*» (*Margari v. Greece*), 2023, § 54) або в публічному списку розшукуваних осіб у відкритій частині поліцейської дільниці («*Негру проти Республіки Молдова*» (*Negru v. the Republic of Moldova*), 2023, § 24);
- розголошення повного імені та адреси заявниці разом з повними текстами судових рішень про відмову в задоволенні її цивільного позову про відшкодування шкоди за сексуальне насильство в загальнодоступній онлайн-базі даних офіційної судової системи («*А.П. проти Вірменії*» (*A.P. v. Armenia*), 2024, § 159).

244. На думку Суду, необхідність захисту конфіденційності певних видів персональних даних іноді може переважати інтерес у розслідуванні та переслідуванні злочину, а також у публічності судового розгляду («*Авілкіна та інші проти Росії*» (*Avilkina and Others v. Russia*), 2013, § 45; «*Z проти Фінляндії*» (*Z v. Finland*), 1997, § 97). Компетентні національні органи повинні мати певну свободу дій у встановленні справедливого балансу між, з одного боку, захистом публічності судового провадження, що є необхідним для підтримки довіри до судів, та, з іншого боку, інтересами сторони або третьої особи в збереженні конфіденційності її даних («*К.К. проти Іспанії*» (*C.C. v. Spain*), 2009, § 35). Будь-який захід, що може призвести до оприлюднення персональних даних особи, незалежно від того, чи є вона стороною або третьою стороною судового провадження, повинен відповідати переважній суспільній потребі («*Вісент Дель Кампо проти Іспанії*» (*Vicent Del Campo v. Spain*), 2018, § 46) і повинен бути обмежений, наскільки це можливо, тим, що є суворо необхідним у зв'язку з особливостями провадження («*Л.Л. проти Франції*» (*L.L. v. France*), 2006, § 45; «*Маргарі проти Греції*» (*Margari v. Greece*), 2023, § 47).

245. Щоб у кожному конкретному випадку визначити, чи є достатні підстави для розголошення в тексті судового рішення особи та інших персональних даних про неї, важливим є питання про те, чи були б можливі інші, менш інтрузивні заходи відповідно до національного законодавства та практики. Це стосується можливості суду не згадувати в рішенні будь-які імена, що дозволяють ідентифікувати суб'єкта даних («*Z проти Фінляндії*» (*Z v. Finland*), 1997, § 113; «*Вісент Дель Кампо проти Іспанії*» (*Vicent Del Campo v. Spain*), 2018, § 50), збереження повної аргументації в таємниці протягом певного періоду й замість цього опублікування скороченої версії аргументації, резолютивної частини та зазначення закону, який було застосовано («*Z проти Фінляндії*» (*Z v. Finland*), 1997, § 113), або обмеження доступу до тексту рішення або до певних питань у ньому («*Вісент Дель Кампо проти Іспанії*» (*Vicent Del Campo v. Spain*), 2018, § 50). Суд вважає, що такі заходи, як правило, здатні зменшити вплив судового рішення на право суб'єкта даних на захист його приватного життя.

246. У справі *«Пантелеєнко проти України» (Panteleyenko v. Ukraine)*, 2006 (§ 82), Суд постановив, що закрите слухання також могло б допомогти запобігти публічному розголошенню під час відкритого слухання конфіденційної інформації про психічне здоров'я особи, отриманої з психіатричної лікарні, та про психіатричне лікування в ній, хоча це не обов'язково запобігло б доведенню цієї інформації до відома сторін та її включенню до матеріалів справи.

247. У справі *«Францу проти Румунії» (Frâncu v. Romania)*, 2020 (§§ 72-73), неспроможність апеляційного суду забезпечити конфіденційність медичної інформації про заявника шляхом відхилення клопотання про проведення закритого слухання у справі про корупцію проти мера була визнана такою, що суперечить статті 8. На думку Суду, просто оголосивши, без подальших пояснень, що справа заявника не відповідає «жодній із ситуацій», передбачених Кримінальним процесуальним кодексом щодо розгляду справи у закритому судовому засіданні, цей суд не дотримався справедливого балансу між загальним інтересом у забезпеченні прозорості судового провадження та інтересом учасника судового процесу у збереженні конфіденційності даних про стан його здоров'я. Навіть якщо припустити, що високий суспільний резонанс обвинуваченого може бути одним із факторів, які слід брати до уваги при аналізі пропорційності клопотання про проведення закритого судового засідання, у цій справі апеляційний суд не провів індивідуальної оцінки пропорційності такого заходу.

248. У справі *«Хадіджа Ісмаїлова проти Азербайджану» (Khadija Ismayilova v. Azerbaijan)*, 2019 (§§ 105-132), Суд постановив, що розголошення органами прокуратури приватної інформації, включаючи конфіденційні персональні дані, такі як ім'я та адреса заявниці, професійної журналістки, а також імена її друзів, родичів і колег у пресрелізі, що нібито містив звіт про хід кримінального розслідування, становило порушення статті 8 (*там само*, §§ 142-150).

249. У справі *«М.П. проти Португалії» (M.P. v. Portugal)*, 2021, §§ 48-49, надання колишнім чоловіком заявниці, без її згоди, в контексті провадження з розірвання шлюбу, електронних повідомлень, якими обмінювалася його дружина на сайті знайомств, до якого вона, як видається, надала йому доступ, не призвело до порушення статті 8, оскільки Суд у справах сім'ї в кінцевому підсумку не взяв їх до уваги, а доступ громадськості до даних у процедурі такого типу в будь-якому випадку був обмежений.

250. У справі *«Дж.С. проти Сполученого Королівства» (J.S. v. the United Kingdom)* (ухв.), 2015 (§§ 71-73), Суд відхилив як явно необґрунтовану скаргу на розголошення в пресрелізі прокуратури особистої інформації, яка не виходила за рамки тієї, що зазвичай надається ЗМІ у відповідь на запити про судовий розгляд, і не розкривала ні імені, ні віку, ні школи заявника (він був неповнолітнім, обвинуваченим у нападі на вчительку), ні будь-якої іншої особистої інформації.

251. У справі *«Л.Л. проти Франції» (L.L. v. France)*, 2006 (§§ 46), в якій суддя поклався, як на альтернативну й другорядну підставу, в рамках процесу розірвання шлюбу, на приватне листування між медичним консультантом і лікарем загальної практики заявника, що містило конфіденційний медичний документ, важливим фактором, який слід взяти до уваги, був той факт, що суддя або слідчий міг виключити медичні дані, про які йдеться, з обґрунтування рішення і все одно дійти такого ж висновку. Оскільки будь-хто міг отримати копію обґрунтування рішення без необхідності доводити особливий інтерес, втручання, якого зазнав заявник у своє право на повагу до приватного життя, не було виправданим з огляду на основоположну роль, яку відіграє захист персональних даних, незважаючи на те, що провадження між сторонами у справі про розлучення не було публічним, а рішення, яке було дійсним щодо третіх осіб, містило лише резолютивну частину (*там само*, §§ 47, 33).

252. У справі *«Вісент Дель Кампо проти Іспанії» (Vicent Del Campo v. Spain)*, 2018 (§§ 53, 56), той факт, що заявник, третя сторона судового провадження, був позбавлений можливості звернутися до суду до винесення рішення з проханням утриматися від розголошення його

особи, становив порушення статті 8. Заявник не був поінформований, не був допитаний, не був викликаний до суду і не був повідомлений у будь-який спосіб.

253. У справі, в якій національні суди обмежили десятирічним строком конфіденційність документів у матеріалах справи, що розголошують особу заявниці та її ВІЛ-позитивний статус, Суд встановив порушення статті 8 на тій підставі, що судові органи не надали достатньої ваги інтересам захисту персональних даних сторін і третіх осіб, які можуть бути зачеплені (*«Z проти Фінляндії» (Z v. Finland)*, 1997, §§ 111-112). Суд постановив, що серйозне втручання в її право на повагу до приватного життя, спричинене використанням у судовому процесі без її згоди інформації про стан її здоров'я, ще більше посилиться, якщо ця медична інформація стане доступною для громадськості через десять років (*там само*, § 112). Навпаки у справі *«Й. проти Туреччини» (Y. v. Turkey)* (ухв.), 2015 (§§ 81-82), той факт, що особа заявника та його ВІЛ-позитивний статус були розголошені в єдиному рішенні про відмову в юрисдикції, винесеному адміністративним судом, яке не було опубліковане або оприлюднене в будь-який інший спосіб і не було доступним для громадськості, в той час як жодне з інших рішень, винесених в контексті того ж провадження, не посилалося на це, не було визнано таким, що порушує право суб'єкта даних на повагу до його приватного життя.

254. У справі *«Дракшас проти Литви» (Drakšas v. Lithuania)*, 2012 (§ 60), розголошення в контексті процедури імпичменту записів телефонних розмов, перехоплених спецслужбами між заявником, відомим політиком, і президентом, якому було оголошено імпичмент, на публічному слуханні в Конституційному суді, що транслювалося в прямому ефірі національними телеканалами, не становило порушення статті 8. Суд дійшов висновку, що як публічна особа заявник неминуче і свідомо поставив себе під пильний контроль кожного свого слова й вчинку як з боку журналістів, так і з боку широкої громадськості. З огляду на це, передбачене законом розголошення його непублічних політичних або комерційних телефонних розмов під час конституційного провадження було необхідним для захисту прав інших осіб.

255. Див. також п. **Error! Reference source not found.** вище щодо розголошення пресі фотографій осіб, які перебувають під арештом або переслідуються, без їхньої згоди, а також пп. 80–82 вище щодо позитивних зобов'язань держави у справах, пов'язаних з розголошенням персональних даних приватними особами.

256. Див. також п. 251 вище щодо розголошення пресі фотографій осіб, які перебувають під арештом або кримінальним переслідуються, без їхньої згоди, а також п. 80-82 вище щодо позитивних зобов'язань Держави у справах, пов'язаних з розголошенням персональних даних приватними особами.

с. Розголошення даних з метою захисту здоров'я населення

257. Право особи на повагу до лікарської таємниці не є абсолютним і має розглядатися у зв'язку з іншими законними правами та інтересами, такими як право роботодавця на змагальний судовий розгляд (*«Eternit проти Франції» (Eternit v. France)* (ухв.), 2012, § 37). Це право може бути переважено необхідністю захисту фундаментального аспекту суспільного інтересу, такого як безпека персоналу лікарні та охорона здоров'я населення (*«Й. проти Туреччини» (Y. v. Turkey)* (ухв.), 2015, § 74).

258. У випадках лікування пацієнтів у лікарні та системі охорони здоров'я передача інформації про стан пацієнта може, за певних обставин, бути доречною та необхідною з метою не лише гарантування належного медичного лікування пацієнта, але й забезпечення захисту прав та інтересів медичних працівників, які беруть участь у його лікуванні, та інших пацієнтів, що дозволить вжити необхідних запобіжних заходів (*«Й. проти Туреччини» (Y. v. Turkey)* (ухв.), 2015, § 74). Якщо медичні працівники самі наражаються на ризик інфікування у зв'язку з виконанням своїх обов'язків, безпека персоналу лікарні та охорона громадського здоров'я

можуть виправдати передачу інформації про стан здоров'я пацієнта між медичним персоналом, який бере участь у його лікуванні, з метою запобігання будь-якому ризику передачі хвороби в межах лікарні (*там само*, § 78).

259. Конфіденційна інформація, така як дані про стан здоров'я пацієнта, повинна передаватися таким чином, щоб запобігти будь-якій формі стигматизації суб'єкта даних і забезпечити достатні гарантії для усунення будь-якого ризику зловживань («*Й. проти Туреччини*» (*Y. v. Turkey*) (ухв.), 2015, § 79). На одержувача інформації повинні поширюватися спеціальні правила конфіденційності, що стосуються медичних працівників, або аналогічні вимоги щодо конфіденційності (*там само*, § 74).

260. У справі «*Й. проти Туреччини*» (*Y. v. Turkey*) (ухв.), 2015 (§§ 78-79), Суд відхилив як явно необґрунтовану заяву щодо обміну інформацією про ВІЛ-позитивний статус пацієнта між різними медичними працівниками лікарні, де він проходив лікування, на тій підставі, що такий обмін інформацією був виправданий безпекою персоналу лікарні та захистом громадського здоров'я, незважаючи на той факт, що суб'єкт даних не давав на це своєї згоди. Суд надав важливого значення тому факту, що згідно з національним законодавством всі медичні працівники були зобов'язані дотримуватися конфіденційності будь-яких даних, переданих їм у зв'язку з їхнім становищем або родом діяльності, під загрозою дисциплінарних або кримінальних санкцій.

d. Розголошення даних з метою захисту національної безпеки

261. У низці справ, що стосуються демонтажу спадщини колишніх комуністичних режимів, Суд розглянув питання публічного розголошення даних, що стосуються далекого минулого особи, зібраних і збережених з метою захисту національної безпеки («*Соро проти Естонії*» (*Sõro v. Estonia*), 2015, § 58; «*Анчев проти Болгарії*» (*Anchev v. Bulgaria*) (ухв.), 2017, § 100). Важливе значення надається індивідуалізованим заходам, що застосовуються для процесу демонтажу, їх регулюванню та наданим гарантіям.

262. Так у справі «*Соро проти Естонії*» (*Sõro v. Estonia*), 2015 (§§ 56-64), розголошення інформації про те, що заявник працював водієм у колишніх службах безпеки, становило порушення статті 8. Хоча заявник був заздалегідь поінформований про те, що дані будуть опубліковані, і мав можливість оскаржити передачу даних, не існувало процедури для оцінки конкретних завдань, які виконували окремі співробітники колишніх служб безпеки, щоб диференціювати небезпеку, яку вони могли становити в демократичній системі через кілька років після закінчення кар'єри в цих установах (*там само*, § 61). Суд постановив, що будь-яка загроза, яку заявник міг спочатку становити для новоствореної демократії, повинна була значно зменшитися з плином часу між відновленням незалежності Естонії та публікацією персональних даних (*там само*, § 62). Хоча Закон про розголошення інформації сам собою не накладав жодних обмежень на нову роботу заявника, він був змушений звільнитися зі своєї посади через позицію його колег, що свідчить про серйозність втручання у право заявника на повагу до його приватного життя (*там само*, § 63).

263. І навпаки, у справі «*Анчев проти Болгарії*» (*Anchev v. Bulgaria*) (ухв.), 2017 (§§ 92-116), в якій процедура розголошення була суворо регламентована й супроводжувалася низкою гарантій проти свавілля і зловживань, включаючи той факт, що вона була доручена спеціальній незалежній комісії, рішення якої підлягали судовому перегляду на двох рівнях юрисдикції, публічне розголошення даних, що стосуються далекого минулого заявника, було визнано несумісним зі статтею 8. Оскільки розголошення не спричинило жодних санкцій або правових обмежень, втручання не вийшло за межі суттєвої свободи розсуду, якою користувалися органи влади (*там само*, §§ 106-113). Суд зазначив, що його висновок міг би бути іншим, якби Держава вжила заходів, що передбачають більш серйозне втручання в особисту сферу суб'єкта даних, таких як заборона на роботу або часткове позбавлення права голосу (*там само*, § 113).

е. Розголошення даних з метою захисту економічного добробуту країни

264. Заходи, які повинні забезпечити захист економічного добробуту країни і які порушують конфіденційність даних, зібраних або збережених органами влади, не обов'язково суперечать статті 8, якщо вони супроводжуються ефективними й задовільними гарантіями (*«М.С. проти Швеції» (M.S. v. Sweden)*, 1997, § 41). При збалансуванні різних конкуруючих інтересів важливими аспектами, які необхідно враховувати, є питання про те, чи регулює національне законодавство заходи, які повинні вживати обробники даних, чи передбачена їхня відповідальність у разі недотримання вимог законодавства, і чи зобов'язаний одержувач даних дотримуватися аналогічних правил і гарантій, зокрема, обов'язку зберігати конфіденційність (*там само*, § 43).

265. У справі *«М.С. проти Швеції» (M.S. v. Sweden)*, 1997 (§§ 31-44), передача медичної документації особи одним державним органом (гінекологічним відділенням лікарні) іншому (Департаменту соціального забезпечення), відповідальному за оцінку того, чи відповідає заявниця юридичним умовам для отримання допомоги, за якою вона сама звернулася, не була порушенням статті 8. Суд постановив, що ця передача даних потенційно мала вирішальне значення для розподілу державних коштів між заявниками, які цього заслуговують, а отже, може розглядатися як така, що переслідувала мету захисту економічного добробуту країни (*там само*, § 38). Розголошення конфіденційних даних заявниці супроводжувалося ефективними і задовільними гарантіями проти зловживань: згідно з відповідним національним законодавством, умовою для розголошення відповідних даних було те, що інформація мала бути важливою для застосування закону про страхування від нещасних випадків на виробництві (*там само*, §§ 18, 43); у разі недотримання цих умов співробітники гінекологічного відділення могли нести цивільну та/або кримінальну відповідальність (*там само*, §§ 22, 43); і на одержувача даних покладался аналогічний обов'язок дотримуватися їхньої конфіденційності (*там само*, §§ 20, 22, 43).

266. Справа *«Л.Б. проти Угорщини» (L.B. v. Hungary)* [ВП], 2023 (§§ 20-29) стосувалася публікації національним податковим органом персональних даних заявника (включаючи його ім'я та домашню адресу) на своєму вебсайті у списку великих податкових боржників. Запроваджена відповідним законодавством як інструмент боротьби з недотриманням податкового законодавства, систематична та обов'язкова публікація таких даних стосувалася всіх платників податків, які на кінець кварталу мали значну заборгованість зі сплати податків за період, що перевищував 180 днів поспіль. Суд зазначив, що вибір законодавцем такої загальної схеми сам собою не проблематичний, як і публікація даних про платників податків як така. Він також встановив, що Договірні Держави користуються широкою свободою розсуду при оцінці необхідності встановлення схеми поширення персональних даних платників податків, які не виконали свої зобов'язання зі сплати податків, як засобу, серед іншого, забезпечення належного функціонування системи збору податків в цілому. Однак він підкреслив, що цей розсуд не є безмежним, і зазначив, що в такому контексті він буде ретельно перевіряти, чи здійснили компетентні національні органи влади, чи то на законодавчому, виконавчому, чи судовому рівні, належний баланс між конкуруючими інтересами, і чи врахували вони при цьому не тільки (i) суспільний інтерес у поширенні інформації, про яку йдеться, але й (ii) характер розголошеної інформації; (iii) наслідки та ризик заподіяння шкоди приватному життю зацікавлених осіб; (iv) потенційне охоплення середовища, яке використовувалося для поширення інформації, зокрема, інтернету; та (v) основні принципи захисту даних, включаючи принципи обмеження мети, обмеження зберігання, мінімізації даних і точності даних. Суд також підкреслив, що існування процесуальних гарантій теж може відігравати важливу роль у вищезазначеному зв'язку (*там само*, § 128).

267. На основі фактів справи Суд виокремив дві особливості оскаржуваної схеми публікації: включення домашньої адреси до персональних даних платника податків, що підлягають

обов'язковій публікації, та відсутність будь-якої дискреції з боку національного податкового органу щодо проведення індивідуальної оцінки пропорційності. З огляду на це, було проаналізовано якість парламентського розгляду та виявлено такі недоліки: (i) не було проведено оцінку необхідності й додаткової цінності оскаржуваного загального заходу (особливо в частині, що стосується публікації домашньої адреси податкового боржника) на тлі існуючих інструментів з тією ж стримувальною метою; (ii) не було враховано вплив на право на приватне життя і, зокрема, ризик неправомірного використання домашньої адреси податкового боржника іншими членами суспільства; (iii) не було враховано потенційне охоплення середовища, яке використовувалося для поширення інформації, про яку йдеться (інтернет), що означає необмежений доступ до досить конфіденційної інформації (ім'я та домашня адреса), з ризиком повторної публікації як природного, ймовірного та передбачуваного наслідку первинної публікації; та (iv) не було враховано вимоги щодо захисту даних відповідно до національного законодавства й права ЄС, а також можливість розробки належних заходів реагування у світлі принципу мінімізації даних. На цьому тлі Суд дійшов висновку, що, попри широку свободу розсуду Держави-відповідача, оскаржуване втручання не було «необхідним у демократичному суспільстві» (*там само*, §§ 129-40).

f. Масове розголошення персональних даних

268. Існування суспільного інтересу в наданні доступу до великих обсягів податкових даних і дозволу на їхнє збирання не обов'язково або автоматично означало, що також існував суспільний інтерес у масовому поширенні таких необроблених даних у незміненому вигляді без будь-якого аналітичного втручання. У справі *«Сатакуннан Марккінапорссі Ой та Сатамедіа Ой проти Фінляндії» (Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland)* [ВП], 2017 (§ 175), Суд підкреслив, що слід розрізняти обробку даних для журналістських цілей та поширення необроблених даних, до яких журналісти мали привілейований доступ. Факт запобігання масовому розголошенню персональних податкових даних за процедурами, несумісними з національним законодавством і правилами ЄС щодо захисту даних, сам по собі не є санкцією, навіть якщо обмеження, накладені на обсяг інформації, що підлягає оприлюдненню, могли на практиці зробити деякі з видів діяльності компаній-заявників менш прибутковими (*там само*, § 197).

V. Права суб'єктів даних

269. Практика Суду надає суб'єктам персональних даних низку конкретних прав, які гарантують реалізацію їхніх прав, передбачених статтею 8.

1. Право на доступ до власних даних

270. Особи, чий персональні дані були зібрані та збережені органами влади, мають захищений статтею 8 інтерес в отриманні інформації: яка була зібрана про них колишніми спецслужбами за тоталітарних режимів і зберігалася в державних архівах (*«Гараламбіє проти Румунії» (Haralambie v. Romania)*, 2009, § 79; *«Йарнеа проти Румунії» (Jarnea v. Romania)*, 2011, § 50; *«Йоанна Шульц проти Польщі» (Joanna Szulc v. Poland)*, 2012, § 87); яка є необхідною щодо їхнього здоров'я або ризиків для здоров'я, яким вони піддалися (*«Роше проти Сполученого Королівства» (Roche v. the United Kingdom)* [ВП], 2005, § 155; *«К.Г. та інші проти Словаччини» (K.N. and Others v. Slovakia)*, 2009, § 44; *«Йончев проти Болгарії» (Yonchev v. Bulgaria)*, 2017, § 46); знати й розуміти їхнє дитинство та ранній розвиток (*«Гаскін проти Сполученого Королівства» (Gaskin v. the United Kingdom)*, 1989, § 41); або простежити їхнє походження, зокрема, особу їхніх батьків (*«Одієвре проти Франції» (Odièvre v. France)* [ВП], 2003, §§ 43-44; *«Годеллі проти Італії» (Godelli v. Italy)*, 2012, §§ 62-63; *«М.Г. проти Сполученого Королівства» (M.G. v. the United Kingdom)*, 2002, § 27).

271. У цих різних контекстах органи влади мають позитивне зобов'язання, притаманне ефективній повазі до приватного життя, як це передбачено статтею 8, забезпечити ефективну та доступну процедуру, що дозволяє заявнику мати доступ до всієї відповідної та належної інформації, необхідної для конкретних цілей («*Роше проти Сполученого Королівства*» (*Roche v. the United Kingdom*) [ВП], 2005, § 162; «*Гараламбіє проти Румунії*» (*Haralambie v. Romania*), 2009, § 86; «*Йоанна Шульц проти Польщі*» (*Joanna Szulc v. Poland*), 2012, §§ 86, 94).

272. І навпаки, якщо Держава обґрунтовано побоюється, що доступ до інформації, яка містить персональні дані, може поставити під загрозу ефективність системи таємного спостереження, призначеної для захисту національної безпеки або боротьби з тероризмом, вона може відмовити в доступі до інформації, зібраної та збереженої в таємному реєстрі, не порушуючи позитивного зобов'язання органів влади за статтею 8 («*Леандер проти Швеції*» (*Leander v. Sweden*), 1987, § 66; «*Зеґерштедт-Віберґ та інші проти Швеції*» (*Segerstedt-Wiberg and Others v. Sweden*), 2006, § 102). Щоб визначити, чи має право Держава вважати, що інтереси національної безпеки та боротьби з тероризмом переважають над інтересами особи бути поінформованою про повний обсяг інформації, що зберігається про неї в органах безпеки, Суд повинен переконатися в тому, що існують достатні гарантії проти свавілля. Якість закону (*там само*, §§ 79-80) і встановлені гарантії, зокрема, можливість перегляду оскаржуваного заходу і засоби правового захисту, доступні суб'єкту даних на національному рівні (*там само.*, §§ 52-68), — важливі критерії, які слід враховувати при збалансуванні конкуруючих інтересів (*там само*, § 103). Аналогічні принципи застосовуються в контексті висилки іноземців. У справі «*Гассіне проти Румунії*» (*Hassine v. Romania*), 2021, §§ 55-69, заявник, громадянин Тунісу, який законно проживав у Румунії, був висланий з країни з міркувань національної безпеки й оголошений небажаною особою в Румунії на п'ятирічний період на підставі певної інформації від румунських спецслужб, яка була класифікована як таємна, і яка нібито свідчила про те, що він займався діяльністю, здатною загрожувати національній безпеці. Ані заявник, ані його адвокат не були уповноважені ознайомитися з цими документами. Суд встановив, що адміністративне провадження щодо вислання заявника не було забезпечено необхідними процесуальними гарантіями, і визнав порушення статті 1 Протоколу № 7.

273. У справі про довгострокову реєстрацію персональних даних заявника в Шенгенській інформаційній системі Суд постановив, що відсутність у заявника повного особистого доступу до інформації, яку він запитував, не може порушувати право на повагу до його приватного життя з огляду на переважну необхідність захисту національної безпеки («*Далеа проти Франції*» (*Dalea v. France*) (ухв.), 2010). Хоча заявник не мав можливості оскаржити точні підстави для його включення до Шенгенської бази даних, йому було надано доступ до всіх інших даних, що стосуються його, і він був поінформований про те, що підставою для складання звіту стали міркування, пов'язані з державною безпекою, обороною і громадською безпекою (*там само*, з посиланням на «*Леандер проти Швеції*» (*Leander v. Sweden*), 1987, § 66).

274. Якщо лише деякі документи у справі, що зберігається органами влади на особу і містить персональні дані, були засекречені в цілях державної таємниці, органи влади могли надати заявнику частковий доступ до цієї справи («*Йончев проти Болгарії*» (*Yonchev v. Bulgaria*), 2017, §§ 55-59). Так у справі про відмову органів влади дозволити заявнику, колишньому співробітнику поліції, ознайомитися з окремими документами з його особової справи, а саме з його психологічними оцінками, Суд встановив порушення статті 8 через надмірно формальне національне регулювання, яке вимагало, щоб, якщо хоча б один з документів у справі був засекречений, решта автоматично також вважалася засекреченою і, отже, підпадала під дію правил про захист засекреченої інформації (*там само*, § 60).

275. Якщо національне законодавство прямо передбачало право на доступ до особистої справи, яка велася і зберігалася колишніми службами безпеки за тоталітарних режимів у колишніх комуністичних Державах, Держава була зобов'язана запровадити ефективну й

доступну процедуру, що дозволяє суб'єкту даних мати розумно швидкий доступ до всієї відповідної інформації («*Гараламбіє проти Румунії*» (*Haralambie v. Romania*), 2009, § 86; «*Йарнеа проти Румунії*» (*Jarnea v. Romania*), 2011, § 50; «*Антонета Тудор проти Румунії*» (*Antoneta Tudor v. Romania*), 2013, § 34; «*Йоанна Шульц проти Польщі*» (*Joanna Szulc v. Poland*), 2012, §§ 86, 94). Суд встановив порушення статті 8 у справі, в якій заявнику було надано доступ лише до частини справи, заведеної на його ім'я, яка була зареєстрована і зберігалася колишніми спецслужбами («*Йарнеа проти Румунії*» (*Jarnea v. Romania*), 2011, §§ 54-60), а також у двох інших справах, в яких заявникам було надано доступ до їхніх документів лише через десять років після їхнього первинного запиту («*Йоанна Шульц проти Польщі*» (*Joanna Szulc v. Poland*), 2012, §§ 93-95; «*Антонета Тудор проти Румунії*» (*Antoneta Tudor v. Romania*), 2013, §§ 34-40). Недоліки архівної системи або фактичні помилки, такі як реєстрація неправильної дати народження в особовій справі заявника, не могли виправдати шестирічну затримку в наданні йому доступу до його персональних даних («*Гараламбіє проти Румунії*» (*Haralambie v. Romania*), 2009, § 95). Похилий вік особи, яка запитувала доступ до такого роду інформації, надавав ще більшої нагальності її інтересу простежити свою особисту історію за часів тоталітарного режиму (*там само*, § 93 *наприкінці*).

276. Що стосується інформації про стан здоров'я або ризики для здоров'я, право на доступ до персональних даних поширюється на надання суб'єкту даних копій його або її файлів даних («*К.Г. та інші проти Словаччини*» (*K.H. and Others v. Slovakia*), 2009, § 47). Саме володілець файлу визначає порядок копіювання файлів персональних даних і те, чи повинен суб'єкт даних нести витрати на копіювання (*там само*, § 48). Суб'єкти даних не повинні бути зобов'язані спеціально обґрунтовувати запит на отримання копії своїх персональних даних. Радше органи влади повинні довести, що існують вагомі причини для відмови в наданні такої можливості (*там само*, § 48). У справі «*К.Г. та інші проти Словаччини*» (*K.H. and Others v. Slovakia*), 2009 (§§ 50-58), колишні пацієнти лікарні не змогли зробити фотокопії своїх оригінальних медичних карток, які були зібрані й зберігалися в державній лікарні, включаючи інформацію, яку вони вважали важливою з точки зору власної моральної та фізичної цілісності. Суд постановив, що єдина можливість, запропонована лікарнею, — зробити рукописні виписки з оригінальних файлів — не забезпечила їм ефективного доступу до відповідних документів, що стосуються їхнього здоров'я.

277. Якщо Уряд здійснює небезпечну діяльність, яка може мати приховані негативні наслідки для здоров'я тих, хто бере участь у такій діяльності, органи влади мають позитивний обов'язок забезпечити «ефективну й доступну процедуру», що дозволяє заявнику мати доступ до «всієї відповідної та належної інформації», яка б дозволила йому оцінити будь-який ризик, на який він наражається («*Мак'їнлі та Еґан проти Сполученого Королівства*» (*McGinley and Egan v. the United Kingdom*), 1998, § 101; «*Роше проти Сполученого Королівства*» (*Roche v. the United Kingdom*) [ВП], 2005, § 161-162). Необґрунтований період очікування, наприклад, коли медичні інформаційні та дослідницькі служби ініціювали відповідні процедури пошуку й розголошення документів майже через десять років після того, як заявник почав шукати відповідні документи, означає невиконання Державою, в порушення статті 8, свого позитивного зобов'язання щодо поваги до приватного життя суб'єкта даних, попри труднощі, пов'язані з віком і розосередженим характером документів (*там само*, § 166).

278. Що стосується доступу до персональних даних особи, яка, будучи дитиною, була взята під опіку після смерті батьків або через їхню нездатність піклуватися про неї, то система, яка ставить доступ до файлів у залежність від згоди «учасників записів», тобто осіб, які створили відповідні документи, може, в принципі, бути сумісною зі статтею 8 в межах свободи розсуду держави. Однак, така система повинна захищати інтереси кожного, хто бажає ознайомитися з документами, що стосуються його приватного та сімейного життя, і відповідати принципу пропорційності лише тоді, коли вона передбачає, що незалежний орган остаточно вирішує, чи повинен бути наданий доступ у випадках, коли особа, яка надала інформацію, не відповідає

або відмовляється надати згоду («*Гаскін проти Сполученого Королівства*» (*Gaskin v. the United Kingdom*), 1989, § 49). У випадках, коли національна система не передбачала оскарження до такого органу у разі відмови соціальних служб надати доступ до всіх документів у певній справі, у тому числі, коли третя сторона, яка стосується інформації або є джерелом такої інформації, не дає згоди на її розголошення, Суд визнав порушення статті 8 (*там само*, § 49; «*М.Г. проти Сполученого Королівства*» (*M.G. v. the United Kingdom*), 2002, §§ 30-32).

279. Суд вважає, що дитина, народжена поза шлюбом, яка прагне встановити правовий зв'язок зі своїм біологічним батьком, має життєво важливий інтерес, захищений Конвенцією, в отриманні інформації, необхідної для того, щоб дізнатися правду про важливий аспект своєї особистої ідентичності («*Мікуліч проти Хорватії*» (*Mikulić v. Croatia*), 2002, § 64; «*Болевіч проти Сербії*» (*Boljević v. Serbia*), 2020, § 50). Система, яка не має засобів примусити передбачуваного батька виконати рішення суду про проведення тесту ДНК, може в принципі вважатися сумісною із зобов'язаннями, що випливають зі статті 8, з огляду на свободу розсуду держави («*Мікуліч проти Хорватії*», 2002, § 64). Однак, відсутність будь-якого процесуального заходу примусу передбачуваного батька до виконання судового рішення відповідає принципу пропорційності лише в тому випадку, якщо він передбачає альтернативні засоби, що дозволяють незалежному органу швидко розглянути позов про встановлення батьківства (*там само*, § 64). Суд встановив порушення статті 8 у справі, де, якщо передбачуваний батько відмовлявся брати участь у медичній процедурі, національна система не передбачала жодних заходів, щоб змусити його пройти ДНК-тест, або альтернативних засобів, які б дозволили незалежному органу швидко визначити позов про встановлення батьківства (*там само*, § 64). Зацікавленість особи у встановленні власного батьківства не зникає з віком, а навпаки («*Йеггі проти Швейцарії*» (*Jäggi v. Switzerland*), 2006, § 40, щодо відмови надати дозвіл на проведення ДНК-тесту померлої особи на вимогу її передбачуваного сина, який бажав встановити своє законне походження; «*Болевіч проти Сербії*» (*Boljević v. Serbia*), 2020, § 54).

280. У випадку дітей, народжених анонімно, питання доступу до свого походження та інформації про особу біологічних батьків відрізняється від питання доступу до матеріалів справи дитини, яка перебуває під опікою, або до доказів передбачуваного батьківства («*Одієвре проти Франції*» (*Odièvre v. France*) [ВП], 2003, § 43; «*Годеллі проти Італії*» (*Godelli v. Italy*), 2012, § 62). Залежно від широкого спектру різних правових систем і традицій, Держави повинні були користуватися певним ступенем свободи розсуду у збереженні конфіденційності особи біологічних батьків («*Одієвре проти Франції*» (*Odièvre v. France*) [ВП], 2003, § 46; «*Годеллі проти Італії*» (*Godelli v. Italy*), 2012, § 65). Національна система, яка надавала заявнику доступ до інформації про його матір та його біологічну сім'ю, за якою не можна ідентифікувати особу, що дозволяло йому встановити деяку інформацію про своє минуле без шкоди для інтересів третіх осіб, а також можливість, згідно з нещодавно прийнятим законодавством, звернутися до послуг незалежного органу, уповноваженого допомагати особам знайти своє біологічне походження, з метою забезпечення розголошення особи його матері, за умови її згоди, була визнана сумісною зі статтею 8 («*Одієвре проти Франції*» (*Odièvre v. France*) [ВП], 2003, § 49; див. також, щодо доступу осіб, народжених за допомогою допоміжних репродуктивних технологій за участю стороннього донора, про доступ до інформації про цього донора, «*Говен-Фурні і Сілію проти Франції*» (*Gauvin-Fournis and Silliau v. France*), 2023, §§ 113-33). І навпаки, система, яка віддавала сліпу перевагу бажанню матері залишитися анонімною та не надавала усиновленій дитині, яка не була визнана при народженні, можливості звернутися за доступом до інформації, що не ідентифікує її походження, або за розголошенням особи її матері, була визнана несумісною з вимогами статті 8 («*Годеллі проти Італії*» (*Godelli v. Italy*), 2012, §§ 70-72).

2. Право на виправлення

281. Суд розглянув декілька справ, що стосувалися зберігання органами влади неправдивих даних або даних, точність яких оскаржувалася заявником («*Ротару проти Румунії*» (*Rotaru v. Romania*) [ВП], 2000, §§ 42-44, 55-63, щодо неможливості заявника спростувати дані про його передбачувану участь у румунському русі легіонерів у справі, заведеної службою безпеки; «*Кемалеттін Канлі проти Туреччини*» (*Cemalettin Canli v. Turkey*), 2008, §§ 34-37, щодо включення до судового розгляду неповних персональних даних, зібраних поліцією; «*Хелілі проти Швейцарії*» (*Khelili v. Switzerland*), 2011, § 56, щодо збереження в поліцейських файлах запису «повія» як роду занять особи, яка сама завжди заперечувала, що займається проституцією).

282. Неможливість особи домогтися виправлення повідомлення про неї в базі даних Шенгенської угоди («*Далеа проти Франції*» (*Dalea v. France*) (ухв.), 2010) та реєстрація етнічного походження особи в офіційних документах («*Чиботару проти Молдови*» (*Ciubotaru v. Moldova*), 2010, § 59) становлять втручання в її право на повагу до приватного життя. За деяких обставин, зокрема, коли йдеться про міркування державної безпеки, національної оборони та громадської безпеки, таке втручання не обов'язково є несумісним зі статтею 8 («*Далеа проти Франції*» (ухв.), 2010). Існування гарантій проти свавілля та можливість ретельного вивчення відповідного заходу незалежним і неупередженим органом, компетентним розглядати всі відповідні питання факту і права, з метою визначення законності заходу і засудження можливого зловживання з боку органів влади, є важливими (*там само*, з посиланням на справу «*Леандер проти Швеції*» (*Leander v. Sweden*), 1987, § 66).

283. Неправдива або неповна персональна інформація, зібрана й збережена органами влади, може ускладнити повсякденне життя суб'єкта даних («*Хелілі проти Швейцарії*» (*Khelili v. Switzerland*), 2011, § 64), виявитися наклепницькою («*Ротару проти Румунії*» (*Rotaru v. Romania*) [ВП], 2000, § 44) або усунути ряд істотних процесуальних гарантій, передбачених законом для захисту прав суб'єктів даних («*Кемалеттін Канлі проти Туреччини*» (*Cemalettin Canli v. Turkey*), 2008, §§ 35, 40-42). У справі, в якій національному суду було представлено поліцейську справу під назвою «інформаційна довідка про інші правопорушення», в якій згадувалися дві кримінальні справи, порушені проти обвинуваченого в минулому за членство в нелегальних організаціях, Суд встановив порушення статті 8. У цій справі не тільки викладена у справі інформація була неправдивою, але також у справі не згадувалося про виправдання заявника за першою кримінальною справою і про закриття провадження за другою (*там само*, § 42). Відсутність згадки про результати двох проваджень суперечило зобов'язанням, чітко викладеним у національному законодавстві, і таким чином усунуло низку суттєвих процесуальних гарантій, передбачених законом для захисту прав заявника (*там само*, 2008, § 42).

284. Факт накладення на особу, яка вимагає виправлення її персональних даних в офіційних державних реєстрах, вимоги, що створює для неї непереборні бар'єри, може виявитися несумісним із зобов'язанням Держави гарантувати ефективну повагу до її приватного життя («*Чиботару проти Молдови*» (*Ciubotaru v. Moldova*), 2010, §§ 51-59). У справі, що стосувалася нездатності заявника домогтися зміни запису про своє етнічне походження в офіційних реєстрах, вимога довести, що його батьки належали до певної етнічної групи, створила непереборні бар'єри для суб'єкта даних при реєстрації етнічної ідентичності, відмінної від тієї, яка була записана щодо його батьків органами влади (*там само*, § 57).

285. У контексті запитів про внесення змін до реєстрів актів цивільного стану з метою врахування післяопераційного статусу транссексуала, узгодженість адміністративної та правової практики в рамках національної системи повинна розглядатися як важливий фактор при оцінці таких запитів за статтею 8 («*Крістін Гудвін проти Сполученого Королівства*» (*Christine Goodwin v. the United Kingdom*) [ВП], 2002, § 78). У справі про відмову органів влади

внести зміни до запису про народження в реєстрі Суд заявив, що його вразив той факт, що зміна статі, яка передбачена законом, не має повного визнання в законодавстві, що може розглядатися як останній та кульмінаційний крок у тривалому й складному процесі трансформації, який пройшов транссексуал (*там само*, § 78, переглядаючи свою судову практику, щоб врахувати розвиток науки й суспільства з часу винесення таких попередніх рішень, як у справах «*Різ проти Сполученого Королівства*» (*Rees v. the United Kingdom*), 1986, §§ 42-44, «*Коссі проти Сполученого Королівства*» (*Cossey v. the United Kingdom*), 1990, §§ 39-40, та «*Шеффілд і Горшем проти Сполученого Королівства*» (*Sheffield and Horsham v. the United Kingdom*) [ВП], 1998, §§ 60-61). Якщо Держава дозволила лікування та хірургічне втручання для полегшення стану транссексуала, профінансувала або допомогла у фінансуванні операцій, а також дозволила штучне запліднення жінки, яка живе з чоловіком-транссексуалом, видається нелогічним відмовлятися визнавати правові наслідки результату, до якого призводить лікування («*Крістін Гудвін проти Сполученого Королівства*» (*Christine Goodwin v. the United Kingdom*) [ВП], 2002, § 78), тим більше, що труднощі, пов'язані з виправленням початкового запису про стать у книзі реєстрації народжень, далеко не є непереборними (*там само*, § 91).

286. У справі «*С.В. проти Італії*» (*S.V. v. Italy*), 2018 (§ 72), відмова органів влади надати дозвіл на зміну прізвища транссексуальній особі під час процесу гендерного переходу і до завершення операції зі зміни статі ґрунтувалася на жорсткому судовому розгляді, який поставив заявницю на необґрунтовано тривалий час (два з половиною роки) в аномальне становище, в якому вона була схильна відчувати почуття уразливості.

287. У справі «*Гемелеїнен проти Фінляндії*» (*Hämäläinen v. Finland*) [ВП], 2014 (§§ 87-89), на думку Суду, не було непропорційним вимагати, як передумову юридичного визнання набутої статі, щоб шлюб заявниці був змінено на зареєстроване партнерство, оскільки це був реальний варіант, який надавав одностатевим парам правовий захист, майже ідентичний правовому захисту шлюбу (у Фінляндії гомосексуальні шлюби незаконні). Отже, незначні відмінності між цими двома правовими концепціями не такі, щоб зробити чинну фінську систему недосконалою з точки зору позитивного зобов'язання Держави. Див. також «*А.П., Гарсон і Ніко проти Франції*» (*A.P., Garçon and Nicot v. France*), 2017, щодо правових умов зміни цивільного статусу трансгендерних осіб, таких як незворотний характер зміни зовнішності (§§ 116-135), реальність розладу гендерної ідентичності (§§ 138-144) та обов'язок пройти медичне обстеження (§§ 149-154).

3. Право на видалення даних

288. Суд розглядав питання права на видалення персональних даних після певного періоду часу в різних контекстах, і, зокрема, щодо:

- «права бути забутим», що стосується вибору або практики засобів масової інформації (повторно) публікувати та/або залишати на своїх вебсайтах інформацію або архіви, що містять персональні дані про осіб, як-от їхні прізвища, імена та фотографії, які були розголошені в минулому («*Венгжиновський і Смольчевський проти Польщі*» (*Węgrzynowski and Smolczewski v. Poland*), 2013; «*М.Л. та В.В. проти Німеччини*» (*M.L. and W.W. v. Germany*), 2018; «*Бьянкарді проти Італії*» (*Biancardi v. Italy*), 2021; «*Медіенгруппе Остеррайх ГмбХ проти Австрії*» (*Mediengruppe Österreich GmbH v. Austria*), 2022; «*Гурбейн проти Бельгії*» (*Hurbain v. Belgium*) [ВП], 2023);
- можливості осіб, обвинувачених або просто підозрюваних у вчиненні злочину, домогтися після певного періоду часу видалення своїх персональних даних (профіль ДНК, фотографії особи та відбитки пальців), зібрані органами влади в базах даних, спрямованих на запобігання та боротьбу зі злочинністю («*Б.Б. проти Франції*» (*B.B. v. France*), 2009; «*Гардель проти Франції*» (*Gardel v. France*), 2009; «*М.Б. проти*

Франції» (M.V. v. France), 2009; «М.К. проти Франції» (M.K. v. France), 2013; «Брунет проти Франції» (Brunet v. France), 2014; «Айкагуер проти Франції» (Aycaquer v. France), 2017; «Кетт проти Сполученого Королівства» (Catt v. the United Kingdom), 2019; «Гогран проти Сполученого Королівства» (Gaughran v. the United Kingdom), 2020));

- нездатності особи домогтися видалення своїх попередніх судимостей з поліцейського досьє після закінчення певного періоду часу (*«М.М. проти Сполученого Королівства» (M.M. v. the United Kingdom), 2012);*
- тривалого зберігання в архівах служби безпеки персональних даних заявників, які вже не відповідали вимозі «необхідності в демократичному суспільстві» з огляду на їхній характер та вік (*«Зегерстедт-Віберг та інші проти Швеції» (Segerstedt-Wiberg and Others v. Sweden), 2006).*

а. «Право на забуття»

289. Хоча концепція «права на забуття» з'явилася нещодавно і все ще перебуває на стадії розробки, її застосування на практиці вже набуло низки характерних рис (*«Гурбейн проти Бельгії» (Hurbain v. Belgium)* [ВП], 2023, §§ 191 і 194). Ця концепція вперше з'явилася в національній судовій практиці в контексті повторної публікації в пресі раніше розголошеної інформації судового характеру, коли особа, яка заявляла про «право на забуття», фактично прагнула домогтися винесення судового рішення проти особи, яка повторно опублікувала інформацію (*там само*, § 194). Згодом у національній судовій практиці з'явився новий аспект «права на забуття», пов'язаний з оцифруванням новинних статей, що призвело до їх широкого розповсюдження на вебсайтах відповідних газет. Ефект такого поширення був одночасно посилений включенням вебсайтів до переліку пошукових систем. Цей аспект, відомий як «право на забуття в інтернеті», стосується запитів на видалення або зміну даних, доступних в інтернеті, або на обмеження доступу до цих даних, що спрямовані проти видавців новин або операторів пошукових систем. У таких випадках питання полягає не в тому, щоб інформація з'явилася знову, а в тому, щоб вона залишалася доступною в інтернеті (*там само*, § 195). Загалом, «право на забуття» на практиці може призвести до різних заходів, яких можуть вжити оператори пошукових систем або видавці новин. Вони стосуються або змісту заархівованої статті (наприклад, видалення, зміни або анонімізації статті), або обмеження доступу до інформації. В останньому випадку обмеження доступу можуть бути встановлені як пошуковими системами, так і видавцями новин (*там само*, § 175).

300. У своїй практиці Суд розглядав декілька справ, що стосувалися запитів про видалення, зміну, анонімізацію або деіндексацію новинних статей, які розголошують персональні дані фізичних осіб. Ці справи розглядалися або за статтею 8, якщо вони подавалися фізичними особами, які посилалися на своє право на повагу до приватного життя (*«Венгжиновський і Смольчевський проти Польщі» (Węgrzynowski and Smolczewski v. Poland), 2013; «М.Л. та В.В. проти Німеччини» (M.L. and W.W. v. Germany), 2018),* або за статтею 10, якщо вони подавалися журналістами, редакторами або власниками ЗМІ, які посилалися на своє право на свободу вираження поглядів (*«Бьянкарді проти Італії» (Biancardi v. Italy), 2021; «Медіенгруппе Остеррайх ГмБХ проти Австрії» (Mediengruppe Österreich GmbH v. Austria), 2022; «Гурбейн проти Бельгії» (Hurbain v. Belgium)* [ВП], 2023).

301. Зокрема, у справі *«Бьянкарді проти Італії» (Biancardi v. Italy), 2021*, Суд вперше отримав можливість винести рішення щодо сумісності зі статтею 10 цивільного позову проти журналіста за те, що він не деіндексував конфіденційну інформацію, опубліковану в інтернеті щодо кримінальних проваджень проти приватних осіб, і рішення журналіста залишити цю інформацію у вільному доступі, незважаючи на протидію зацікавлених осіб. У цій справі не виникло питання про анонімізацію особи в онлайн-статті. Суд зазначив, що стаття залишалася легкодоступною в інтернеті протягом восьми місяців після офіційного звернення зацікавлених

осіб з проханням видалити її. Суворість санкції — відповідальність за цивільним, а не кримінальним правом — і сума присудженої компенсації не видалися надмірними.

290. У контексті первинної публікації інформації, що стосується минулого особи, Суд розглянув справу *«Медіенгруппе Остеррайх ГмБХ проти Австрії» (Mediengruppe Österreich GmbH v. Austria)*, 2022, яка стосувалася судового наказу, що вимагав від щоденної газети не публікувати певну інформацію про особу, опосередковано пов'язану з передвиборчою кампанією політичного кандидата напередодні президентських виборів. Газета опублікувала фотографію брата офіс-менеджера кандидата на «правій сцені» і повідомила, що він був «засудженим неонацистом». Між цим засудженням і публікацією статті, про яку йдеться, минуло понад двадцять років, а з моменту його звільнення з в'язниці — близько сімнадцяти років; крім того, на момент публікації статті судимість вже була вилучена з його кримінального досьє. Національний вищий суд вказав на відсутність часового зв'язку і заборонив компанії-заявнику публікувати фотографії брата офіс-менеджера без його згоди, якщо в тій же статті в супровідному повідомленні повідомлялося, що він був засуджений за неонацизм. Суд не знайшов порушення статті 10, підкресливши, зокрема, проміжок часу між засудженням, звільненням і публікацією статті, про яку йдеться; втрату особою сумнозвісної слави; той факт, що вона більше не була засуджена до кримінальної відповідальності; важливість реінтеграції в суспільство осіб, які відбули покарання; а також їхній законний і дуже значний інтерес у тому, щоб через певний час більше не зіштовхуватися із власним засудженням.

291. Що стосується вебархівів ЗМІ, котрі містять персональні дані особи, яка була предметом публікації в минулому, Суд зазначив, що цей контекст відрізняється від ситуацій, пов'язаних з первинною публікацією (*«Гурбейн проти Бельгії» (Hurbain v. Belgium)* [ВП], 2023, § 205), і визначив, що основним питанням, яке необхідно вирішити, є подальша доступність такої інформації в інтернеті, а не її первинна публікація (*там само*, § 174).

292. У цьому контексті відмова судів ухвалити рішення про вилучення статті, яка завдавала шкоди репутації адвоката й була доступна в інтернет-архівах газети, була визнана такою, що не порушує статтю 8 у справі *«Венгжиновський і Смольчевський проти Польщі» (Węgrzynowski and Smolczewski v. Poland)*, 2013 (§§ 60-70). Суд визнав, що судові органи не повинні займатися переписуванням історії, наказуючи вилучати із суспільного надбання всі сліди публікацій, які в минулому були визнані остаточними судовими рішеннями як такі, що становлять невинуватий напад на репутацію особи (*там само*, § 65). Крім того, законний інтерес громадськості до доступу до публічних інтернет-архівів преси захищається статтею 10 (*там само*, § 65). Варто зазначити, що польські суди звернули увагу на те, що до статті на сайті газети було б бажано додати коментар, який би інформував громадськість про результати першого етапу провадження. На думку Суду, це свідчить про те, що національні суди усвідомлювали значення, яке публікації, доступні широкому загалу в інтернеті, можуть мати для ефективного захисту прав особистості, і що вони оцінили цінність наявності на вебсайті газети повної інформації про судові рішення, що стосуються статті. Адвокат не просив додати до статті посилання на попередні судові рішення на його користь (*там само*, §§ 66-67).

293. У справі *«М.Л. та В.В. проти Німеччини» (M.L. and W.W. v. Germany)*, 2018, двоє осіб, які були засуджені за вбивство і через чотирнадцять років вийшли на свободу, відбувши термін покарання, безуспішно просили видалити з вебархіву газети їхні фотографії та повну інформацію про них (прізвища та імена), щоб дати їм змогу почати нове життя поза увагою громадськості. Суд не знайшов порушення статті 8 на тій підставі, що суспільний інтерес у доступі до точних і об'єктивних архівів повинен мати пріоритет (*там само*, § 116). Зокрема, Суд взяв до уваги такі міркування: той факт, що на момент подання заявниками заяв про анонімність оскаржувани повідомлення продовжували сприяти обговоренню питань, що становлять суспільний інтерес; той факт, що заявники не були просто приватними особами, невідомими громадськості; поведінку заявників щодо засобів масової інформації, до яких вони звернулися після винесення вироку з метою поновлення провадження у справі; той факт, що

повідомлення висвітлювали факти об'єктивно і без наміру представити заявників у принизливому світлі або завдати шкоди їхній репутації; а також обмежену доступність інформації (*там само*, §§ 98-115).

294. У справі «Гурбейн проти Бельгії» (*Hurbain v. Belgium*) [ВП], 2023, Суд переглянув свою існуючу судову практику та скоригував критерії, які мають застосовуватися для збалансування відповідних прав за статтею 8 і статтею 10 щодо подальшої доступності електронної архівної версії статті, що розкриває персональні дані особи. Справа була порушена видавцем газети, якого національні суди зобов'язали анонімізувати електронну архівну версію статті, яка була опублікована близько двадцяти років тому і містила точний звіт про смертельну аварію, на підставі «права на забуття» водія, який спричинив цю аварію.

295. У своєму рішенні Суд визнав негативні наслідки постійної доступності певної інформації в інтернеті, зокрема, значний вплив на те, як відповідна особа сприймається громадською думкою, а також ризики, пов'язані зі створенням профілю відповідної особи та фрагментарним і викривленим представленням реальності. Утім, він пояснив, що вимога про право бути забутим не є самостійним правом, захищеним Конвенцією, і тією мірою, якою вона охоплюється статтею 8, може стосуватися лише певних ситуацій і відомостей (*там само*, § 199).

296. Далі Суд роз'яснив, що баланс відповідних прав (які мають рівну цінність), що має здійснюватися в контексті запиту на зміну архівного журналістського контенту в інтернеті, повинен враховувати такі критерії: (i) характер архівної інформації; (ii) час, що минув з моменту подій і з моменту первинної та онлайн публікації; (iii) сучасний інтерес до інформації; (iv) чи добре відома особа, яка претендує на право бути забутою, та її поведінка після подій; (v) негативні наслідки подальшої доступності інформації в інтернеті; (vi) ступінь доступності інформації в цифрових архівах; і (vii) вплив заходу на свободу вираження поглядів і, зокрема, на свободу преси (*там само*, § 205).

297. Крім того, Суд підкреслив, що в більшості випадків для визначення захисту, який повинен надаватися приватному життю, необхідно одночасно враховувати кілька критеріїв у порівнянні з іншими інтересами, що перебувають під загрозою, і засобами, що застосовуються для забезпечення цього захисту в конкретній справі. Так захист приватного життя в контексті утвердження права на забуття не може розглядатися у відриві від засобів, за допомогою яких він реалізується на практиці. З цієї точки зору, мова йде про проведення балансу з метою встановлення того, чи не є надмірною, з огляду на відповідне значення конкуруючих інтересів та обсяг засобів, використаних у конкретній справі, значення, надане «праву на забуття» через право на повагу до приватного життя або свободу вираження поглядів, або ж свободу вираження поглядів. Крім того, не всі критерії, що застосовувалися, мали однакове значення. Особливу увагу слід було приділити належному балансуванню, з одного боку, інтересів осіб, які вимагають вжиття заходів, і, з іншого боку, впливу таких запитів на видавців. Принцип збереження цілісності архівів преси вимагав, щоб зміна і, тим паче, видалення контенту обмежувалося лише тим, що є суворо необхідним, щоб запобігти будь-якому негативному впливу на виконання пресою свого завдання з поширення інформації та ведення архівів (*там само*, § 206 і 211).

298. Застосовуючи вищезазначені критерії до обставин справи, що розглядається, Суд зазначив, що національні суди узгоджено врахували характер і серйозність судових фактів, викладених у статті, про яку йдеться, той факт, що стаття не мала актуального, історичного або наукового інтересу, а також той факт, що відповідна особа не була добре відома. Крім того, вони надали важливого значення серйозній шкоді, якої зазнала ця особа в результаті подальшої наявності статті в інтернеті з необмеженим доступом, що могло створити «віртуальну судимість», особливо з огляду на тривалий час, що минув з моменту первинної публікації статті. Крім того, розглянувши заходи, які можна було б розглянути з метою забезпечення балансу прав, Суд постановив, що анонімізація статті не покладала на заявника

надмірного і нездійсненого тягаря, водночас будучи найбільш ефективним засобом захисту приватного життя зазначеної особи (*там само*, § 255). Таким чином, Суд був задоволений тим, що національні суди провели належну перевірку, і не виявив порушення статті 10 (*там само*, § 256).

б. Інші контексти

299. У справі *«М.М. проти Сполученого Королівства» (M.M. v. the United Kingdom)*, 2012, §§187-207, довічна реєстрація попередження в поліцейському досьє особи призвела до встановлення порушення статті 8. Суд постановив, що судимість або попередження, винесені особі в минулому, з плином часу стають невід'ємною частиною її приватного життя, яку необхідно поважати. Хоча дані про судимість у певному сенсі становлять публічну інформацію, їхнє систематичне зберігання в центральних архівах означає, що вони можуть бути розголошені через тривалий час після події, коли всі, крім суб'єкта даних, ймовірно, вже забудуть про інцидент. Суд визнав тривожним той факт, що критерії перевірки для видалення даних були дуже обмежувальними, і що запити на видалення дозволялися лише у виняткових випадках (*там само*, § 202).

300. Суд вважає, що коли Держава розширює межі своєї свободи розсуду до крайнощів, максимізуючи власні повноваження у сфері зберігання даних, тобто зберігає дані на невизначений строк, вирішальне значення має наявність ефективних гарантій, що передбачають видалення персональних даних, коли їхнє подальше зберігання стає непропорційним (*«Кетт проти Сполученого Королівства» (Catt v. the United Kingdom)*, 2019, § 119; *«Гогран проти Сполученого Королівства» (Gaughran v. the United Kingdom)*, 2020, § 94). Суд встановив порушення статті 8 у справі, в якій біометричні дані та фотографії заявника, засудженого за керування в стані алкогольного сп'яніння, зберігалися відповідно до політики безстрокового зберігання персональних даних осіб, визнаних винними у вчиненні кримінального правопорушення (*там само*, § 98). Не існувало положення, яке дозволяло б заявнику подати заяву про видалення даних, що його стосуються, якщо збереження даних більше не було необхідним з огляду на характер правопорушення, вік особи, тривалість часу, що минув, та особистість людини, яка зараз перебуває під слідством. Поліція могла видаляти біометричні дані та фотографії засуджених лише у виняткових випадках. Можливості перегляду були настільки вузькими, що були майже гіпотетичними (*там само*, § 94).

301. Брак ефективних гарантій щодо видалення персональних даних, які більше не є актуальними для цілей зберігання, викликає особливе занепокоєння у випадку особливих категорій конфіденційних персональних даних, які потребують підвищеного рівня захисту (*«Кетт проти Сполученого Королівства» (Catt v. the United Kingdom)*, 2019, § 112). У справі, що стосувалася зберігання в поліцейській базі даних конфіденційних даних про мирного демонстранта, які розкривали його політичні погляди, Суд встановив порушення статті 8 (*там само*, § 128). За відсутності будь-яких правил щодо максимального строку зберігання таких даних, заявник повністю залежав від того, наскільки ретельно органи влади застосовуватимуть гарантії, викладені у відповідному кодексі практики, які є дуже гнучкими, з метою забезпечення пропорційності строку зберігання його даних. Суд постановив, що гарантія видалення даних має обмежений вплив у випадках, коли органи влади відмовляються видалити дані на вимогу суб'єкта даних або пояснити причини свого рішення про їхнє зберігання (*там само*, §§ 118 і 122).

302. У декількох справах, що стосувалися зберігання персональних даних осіб, засуджених за сексуальне насильство, Суд не виявив порушення статті 8, зазначивши, що суб'єкти даних мали можливість подати запит на видалення, якщо зберігання їхніх даних більше не здавалося доречним з огляду, зокрема, на сплив часу з моменту їх засудження (*«Б.Б. проти Франції» (B.B. v. France)*, 2009, §§ 66-68; *«Гардель проти Франції» (Gardel v. France)*, 2009, §§ 67-69; *«М.Б. проти Франції» (M.B. v. France)*, 2009, §§ 58-60). Водночас відсутність можливості вимагати

видалення даних не обов'язково означає порушення статті 8 і має оцінюватися у світлі мети, яку переслідує зберігання таких даних, характеру дати, а також гарантій, наданих зацікавленим особам проти ризику свавілля і зловживань. Зокрема, якщо відповідні дані, що зберігалися у внутрішній базі даних Міністерства юстиції, не були «конфіденційними» у розумінні статті 6 Конвенції 108 й обмежувалися фактичною та об'єктивною інформацією, пов'язаною із судовим провадженням, учасником якого була особа, а їх обробка мала на меті забезпечення належного здійснення правосуддя і належного функціонування відповідних державних служб і супроводжувалася відповідними гарантіями (можливість забезпечення точності даних та обмежений термін їх зберігання), відсутність процедури передбачуваного видалення таких даних не була непропорційною («Л.Ф. проти Франції» (*L.F. v. France*) (ухв.), 2024, §§ 44-47).

303. У справі «Перуззо і Мартенс проти Німеччини» (*Peruzzo and Martens v. Germany*) (ухв.), 2013 (§ 46), що стосується зберігання персональних даних у справі після засудження за тяжкі злочини, пов'язані з незаконним обігом наркотиків, Суд визнав, що, хоча закон не встановлює максимальних строків зберігання профілів ДНК, Федеральне кримінальне відомство було зобов'язане перевіряти через регулярні проміжки часу, що не перевищують 10 років, чи зберігання даних все ще необхідне, беручи до уваги в кожному конкретному випадку мету зберігання даних, а також характер і тяжкість обставин справи.

304. У справі «Айсагуер проти Франції» (*Auçaguer v. France*), 2017 (§ 44), Суд встановив порушення статті 8, оскільки через передбачені тривалість і неможливість видалення чинні правила зберігання профілів ДНК у національній базі даних, проти яких заперечував заявник, відмовляючись від здачі зразків, не забезпечували суб'єкту даних достатнього захисту (*там само*, § 45). Суд наголосив, що засудженим особам, як і особам, які підозрювалися у вчиненні кримінального правопорушення, були звільнені або виправдані, повинна бути надана конкретна можливість подати запит на видалення збережених даних, щоб гарантувати, що період зберігання даних пропорційний характеру правопорушень і цілям обмежень (*там само*, § 45; «Б.Б. проти Франції» (*B.B. v. France*), 2009, § 68; «Брунет проти Франції» (*Brunet v. France*), 2014, §§ 41-43).

305. У зв'язку з можливістю видалення персональних даних, право в будь-який момент подати запит на видалення до суду може вступити в конфлікт з інтересами слідчих органів, які вимагають доступу до бази даних з якомога більшою кількістю посилань. Відповідно, оскільки інтереси, про які йдеться, суперечливі, хоча б частково, видалення забезпечує гарантію, яка є «теоретичною та ілюзорною», а не «практичною та ефективною» («М.К. проти Франції» (*M.K. v. France*), 2013, §§ 44-47).

306. У справі «Зегерштедт-Віберг та інші проти Швеції» (*Segerstedt-Wiberg and Others v. Sweden*), 2006 (§§ 73-92), зберігання у файлах служб державної безпеки дуже давніх персональних даних, що стосуються відвідування заявниками політичних зборів, того факту, що вони виступали за насильницький опір поліцейським перевіркам під час демонстрацій, а також їхнього членства в певній політичній партії, становило порушення статті 8. Суд постановив, що інтерес Держави у захисті національної безпеки та боротьбі з тероризмом, який виправдовує збір і зберігання інформації, про яку йдеться, повинен бути збалансований із серйозністю втручання у здійснення кожним із заявників свого права на повагу до приватного життя. З огляду на характер і вік інформації про заявників, причини її зберігання, хоча і є актуальними, через тридцять років не можуть вважатися достатніми (*там само*, § 90).

4. Право на особливі процесуальні гарантії та ефективні процесуальні норми для захисту своїх прав

307. Хоча стаття 8 не містить чітких процесуальних вимог, для ефективного здійснення прав, гарантованих цим положенням, важливо, щоб відповідний процес прийняття рішень був справедливим і таким, що забезпечує належну повагу до інтересів, які він захищає. Такий

процес може вимагати існування ефективних процесуальних норм, за допомогою яких заявник може відстоювати свої права за статтею 8 в умовах справедливості, в тому числі в питаннях доказування та доказів (*«I. проти Фінляндії» (I. v. Finland)*, 2008, § 44; *«Чиботару проти Молдови» (Ciubotaru v. Moldova)*, 2010, § 51). Факт встановлення вимоги, яка створює нездоланий бар'єр для особи, яка вимагає виправлення своїх персональних даних в офіційних державних реєстрах, може бути несумісним з позитивним зобов'язанням Держави гарантувати ефективне дотримання права на повагу до приватного життя (*там само*, §§ 51-59). У справі, що стосувалася розголошення ВІЛ-позитивного статусу заявниці, Суд, встановивши порушення статті 8, надав значення тому факту, що Держава поклала на заявницю надмірно важкий тягар доказування в рамках цивільного провадження, під час якого вона вимагала компенсації за поширення інформації про стан її здоров'я (*«I. проти Фінляндії» (I. v. Finland)*, 2008, § 44).

308. Обмеження, накладені законом на повноваження національних судів відшкодувати шкоду, заподіяну розголошенням у пресі конфіденційної інформації про стан здоров'я ідентифікованих осіб, і запобігати повторенню таких зловживань, могли перешкоджати ефективності будь-якого оскарження, таким чином, не забезпечуючи заявникам такого захисту їхнього приватного життя, на який вони могли б законно розраховувати. Так у справах *«Армонієне проти Литви» (Armonienė v. Lithuania)*, 2008 (§§ 47-48) і *«Бірюк проти Литви» (Biriuk v. Lithuania)*, 2008 (§§ 46-47), Суд встановив порушення статті 8, оскільки Закон про надання інформації громадськості, що діяв на момент розгляду справи, встановлював верхню межу відшкодування збитків, присуджених заявникам національними судами після розголошення їхнього ВІЛ-позитивного статусу в провідній національній щоденній газеті, без їхньої згоди та без розголошення їхніх особистостей.

309. Незабезпечення Державою на національному рівні незалежного розгляду обґрунтованості зберігання персональних даних, зібраних в рамках кримінального провадження або після кримінального провадження, в якому обвинуваченого було виправдано, звільнено або засуджено, є важливим аспектом, який необхідно враховувати при визначенні того, чи таке зберігання даних сумісне зі статтею 8 (*«С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom)* [ВП], 2008, §§ 119, 125). У справі, що стосувалася безстрокового зберігання зразків клітин, профілів ДНК і відбитків пальців двох осіб після того, як кримінальне провадження проти них завершилося виправдувальним вироком і звільненням відповідно, Суд визнав порушення статті 8, зазначивши, що у заявників було мало шансів домогтися видалення даних з національної бази даних або знищення зразків.

310. У справі *«Вісент Дель Кампо проти Іспанії» (Vicent Del Campo v. Spain)*, 2018 (§§ 39, 53), неможливість заявника, третьої сторони в судовому провадженні, звернутися до національного суду з заявою про утримання від повідомлення його особи або особистої інформації про нього до винесення рішення позбавила його ефективних процесуальних рамок для захисту власних прав.

311. Нездатність органів влади провести аналіз пропорційності конкуруючих інтересів, що стоять на кону, та врахувати права заявника на приватне життя і питання захисту даних суперечитиме вимогам статті 8 Конвенції (*«Лібшер проти Австрії» (Liebscher v. Austria)*, 2021, §§ 64-69).

312. У справі *«М.Д. та інші проти Іспанії» (M.D. and Others v. Spain)*, 2022 (§§ 65-72) що стосується витoku в пресу персональних даних заявників з бази даних поліції, до якої мали доступ лише органи влади, Суд постановив, що стосовно такого незаконного розголошення приватних даних, які зберігаються державними органами, позитивне зобов'язання за статтею 8 передбачає «зобов'язання провести ефективне розслідування» з метою встановлення обставин, за яких журналісти отримали доступ до даних, і, за необхідності, покарання осіб, відповідальних за допущені недоліки. Непроведення владою таких розслідувань становило

порушення статті 8. Аналогічно у справі *«Й.Г. проти Росії» (Y.G. v. Russia)*, 2022, (§§ 46-53), де заявник скаржився на те, що база даних, яка містила його персональні дані, включаючи інформацію про стан його здоров'я, була доступна для продажу на ринку, Суд постановив, що перед обличчям такого серйозного порушення права на приватність заявник, діючи самостійно, без допомоги Держави у вигляді офіційного розслідування, не мав ефективних засобів для встановлення осіб, які вчинили ці дії, а отже, подача скарги в порядку кримінального судочинства за цих обставин не була недоречним засобом захисту. Не провівши розслідування, органи влади порушили своє позитивне зобов'язання забезпечити належний захист його права на повагу до приватного життя.

313. Ефективність засобів правового захисту, доступних на національному рівні для осіб, які бажають отримати доступ до своїх персональних даних, вимагає, щоб заяви, подані суб'єктами даних, оброблялися протягом розумного строку. У справі *«Роше проти Сполученого Королівства» (Roche v. the United Kingdom)* [ВП], 2005 (§§ 166-167, 169), Суд визнав порушення статті 8 у зв'язку з необґрунтованим періодом очікування для заявника доступу до документів, що містять персональні дані, які дозволили б йому оцінити потенційні ризики для здоров'я, викликані участю у військових випробуваннях газів.

314. Суворі строки або процесуальні обмеження також потребують ретельної перевірки. У справі *«Молдован проти України» (Moldovan v. Ukraine)*, 2024, (§§ 52-53), заявник скаржився на те, що національні суди, які розглядали його позов про визнання біологічного батька, застосували старі правові норми, які робили доказ спільного проживання необхідним для визнання батьківства, незважаючи на наявність тесту ДНК. На думку Суду, наслідки такого підходу національних судів можна порівняти з наслідками негнучких строків або інших процесуальних обмежень. Суд дійшов висновку, що такий підхід у поєднанні з тим, що національні суди не розглянули надані їм докази ДНК з достатньою ретельністю, становив порушення їхніх позитивних зобов'язань за статтею 8 Конвенції.

315. Надмірне значення, яке національні органи влади надають вимозі конфіденційності даних про трафік інтернет-користувачів, за певних обставин може суперечити статті 8, якщо це перешкоджає ефективності кримінального розслідування, спрямованого на виявлення та покарання правопорушника (*«К.У. проти Фінляндії» (K.U. v. Finland)*, 2008, § 49). У справі *«К.У. проти Фінляндії» (K.U. v. Finland)*, 2008 (§§ 49-50), Суд встановив порушення статті 8 у зв'язку з відсутністю процесуальної бази, що дозволяє ідентифікувати та притягнути до відповідальності особу, яка опублікувала в інтернеті оголошення, що робить неповнолітню особу об'єктом домагань з боку педофілів, з тим, щоб жертва могла вимагати відшкодування матеріальної шкоди від цієї особи. Гарантії, якими користуються абоненти телекомунікацій та інтернет-послуг щодо поваги до їхньої приватності, іноді поступаються іншим законним інтересам, таким як запобігання заворушенням чи злочинам або захист прав і свобод інших осіб.

316. У сфері національної безпеки кожна особа, до якої застосовуються заходи з вищезазначених причин, повинна мати можливість домогтися перегляду оскаржуваного заходу незалежним і неупередженим органом, уповноваженим розглядати всі відповідні фактичні та юридичні питання і, за необхідності, карати за будь-які зловживання, вчинені органами влади. Перед таким органом зацікавлені особи повинні користуватися перевагами змагального процесу, що дозволяє їм представити свою точку зору і спростувати аргументи, висунуті владою. Так у справі *«Далеа проти Франції» (Dalea v. France)* (ухв.), 2010, Суд постановив, що тривала реєстрація персональних даних заявника в Шенгенській базі даних може вважатися «необхідною в демократичному суспільстві», оскільки він отримав користь від перегляду оскаржуваного заходу. Хоча заявник не мав можливості заперечити проти конкретної причини реєстрації його даних, він був ознайомлений з усіма іншими даними, що його стосуються, в Шенгенській базі даних.

317. Незалежний і неупереджений орган, до якого із заявою про перегляд оскаржуваного заходу повинна мати можливість звернутися будь-яка особа, до якої застосовано захід з міркувань національної безпеки, не обов'язково повинен мати статус судового органу. У справі *«Леандер проти Швеції» (Leander v. Sweden)*, 1987 (§ 59), що стосувалася використання секретної поліцейської картотеки для найму телі, Суд не встановив порушення статті 8 через існування гарантій, включаючи можливість парламенту і незалежних установ проводити перевірку операцій, що дозволяють відповідним національним органам збирати й зберігати в секретних файлах інформацію про осіб, а потім використовувати її (*там само*, § 65), попри те, що заявник не мав права на судовий засіб правового захисту (*там само*, §§ 62, 67). Щоб оцінити ефективність засобу правового захисту в органі, відповідальному на національному рівні за перегляд заходів з міркувань національної безпеки, необхідно враховувати процесуальні повноваження та гарантії, що застосовуються цим органом (*там само*, §§ 77, 80, 83-84). Ієрархічне оскарження до безпосереднього керівника органу, дії якого оскаржуються, не відповідає необхідним стандартам незалежності, необхідним для забезпечення достатнього захисту від зловживання владою (*«Роман Захаров проти Росії» (Roman Zakharov v. Russia)* [ВП], 2015, § 292).

318. У рамках заходів таємного спостереження перегляд і нагляд за заходами такого виду можуть здійснюватися на трьох етапах: під час отримання дозволу на проведення спостереження, під час його здійснення або після його завершення. Що стосується перших двох етапів, то сама природа і логіка таємного спостереження диктує, що не тільки саме спостереження, але й супутній перегляд повинні здійснюватися без відома особи. Отже, оскільки особа неминуче буде позбавлена можливості шукати ефективний засіб правового захисту за власним бажанням або брати безпосередню участь у будь-якій процедурі перегляду, важливо, щоб встановлені процедури самі по собі забезпечували адекватні й еквівалентні гарантії захисту її прав. У сфері, де зловживання потенційно настільки легкі в окремих випадках і можуть мати такі шкідливі наслідки для демократичного суспільства в цілому, в принципі бажано довірити наглядовий контроль судді, судовий контроль пропонує найкращі гарантії незалежності, неупередженості та належної процедури (*там само*, § 233; *«Класс та інші проти Німеччини» (Klass and Others v. Germany)*, 1978, §§ 55-56).

3191. Що стосується третього етапу, після припинення спостереження, то питання подальшого повідомлення про заходи спостереження нерозривно пов'язане з ефективністю засобів правового захисту в судах, а отже, з існуванням ефективних гарантій проти зловживання повноваженнями з моніторингу (*«Роман Захаров проти Росії» (Roman Zakharov v. Russia)* [ВП], 2015, § 234). В принципі, існує мало можливостей для звернення до суду зацікавленої особи, якщо тільки вона не була повідомлена про заходи, вжиті без її відома, і, таким чином, не може оскаржити їх законність ретроспективно (*«Класс та інші проти Німеччини» (Klass and Others v. Germany)*, 1978, §§ 57-59; *«Вебер і Саравія проти Німеччини» (Weber and Saravia v. Germany)* (ухв.), 2006, §§ 135-137), або якщо будь-яка особа, яка підозрює, що її комунікації перехоплюються або були перехоплені, може звернутися до суду, з тим, щоб юрисдикція суду не залежала від повідомлення суб'єкта перехоплення про те, що його комунікації були перехоплені (*«Кеннеді проти Сполученого Королівства» (Kennedy v. the United Kingdom)*, 2010, §§ 167, 169; *«Роман Захаров проти Росії» (Roman Zakharov v. Russia)* [ВП], 2015, § 234).

320. У справах *«Класс та інші проти Німеччини» (Klass and Others v. Germany)*, 1978 (§§ 57-59) і *«Вебер і Саравія проти Німеччини» (Weber and Saravia v. Germany)* (ухв.), 2006 (§§ 135-137), Суд постановив, що засоби правового захисту, доступні на національному рівні, були достатніми. Особи, чиї комунікації були предметом моніторингу, були повідомлені про це в найкоротший строк, не ставлячи під загрозу мету моніторингу. Засоби правового захисту також покривалися ефективними гарантіями, такими як той факт, що незалежний орган був уповноважений вирішувати, чи слід повідомляти особу, за якою ведеться спостереження, про захід. На підставі такого повідомлення особа мала різні варіанти судового захисту, наприклад, подати цивільний позов про відшкодування збитків або звернутися до Федерального

конституційного суду з проханням винести рішення про можливе порушення Основного закону (*«Класс та інші проти Німеччини» (Klass and Others v. Germany)*, 1978, §§ 57, 24).

321. Для систем, які не передбачають повідомлення зацікавленої особи про вжиті проти неї заходи, той факт, що зацікавлені особи вважають, що їхнє право на повагу до приватного життя було порушено заходом таємного моніторингу, можуть звернутися до незалежного й неупередженого органу, навіть якщо вони не були заздалегідь поінформовані про те, що їхні комунікації були перехоплені, був розглянутий Судом як важлива гарантія у справі, в якій він не знайшов порушення статті 8 (*«Кеннеді проти Сполученого Королівства» (Kennedy v. the United Kingdom)*, 2010, §§ 167, 169). І навпаки, якщо засоби правового захисту, доступні в рамках національної системи, відкриті виключно для осіб, які мають мінімум інформації про оскаржуваний захід, Суд постановив, що зацікавлені особи не мали ефективного засобу правового захисту проти заходів таємного моніторингу, що є порушенням статті 8 (*«Роман Захаров проти Росії» (Roman Zakharov v. Russia)* [ВП], 2015, §§ 293-298, 305).

III. Взаємодія з іншими положеннями Конвенції та Протоколами до неї

322. Окрім права на повагу до приватного і сімейного життя, житла і кореспонденції, гарантованого статтею 8 Конвенції, яка є основним джерелом захисту персональних даних у системі Конвенції, питання, пов'язані з цим захистом, можуть також виникати відповідно до інших положень Конвенції та Протоколів до неї. У таких випадках основне завдання Суду — зважити цей захист та узгодити його з іншими правами і законними інтересами. У деяких випадках питання захисту персональних даних дозволило Суду визначити обсяг іншого права, гарантованого Конвенцією та додатковими Протоколами до неї.

А. Захист даних і матеріальні права¹⁰

Стаття 9 Конвенції

«1. Кожен має право на свободу думки, совісті та релігії; це право включає свободу змінювати свою релігію або переконання, а також свободу сповідувати свою релігію або переконання під час богослужіння, навчання, виконання та дотримання релігійної практики і ритуальних обрядів як одноособово, так і спільно з іншими, як прилюдно, так і приватно.

2. Свобода сповідувати свою релігію або переконання підлягає лише таким обмеженням, що встановлені законом і є необхідними в демократичному суспільстві в інтересах громадської безпеки, для охорони публічного порядку, здоров'я чи моралі або для захисту прав і свобод інших осіб».

Стаття 10 Конвенції

«1. Кожен має право на свободу вираження поглядів. Це право включає свободу дотримуватися своїх поглядів, одержувати та передавати інформацію та ідеї без втручання органів державної влади та незалежно від кордонів. Ця стаття не перешкоджає державам вимагати ліцензування діяльності радіомовних, телевізійних або кінематографічних підприємств.

2. Здійснення цих свобод, оскільки воно пов'язане з обов'язками та відповідальністю, може підлягати таким формальностям, умовам, обмеженням або санкціям, що встановлені законом і є необхідними в демократичному суспільстві в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, для охорони здоров'я чи моралі, для захисту репутації чи прав інших осіб, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету і безсторонності суду».

Стаття 14 Конвенції

«Користування правами та свободами, визнаними в цій Конвенції, має бути забезпечене без дискримінації за будь-якою ознакою — статі, раси, кольору шкіри, мови, релігії, політичних чи інших переконань, національного чи соціального походження, належності до національних меншин, майнового стану, народження, або за іншою ознакою».

Стаття 1 Першого протоколу

«Кожна фізична або юридична особа має право мирно володіти своїм майном. Ніхто не може бути позбавлений своєї власності інакше як в інтересах суспільства та на умовах, передбачених законом і загальними принципами міжнародного права.

Проте попередні положення жодним чином не обмежують право держави вводити в дію такі закони, які вона вважає за необхідне, щоб здійснювати контроль за користуванням майном відповідно до загальних інтересів або для забезпечення сплати податків чи інших зборів або штрафів».

Стаття 2 Протоколу № 4

«1. Кожен, хто законно перебуває на території будь-якої держави, має право вільно пересуватися і вільно вибирати місце проживання в межах цієї території.

2. Кожен є вільним залишати будь-яку країну, включно зі своєю власною.

3. На здійснення цих прав не можуть бути встановлені жодні обмеження, крім тих, що передбачені законом і є необхідними в демократичному суспільстві в інтересах національної чи громадської безпеки, для підтримання публічного порядку, запобігання злочину, для захисту

¹⁰ Цей розділ слід читати у світлі та в поєднанні з [Посібником зі статті 9](#), [Посібником зі статті 10](#), [Посібником зі статті 14](#) і [статті 1 Протоколу № 12](#) та [Посібником зі статті 1 Першого протоколу](#).

здоров'я чи моралі або з метою захисту прав і свобод інших осіб.

4. Права, викладені в пункті 1, також можуть у певних місцевостях підлягати обмеженням, що встановлені згідно із законом і виправдані суспільними інтересами в демократичному суспільстві».

1. Захист даних і свобода думки, совісті та релігії (стаття 9 Конвенції)

323. У деяких справах, які також порушують питання захисту персональних даних, Суд встановив порушення статті 9, в той час як в інших справах порушення не встановив.

324. У справі *«Сінан Ішук проти Туреччини» (Sinan Işık v. Turkey)*, 2010 (§§ 37-53), Суд зіткнувся з питанням про зазначення — обов'язкове чи необов'язкове — віросповідання заявника в його посвідченні особи. На думку Суду, факт необхідності письмового звернення до органів влади з проханням про зміну віросповідання в актах цивільного стану й посвідченні особи, а також сам факт наявності посвідчення особи з незаповненою графою «віросповідання» зобов'язував особу проти її волі розголошувати інформацію, що стосується аспекту її релігії або найбільш особистих переконань. Суд визнав порушення статті 9, нагадавши, що свобода сповідувати релігію або переконання має і негативний аспект, а саме право особи не бути зобов'язаною розкривати свою релігію або діяти таким чином, щоб можна було зробити висновок про те, що вона має — або не має — такі переконання. Хоча графу про віросповідання можна було залишити незаповненою, сам факт її заповнення мав певний підтекст, оскільки це неминуче дозволило б розрізнити власників посвідчень особи, що містять відповідну інформацію, і тих, хто вирішив її не вказувати (*там само*, § 51).

325. У справі *«Александрідіс проти Греції» (Alexandridis v. Greece)*, 2008 (§ 41), вимога до адвоката повідомити суду, що він не є православним християнином, і що він хоче зробити урочисту заяву, а не скласти релігійну присягу, втрутилася в його права за статтею 9. Державні органи не мають права втручатися у сферу індивідуальної совісті та з'ясовувати релігійні переконання особи або зобов'язувати її розкривати свої переконання щодо духовних питань. Це тим більше стосується випадків, коли особа була зобов'язана вчинити такі дії з метою виконання певних обов'язків, зокрема, при прийнятті присяги (*там само*, § 38). У справі *«Дімітрас та інші проти Греції» (Dimitras and Others v. Greece)*, 2010 (§ 88), вимога до заявників розкрити свої релігійні переконання, щоб не складати релігійну присягу в ролі свідків у кримінальному провадженні, також була визнана такою, що порушує статтю 9. Суд вважав, що положення Кримінального процесуального кодексу, які передбачали, що з метою встановлення особи всі свідки повинні були, серед іншої інформації, повідомити про своє віросповідання перед тим, як давати свідчення, важко узгодити зі свободою віросповідання (*там само*, § 88).

326. У справі *«Моккуте проти Литви» (Mockutė v. Lithuania)*, 2018 (§ 129), Суд був готовий визнати, що потреби психіатричного лікування можуть зробити необхідним обговорення психіатром різних питань, включаючи релігію, з пацієнтом. Однак такі обговорення не повинні набувати форми втручання психіатрів у переконання пацієнта з метою їх «виправлення», якщо немає явного і неминучого ризику того, що такі переконання можуть проявитися в діях, небезпечних для пацієнта або інших осіб. Держава не може диктувати людині, у що вона вірить, або вживати примусових заходів, щоб змусити її змінити свої переконання, так само як і межі свободи розсуду Держави не можуть бути ширшими або вужчими в залежності від характеру релігійних переконань.

327. У справі *«Свідки Єгови проти Фінляндії» (Jehovah's Witnesses v. Finland)*, 2023 (§§ 80-99), Суд був покликаний вирішити, чи був досягнутий справедливий баланс між правом громади-заявника на свободу релігії та правом на приватне життя осіб (суб'єктів даних), яких члени громади-заявника відвідували в контексті своєї проповіді «від дверей до дверей». На

національному рівні компетентні органи встановили, що під час цієї діяльності вимагалася однозначна або явна згода суб'єктів даних, коли збиралися та оброблялися персональні та конфіденційні дані (їхні імена та адреси). Суд визнав, що застосування вимоги про згоду в контексті проповіді громади-заявника «від дверей до дверей» — релігійної діяльності, спрямованої на сповідування або поширення віри — становило втручання в права цієї громади відповідно до статті 9 (§ 81). Водночас Суд постановив, що оскаржуване втручання було «передбачене законом», зокрема, з огляду на те, що Вищий адміністративний суд витлумачив відповідний національний нормативно-правовий акт, який слугував підставою для оскаржуваних заходів, і який сам ґрунтувався на відповідній директиві ЄС, згідно з тлумаченням, наданим Судом справедливості ЄС (§§ 84-88). Оскаржуваний захід також переслідував законну мету захисту «прав і свобод інших осіб» (§ 89) і був «необхідним у демократичному суспільстві». В останньому відношенні Суд зазначив, що, хоча вимога згоди була належною і необхідною гарантією для запобігання будь-якій передачі або розголошенню персональних і конфіденційних даних в контексті проповіді «від дверей до дверей» громади-заявника, заявник не зміг продемонструвати, яким чином ця вимога перешкоджала б суті його права на свободу віросповідання (§ 95). Більше того, відповідна вимога була застосовна до всіх релігійних громад і релігійної діяльності (§ 96), а на громаду-заявника не було накладено жодного покарання, незважаючи на таку вимогу (§ 97).

2. Захист даних і свобода вираження поглядів (стаття 10 Конвенції)¹¹

328. Як правило, у справах, в яких Суду доводилося зважувати й узгоджувати право на захист персональних даних, гарантоване статтею 8, та право на свободу вираження поглядів, гарантоване статтею 10, він дійшов висновку, що результат, в принципі, не повинен відрізнятися залежно від того, чи була заява подана за статтею 8, чи за статтею 10. На думку Суду, ці два права заслуговують на однакову повагу (*«Сатакуннан Марккінапорсси Ой та Сатамедіа Ой проти Фінляндії» (Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland)* [ВП], 2017, § 163; *«Альфа Дорифорікі Тілеорасі Анонімі Етайріа проти Греції» (Alpha Doryforiki Tileorasi Anonymi Etairia v. Greece)*, 2018, § 46).

329. Відмова органів влади надати неурядовим організаціям доступ до певної інформації, що містить персональні дані, якими володіє Держава, була визнана порушенням статті 10 у таких справах:

- *«Центр демократії та верховенства права проти України» (Centre for Democracy and the Rule of Law v. Ukraine)*, 2020 (§§ 120-121), щодо відмови Центральної виборчої комісії надати громадській організації копії автобіографій лідерів політичних партій, які балотувалися на парламентських виборах, на підставі того, що запитувана інформація конфіденційна і може бути розкрита в повному обсязі лише за згодою відповідних осіб;
- *«Мадяр Гельсінкі Бізотцаг проти Угорщини» (Magyar Helsinki Bizottság v. Hungary)* [ВП], 2016 (§§ 195-197, 200), де влада відмовилася надати неурядовій організації, яка проводила опитування, імена адвокатів, призначених *ex officio*, та кількість їхніх відповідних призначень;
- *«Молодіжна ініціатива за права людини проти Сербії» (Youth Initiative for Human Rights v. Serbia)*, 2013 (§§ 24-26), щодо відмови спецслужби надати інформацію НУО, попри те, що їй було наказано це зробити.

¹¹ Цей розділ слід читати у світлі та в поєднанні з [Посібником зі статті 10](#) (див., зокрема, пп. 26-47; 58-60 і 62-65).

330. Що стосується розголошення персональних даних у друкованих або аудіовізуальних засобах масової інформації, Суд встановив порушення статті 10 у низці справ, серед яких:

- *«Н.Ш. проти Хорватії» (N.Š. v. Croatia)*, 2020 (§§ 92-117), де заявницю було засуджено за розголошення на телебаченні нібито конфіденційної інформації, яку вона отримала під час адміністративного провадження щодо опіки над дитиною. Суд постановив, що, зважаючи на вразливість дітей, захист їхніх персональних даних необхідний (*там само*, § 99). Однак надмірно формалістичний підхід, застосований національними судами, який не брав до уваги передумови розголошення інформації і, зокрема, той факт, що інформація вже була в суспільному надбанні, був несумісний зі статтею 10 (*там само*, §§ 115-116);
- *«Гірлеану проти Румунії» (Gîrleanu v. Romania)*, 2018 (§§ 68-100), щодо наказу про сплату заявником адміністративного штрафу за розголошення конфіденційної військової інформації в рамках журналістського розслідування;
- *«Кудерк і Хашетте Філіпаччі Ассосіє проти Франції» (Couderc and Hachette Filipacchi Associés v. France)* [ВП], 2015 (§§ 94-153), щодо судового рішення проти директора видавництва та видавця щотижневого журналу за публікацію статті та фотографій, які розкривали існування таємної дитини монарха;
- *«Аксель Шпрінгер АГ проти Німеччини» (Axel Springer AG v. Germany)* [ВП], 2012 (§§ 75-111), щодо заборони повідомляти про арешт і засудження відомого актора;
- *«Дюпюї та інші проти Франції» (Dupuis and Others v. France)*, 2007 (§§ 30-32, 39-49), щодо засудження журналістів за використання та відтворення у своїй книжці інформації з матеріалів судового розслідування, включаючи персональні дані обвинувачених.

331. І навпаки, Суд не вбачив порушення статті 10 або визнав неприйнятними заяви, зокрема, у кількох справах:

- *«Гурбейн проти Бельгії» (Hurbain v. Belgium)* [ВП], 2023 (§§ 167-257), стосовно цивільного рішення, яке зобов'язувало видавця газети анонімізувати електронну онлайн-версію статті, в якій згадувалося повне ім'я водія, відповідального за смертельну аварію, що сталася багато років тому;
- *«Бьянкарді проти Італії» (Biancardi v. Italy)*, 2021 (§§ 67-71) стосовно цивільного рішення проти редактора газети за те, що він не деіндексував конфіденційну інформацію, опубліковану в інтернеті щодо кримінального провадження проти приватної особи, та рішення журналіста залишити інформацію легкодоступною, незважаючи на заперечення особи;
- *«Сатакуннан Марккінапоррсі Ой та Сатамедіа Ой проти Фінляндії» (Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland)* [ВП], 2017 (§§ 139-199), щодо судового рішення про заборону масової публікації даних про особисте оподаткування;
- *«Бедат проти Швейцарії» (Bédat v. Switzerland)* [ВП], 2016 (§§ 44-82), про засудження журналіста за публікацію інформації, що становить таємницю кримінального розслідування;
- *Медієнгруппе Остеррайх ГмбГ проти Австрії (Mediengruppe Österreich GmbH v. Austria)*, 2022 (§§ 44-73), щодо судового наказу щоденній газеті не публікувати фотографію з підписом «засуджений неонацист» стосовно особи, яка була опосередковано пов'язана з кампанією кандидата на політичну посаду, напередодні президентських виборів, а власне публікація була зроблена більше ніж через двадцять років після засудження;
- *«Гаф'юк проти Румунії» (Gafiuc v. Romania)*, 2020 (§§ 85-90), щодо відкриття акредитації журналіста на обшук в архівах таємної поліції Секурітате після

розголошення в кількох написаних ним статтях персональних даних у «необробленому» вигляді щодо різних відомих спортивних діячів, без оцінки релевантності даних у світлі заявленого предмета його дослідження, а саме спорту в Румунії за часів комуністичного режиму;

- *«Гісбер та інші проти Франції» (Giesbert and Others v. France)*, 2017 (§§ 77-103), щодо висновків судів проти газети за публікацію документів з низки кримінальних проваджень до того, як вони мали бути зачитані на публічному слуханні;
- *«Ферлагсгруппе Дрьомер Кнауер ГмбХ унд Ко. КГ проти Німеччини» (Verlagsgruppe Droemer Knaur GmbH & Co. KG v. Germany)*, 2017 (§§ 36-62), щодо зобов'язання видавничої компанії відшкодувати збитки за непроведення ретельного дослідження та за серйозне втручання в особисті права особи;
- *«Кур'єр Цайтунгсферлаг унд Друкерай ГмбХ проти Австрії» (Kurier Zeitungsverlag und Druckerei GmbH v. Austria)*, 2012 (§§ 47-56), щодо вимоги виплатити компенсацію дитині, яка стала жертвою сексуального насильства і особистість якої була розголошена в статті в пресі. З огляду на вразливість жертв злочинів, їхня особистість заслуговує на особливий захист;
- *«Ем-Джі-Ен Лімітед проти Сполученого Королівства» (MGN Limited v. the United Kingdom)*, 2011 (§ 152), у якій Суд був переконаний, серед інших міркувань, тим фактом, що розголошення в пресі подробиць лікування знаменитості від наркозалежності було шкідливим і могло спричинити значний регрес у її одужанні;
- *«Едісьон Плон проти Франції» (Editions Plon v. France)*, 2004 (§§ 22-55), щодо остаточного призупинення розповсюдження книжки, яка містила інформацію, що стосується померлого глави Держави і становить лікарську таємницю;
- *«Мітов та інші проти Болгарії» (Mitov and Others v. Bulgaria)* (ухв.), 2023 (§§ 30-41), щодо правил анонімізації, встановлених Головою Вищого адміністративного суду, і законодавства, що вводить правило відкладеної публікації деяких кримінальних рішень, після чого заявники, журналісти-розслідувачі, не змогли отримати вільний доступ в інтернеті до всіх відсканованих матеріалів справ, наявних в базі даних цього суду;
- *«Рамадан проти Франції» (Ramadan v. France)* (ухв.), 2024 (§§ 28-46), де заявник, обвинувачений у сексуальному насильстві в рамках кримінального провадження, поширив у своїй книжці та двох інших засобах масової інформації інформацію про особу передбачуваної жертви цього насильства без згоди останньої, яка раніше була розкрита третіми особами у ЗМІ.

332. Що стосується розповсюдження особистих зображень у пресі або засобах масової інформації, а також судових рішень про заборону розповсюдження таких персональних даних, Суд встановив порушення статті 10 у кількох справах, серед яких: *«Пінто Коельйо проти Португалії» (№ 2) (Pinto Coelho v. Portugal (no. 2))*, 2016 (§§ 31-56), щодо засудження журналіста за трансляцію запису судового засідання без дозволу; *«Галдіманн та інші проти Швейцарії» (Haldimann and Others v. Switzerland)*, 2015 (§§ 63-68), в якому чотири журналісти, переслідуючи мету в суспільних інтересах, були засуджені за запис і трансляцію інтерв'ю з приватним страховим брокером за допомогою прихованої камери; *«Кроне Ферлаг ГмбХ унд Ко. КГ проти Австрії» (Krone Verlag GmbH & Co. KG v. Austria)*, 2002, (§§ 21-39), щодо судової заборони утримуватися від публікації фотографії політика; і *«Ньюз Ферлагс ГмбХ і Ко. КГ проти Австрії» (News Verlags GmbH & Co. KG v. Austria)*, 2000 (§§ 37-60), щодо заборони газеті публікувати фотографію підозрюваного у кримінальному провадженні.

333. Однак, розповсюдження таких зображень або розпорядження утриматися від їх розповсюдження було визнано таким, що не порушує статтю 10 у таких справах: *«Друкарня та видавництво проти Франції» (Société de Conception de Presse and d'Édition v. France)*, 2016

(§§ 32-54), щодо судового рішення про затушовування фотографії в журналі, який вже був у продажу, особи, яка перебувала в полоні та піддавалася тортурам; *«Аксель Шпрінгер СЕ та РТЛ Телевізійон ГмБХ проти Німеччини» (Axel Springer SE and RTL Television GmbH v. Germany)*, 2017 (§§ 43-59), щодо рішення про заборону публікації зображень, які б дозволили ідентифікувати особу, яку судять за вбивство; *«Егеланд і Гансайд проти Норвегії» (Egeland and Hanseid v. Norway)*, 2009 (§§ 56-65), щодо засудження головних редакторів двох газет за публікацію фотографій особи, яку збиралися доставити до в'язниці для початку відбування тривалого покарання. Див. також п. 17 і п. 65 вище щодо справи *«Вучина проти Хорватії» (Vučina v. Croatia)* (ухв.) 2019.

334. У справі *«Альфа Дорифорікі Тілеорасі Анонімі Етайріа проти Греції» (Alpha Doryforiki Tileorasi Anonymi Etairia v. Greece)*, 2018 (§§ 59-69, 77-78), поширення в журналістських цілях кількох відео, знятих прихованою камерою в рамках прихованого спостереження за публічною особою, призвело до одного висновку про порушення, а в іншому — про відсутність порушення статті 10, залежно від того, чи було зроблено запис у публічному чи приватному просторі.

335. Що стосується розміщення в інтернеті приватними особами зображень інших осіб, знятих таємно, без згоди суб'єкта даних, Суд встановив у справі *«Хадіджа Ісмаїлова проти Азербайджану» (Khadija Ismayilova v. Azerbaijan)*, 2019 (§§ 158-166), що Держава-відповідач не змогла захистити заявницю, журналістку, яка була знята невідомими особами за допомогою прихованих камер, встановлених в її квартирі. Необґрунтоване публічне розголошення владою в пресрелізі, який мав на меті надати інформацію про хід кримінального розслідування, особистих даних, як-от ім'я заявниці та адреси її друзів і колег, ще більше ускладнило ситуацію, що суперечить духу середовища, яке захищає журналістику (*там само*, § 165).

336. У справі про захист свободи вираження поглядів викривача й розголошення конфіденційної інформації, що впливає на державну безпеку, Суд встановив порушення статті 10 у зв'язку із засудженням заявника за оприлюднення низки порушень у збиранні персональних даних спецслужбою, які він виявив у ході своєї професійної діяльності (*«Букур і Тома проти Румунії» (Bucur and Toma v. Romania)*, 2013, §§ 95-120). В іншій справі викривача, заступника головного лікаря державної лікарні було звільнено після того, як він повідомив про свої підозри, які згодом виявилися безпідставними, щодо активної евтаназії з боку свого керівника. Суд не встановив порушення статті 10: заявник ґрунтував свої підозри на інформації, наявній в електронних медичних картах (які, як йому було відомо, не містили всієї інформації про стан здоров'я пацієнтів), а не в паперових файлах (які містили всю інформацію). Таким чином, хоча він діяв добросовісно, він не зміг ретельно перевірити, чи була розкрита інформація точною та достовірною (*«Гоулік проти Ліхтенштейну» (Gawlik v. Liechtenstein)*, 2021, §§ 74-78).

337. Питання захисту персональних даних журналістів або даних, якими вони володіють і які можуть призвести до ідентифікації їхніх джерел, розглядалося Судом, зокрема, у низці справ:

- *«Седлецька проти України» (Sedletska v. Ukraine)*, 2021 (§§ 59-60 і 64-73), де судовий дозвіл, наданий слідчим органам на доступ і збір даних про комунікацію журналістки — дати, час і місцезнаходження її мобільного телефону поблизу зазначених вулиць і місць протягом шістнадцяти місяців — які зберігалися її оператором мобільного зв'язку, було визнано таким, що порушує статтю 10, оскільки він не був обґрунтований «переважною вимогою в інтересах суспільства» та не мав процесуальних гарантій;
- *«Джекер проти Швейцарії» (Jecker v. Switzerland)*, 2020 (§§ 37-43), де наказ журналісту розкрити особу одного зі своїх джерел, щоб допомогти органам прокуратури ідентифікувати наркоторговця, був визнаний Судом таким, що

суперечить статті 10 за відсутності будь-якого балансу конкретних інтересів, які були поставлені на карту;

- *«Телеграф Медіа Недерланд Ланделійке Медіа Б.В. та інші проти Нідерландів» (Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands)*, 2012 (§ 102), в якій розміщення журналістів під наглядом без попереднього розгляду незалежним органом, а також наказ видати документи, які можуть привести до ідентифікації їхніх джерел, були визнані такими, що порушують статті 8 і 10 разом узяті. Перегляд *post factum* не був би достатнім, оскільки конфіденційність журналістських джерел не могла бути відновлена після їх знищення (*там само*, §§ 100-101);
- *«Файненшіал Таймз Лтд та інші проти Сполученого Королівства» (Financial Times Ltd and Others v. the United Kingdom)*, 2009 (§ 63), в якій Суд вказав, що поведінка джерела ніколи не може бути вирішальною при визначенні того, чи слід видавати рішення про розголошення інформації, а лише одним, хоча й важливим, фактором, який слід брати до уваги при здійсненні необхідного балансу;
- *«Вебер і Саравія проти Німеччини» (Weber and Saravia v. Germany)* (ухв.), 2006 (§§ 143-153), де Суд визнав явно необґрунтованою скаргу на порушення свободи вираження поглядів, що впливало з положень закону, який дозволяв стратегічний моніторинг телекомунікацій і унеможлиблював для журналістів гарантії збереження конфіденційності інформації, яку вони отримували в ході своєї роботи;
- *«Ернст та інші проти Бельгії» (Ernst and Others v. Belgium)*, 2003 (§§ 94-105), де широкомасштабні обшуки й вилучення в офісі журналістів, спрямовані на виявлення їхніх джерел, були визнані порушенням статті 10. (Див. також справи *«Роємен і Шміт проти Люксембургу» (Roemen and Schmit v. Luxembourg)*, 2003, §§ 47-60, щодо обшуків у будинку журналіста з метою виявлення його джерел; *«Тіллак проти Бельгії» (Tillack v. Belgium)*, 2007, §§ 56-68, щодо обшуку та вилучення, проведених вдома та в офісі журналіста, підозрюваного у підкупі європейського державного службовця з метою отримання конфіденційної інформації про розслідування, яке проводилися в європейських установах, з метою встановлення джерела розголошення; *«Саномат Уйтгеверс Б.В. проти Нідерландів» (Sanoma Uitgevers B.V. v. the Netherlands)* [ВП], 2010, §§ 64-100, щодо вилучення поліцією документів, які дозволили б встановити джерела журналістської інформації; *«Нагла проти Латвії» (Nagla v. Latvia)*, 2013, §§ 78-102, щодо термінових обшуків у журналістки, які включали вилучення носіїв інформації, котрі містили її джерела інформації; *«Сервуло енд Ассоциадос — Сосьєдад де Адвогадос, РЛ та інші проти Португалії» (Sérvulo & Associados - Sociedade de Advogados, RL and Others v. Portugal)*, 2015, §§ 101-120, щодо масового вилучення комп'ютерних файлів та електронної пошти в офісі юридичної фірми; та *«Гьормюш та інші проти Туреччини» (Görmüş and Others v. Turkey)*, 2016, §§ 32-77, щодо захисту джерел журналіста, державних службовців, які висвітлили незадовільну практику на своєму робочому місці, в контексті конфіденційності військових питань); а також
- *«Біг Бразер Вотч та інші проти Сполученого Королівства» (Big Brother Watch and Others v. the United Kingdom)* [ВП], 2021, §§ 442-458, щодо масового перехоплення комунікацій, що дозволило спецслужбам ненавмисно отримати доступ до великого обсягу конфіденційних журналістських матеріалів як «побічного результату» масової операції. Суд встановив порушення статті 10 Конвенції.

3. Захист даних і заборона дискримінації (стаття 14 Конвенції)

338. У справі *«Шеффілд і Горшем проти Сполученого Королівства» (Sheffield and Horsham v. the United Kingdom)* [ВП], 1998 (§§ 51-61, 76-77), яка стосувалася питання, чи зобов'язана

Держава-відповідач юридично визнати нову гендерну ідентичність двох заявників, які пройшли операцію зі зміни статі на жіночу, Суд постановив, що не було порушення статті 8, взятої окремо або в поєднанні зі статтею 14. На думку Суду, ситуації, в яких заявники могли бути змушені розголошувати свої персональні дані, не траплялися з такою частотою, щоб можна було сказати, що це непропорційно порушує їхнє право на повагу до приватного життя. Суд також зазначив, що Держава-відповідач намагалася певною мірою звести до мінімуму нав'язливі запити щодо гендерного статусу трансгендерних осіб, дозволивши їм отримувати водійські права, паспорти та інші види офіційних документів на нове ім'я та стать, а також офіційно не рекомендувала використовувати свідоцтва про народження як засіб ідентифікації (*там само*, § 59; *«Коссі проти Сполученого Королівства» (Cossey v. the United Kingdom)*, 1990, §§ 36-42).

339. У кількох справах, в яких Суд розглядав питання, тісно пов'язані із захистом персональних даних за статтею 8 або статтею 9, Суд не виявив окремого питання за статтею 14 (*«Сінан Ішик проти Туреччини» (Sinan Işık v. Turkey)*, 2010, § 57, щодо зазначення — обов'язкового чи необов'язкового — віросповідання заявника в посвідченні особи; *«Авілкіна та інші проти Росії» (Avilkina and Others v. Russia)*, 2013, § 61, щодо розголошення медичної документації кількох Свідків Єгови, які відмовилися від переливання крові; *«Крістін Гудвін проти Сполученого Королівства» (Christine Goodwin v. the United Kingdom)* [ВП], 2002, §§ 92-93 і 108, та *«Ай. проти Сполученого Королівства» (I. v. The United Kingdom)* [ВП], 2006, §§ 72-73, 88, щодо юридичного визнання зміни статі особи).

4. Захист даних і право на мирне володіння майном (Стаття 1 Першого протоколу)

340. Суд розглядав питання захисту персональних даних і права на мирне володіння майном у контексті обшуків і вилучень.

341. У справі *«Смірнов проти Росії» (Smirnov v. Russia)*, 2007 (§§ 53-59), Суд постановив, що національні органи влади не встановили «справедливого балансу» між вимогами загального інтересу суспільства та вимогами захисту права заявника на мирне володіння своїм майном. Таким чином, мало місце порушення статті 1 Першого протоколу у зв'язку з обшуком, проведеним у будинку заявника, адвоката, з подальшим вилученням, серед інших речей, блоку його комп'ютера, що містив жорсткі диски з його особистими даними. Хоча збереження речових доказів може бути необхідним в інтересах належного здійснення правосуддя, сам комп'ютер не був об'єктом, знаряддям або продуктом будь-якого кримінального правопорушення. Оскільки інформація, що зберігалася на жорсткому диску, яка була потенційно цінною та корисною для розслідування, була вивчена слідчим, роздрукована й долучена до матеріалів справи, не було жодних підстав для подальшого утримання центрального блоку. Ба більше, комп'ютер був робочим інструментом заявника, а також використовувався для зберігання даних його клієнтів.

342. У справі *«Круглов та інші проти Росії» (Kruglov and Others v. Russia)*, 2020 (§§ 145-146), поліцейські обшуки будинків та офісів заявників, адвокатів за професією, та їхніх клієнтів, а також вилучення комп'ютерів і жорстких дисків, що містили особисту інформацію та документи, що становлять професійну таємницю, які самі по собі не були об'єктом, знаряддям або результатом будь-якого кримінального правопорушення, були визнані такими, що порушують статтю 1 Першого протоколу.

343. У справі *«Пендов проти Болгарії» (Pendov v. Bulgaria)*, 2020 (§§ 43-51), Суд постановив, що невинувато тривале утримання комп'ютерного сервера заявника в контексті кримінального провадження проти третіх осіб становило порушення статті 1 Першого протоколу. Той факт, що сервер жодного разу не досліджувався для цілей кримінального розслідування, яке стосувалося виключно третіх осіб; можливість копіювання необхідної інформації; важливість

сервера для професійної діяльності заявника; часткова бездіяльність прокуратури — все це означало, що утримання сервера заявника протягом семи з половиною місяців було непропорційним (*там само*, § 51).

5. Захист даних і свобода пересування (стаття 2 Протоколу № 4)

344. Суд розглянув низку справ, в яких свобода пересування особи була обмежена через персональні дані, що зберігалися органами влади. Суд розглядав справи за статтею 8.

345. Так у справі *«Далеа проти Франції» (Dalea v. France)* (ухв.), 2010, зберігання поліцією в Шенгенській інформаційній системі даних, достовірність яких оскаржував заявник, перешкоджало його вільному пересуванню в межах Шенгенської зони. Заявник не міг отримати доступ до персональних даних, що містилися в базі даних, і виправити їх. Суд повторив, що стаття 8 як така не гарантує право іноземця на в'їзд або проживання в певній країні. У цій справі втручання в приватне життя заявника у зв'язку з його включенням французькими органами влади до Шенгенської бази даних відповідало закону й переслідувало законну мету захисту національної безпеки. Це було пропорційно переслідуваній меті й було необхідним у демократичному суспільстві. Заявник не посилався на статтю 2 Протоколу № 4.

346. У справі *«Шимоволос проти Росії» (Shimovolos v. Russia)*, 2011 (§§ 64-71), інформація про поїздки заявника поїздом і літаком була внесена до «баз даних спостереження» через його членство в правозахисній організації. Щоразу, коли особа, чие ім'я було в цьому списку, купувала квиток на поїзд або літак, Управління транспорту внутрішніх справ отримувало автоматичне сповіщення. В результаті, коли заявник сів у потяг, щоб поїхати до Самари у зв'язку з самітом ЄС — Росія та взяти участь у мітингу протесту в цьому місті, троє співробітників міліції перевірили його документи і запитали про мету його поїздки. Суд встановив, що, збираючи та зберігаючи дані про пересування заявника відповідно до міністерського наказу, який не був опублікований і не був доступний для громадськості, органи влади втрутилися в його приватне життя у спосіб, несумісний з правами, гарантованими статтею 8. Суд також встановив, що окремого питання за статтею 2 Протоколу № 4 не виникло (*там само*, § 73).

347. У справі *«Беггал проти Сполученого Королівства» (Beghal v. the United Kingdom)*, 2019 (§§ 89-109), в якій порушувалося питання важливості моніторингу міжнародних пересувань терористів, Суд, перш ніж визнати порушення статті 8, постановив, що повноваження, надані антитерористичним законодавством поліції, імміграційним службам і призначеним митникам зупиняти, обшукувати й допитувати пасажирів у портах, аеропортах і міжнародних залізничних терміналах, не були достатньо обмежені, а також не існувало належних правових гарантій проти зловживань. Зокрема, законодавство не вимагало попереднього дозволу, а повноваження зупиняти і допитувати могли бути використані навіть за відсутності підозр у причетності до тероризму.

348. У справі *«Віллемс проти Нідерландів» (Willems v. the Netherlands)* (ухв.), 2021, щодо обов'язку відповідно до Закону про паспорти здавати відбитки пальців при подачі заяви на отримання паспорта, а також зберігання таких відбитків на електронному чіпі після включення у внутрішнє законодавство Регламенту ЄС про стандарти щодо елементів безпеки та біометричних даних у паспортах та проїзних документах, що видаються Державами-членами, скарги були відхилені як явно необґрунтовані через «презумпцію еквівалентного захисту» у праві ЄС (*там само*, §§ 26-36).

В. Захист даних і процесуальні права

Стаття 6 Конвенції

«1. Кожен має право на справедливий і публічний розгляд його справи упродовж розумного строку незалежним і безстороннім судом, встановленим законом, який вирішить спір щодо його прав та обов'язків цивільного характеру або встановить обґрунтованість будь-якого висунутого проти нього кримінального обвинувачення. Судове рішення проголошується публічно, але преса і публіка можуть бути не допущені в зал засідань протягом усього судового розгляду або його частини в інтересах моралі, громадського порядку чи національної безпеки в демократичному суспільстві, якщо того вимагають інтереси неповнолітніх або захист приватного життя сторін, або — тією мірою, що визнана судом суворо необхідною, — коли за особливих обставин публічність розгляду може зашкодити інтересам правосуддя.

2. Кожен, кого обвинувачено у вчиненні кримінального правопорушення, вважається невинуватим доти, доки його вину не буде доведено в законному порядку.

3. Кожний обвинувачений у вчиненні кримінального правопорушення має щонайменше такі права:

(а) бути негайно і детально поінформованим зрозумілою для нього мовою про характер і причини обвинувачення, висунутого проти нього;

(б) мати час і можливість, необхідні для підготовки свого захисту;

(с) захищати себе особисто чи використовувати юридичну допомогу захисника, вибраного на власний розсуд, або — за браком достатніх коштів для оплати юридичної допомоги захисника — одержувати таку допомогу безоплатно, коли цього вимагають інтереси правосуддя;

(д) допитувати свідків обвинувачення або вимагати, щоб їх допитали, а також вимагати виклику й допиту свідків захисту на тих самих умовах, що й свідків обвинувачення;

(е) якщо він не розуміє мови, яка використовується в суді, або не розмовляє нею, — одержувати безоплатну допомогу перекладача.

Стаття 13 Конвенції

«Кожен, чиї права та свободи, визнані в цій Конвенції, було порушено, має право на ефективний засіб правового захисту в національному органі, навіть якщо таке порушення було вчинене особами, які здійснювали свої офіційні повноваження».

1. Право на справедливий суд (стаття 6 Конвенції)¹²

349. Будь-яка особа, чиї персональні дані піддаються автоматизованій обробці в контексті судового провадження, повинна користуватися гарантіями статті 6, незалежно від її статусу в провадженні (заявник, відповідач, свідок, обвинувачений або третя особа).

а. Загальні гарантії (пункт 1 статті 6 Конвенції)

350. У кількох справах Суд оцінював з точки зору пункту 1 статті 6 необхідність захисту персональних даних сторін або третіх осіб у контексті різних загальних гарантій, покликаних забезпечити справедливість судового розгляду. До таких гарантій належать, зокрема, рівність сторін і право на змагальність, право на публічний розгляд справи та публічне оголошення

¹² Цей розділ слід читати з огляду на та в поєднанні з Посібниками зі статті 6 Конвенції у її [цивільному аспекті](#) (стор. 60-91) та [кримінально-правовому аспекті](#) (стор. 32-100).

судового рішення, збір доказів, розумну тривалість провадження та вимога щодо обґрунтування судових рішень.

i. Рівність сторін і дотримання принципу змагальності у провадженнях, що стосуються конфіденційної або секретної інформації

351. У справі *«Eternit проти Франції» (Eternit v. France)* (ухв.), 2012 (§§ 35-42), роботодавець порушив провадження, оскаржуючи рішення бюро медичного страхування про визнання професійного характеру хвороби одного з його працівників. Суд не визнав провадження таким, що порушує пункт 1 статті 6, незважаючи на те, що роботодавцю не було надано копію зауважень, зроблених медичним консультантом страхової компанії. Ненадання роботодавцю медичної картки працівника було виправдано необхідністю захисту конфіденційності його медичних даних, яку суди повинні були поставити в один ряд з правом компанії-заявника на змагальний процес, щоб гарантувати, що сама суть цього права не була порушена в жодному з випадків. Необхідний баланс був досягнутий, коли роботодавець міг звернутися до суду з проханням призначити незалежного медичного експерта для вивчення медичної документації працівника і складання звіту — з дотриманням конфіденційності медичної документації — аби суд і сторони могли ним керуватися (*там само.*, § 37). Той факт, що експертний звіт не призначався щоразу, коли роботодавець вимагав його, а лише тоді, коли суд вважав, що він не мав достатньої інформації, не суперечив вимогам справедливого судового розгляду згідно з пунктом 1 статті 6 Конвенції (*там само.*, §§ 35-39).

352. У справі *«Кеннеді проти Сполученого Королівства» (Kennedy v. the United Kingdom)*, 2010 (§§ 184-191), обмеження принципу рівності сторін і принципу змагальності у провадженнях у Трибуналі з питань слідчих повноважень, незалежному органі, створеному для розгляду скарг осіб, які підозрюють, що їхні повідомлення були незаконно перехоплені органами влади, не були визнані несумісними з пунктом 1 статті 6. Інтереси національної безпеки та необхідність зберігати в таємниці певні методи кримінального розслідування повинні були бути зіставлені з правом на змагальний судовий розгляд. На думку Суду, існувала необхідність зберігати в таємниці конфіденційні та секретні матеріали, розголошення яких завадило б досягненню переслідуваної мети (*там само.*, §§ 186-187).

353. У більш загальному плані Суд підкреслив, що право на змагальний судовий розгляд означає, що в кримінальній справі як обвинувачення, так і захист повинні мати можливість ознайомитися з поданими зауваженнями та доказами, наданими іншою стороною, включаючи, наприклад, відеозапис обвинуваченої, використаний як доказ проти неї, і прокоментувати їх (*«Муртазалієва проти Росії» (Murtazaliyeva v. Russia)*, [ВП], 2018, §§ 90-95).

ii. Вмотивованість судових рішень і захист даних

354. У справі *«Суріков проти України» (Surikov v. Ukraine)*, 2017 (§§ 102-103), Суд встановив порушення пункту 1 статті 6 на тій підставі, що національні суди не розглянули низку доречних і важливих питань, які були порушені. Заявник стверджував, що його роботодавець свавільно збирав і зберігав конфіденційну та застарілу інформацію про його психічне здоров'я, використовував цю інформацію при розгляді його заяви про підвищення, а також незаконно розголошував її своїм колегам і суду. Суд підтвердив, що стаття 6 зобов'язує суди обґрунтовувати свої рішення. Хоча це зобов'язання не можна розуміти як таке, що вимагає детальної відповіді на кожен аргумент, принцип справедливості буде порушений, якщо національні суди проігнорують конкретне, доречне та важливе зауваження, зроблене заявником (*там само.*, § 101 та наведена в ньому судова практика).

355. У справі *«Самойлова проти Росії» (Samoylova v. Russia)*, 2021 (§§ 50-52), яка стосувалася трансляції телевізійного репортажу з точною адресою заявниці, її ідентифікаційним

податковим номером і фотографіями з її заміського будинку, Суд встановив, що національні суди не надали конкретної та чіткої відповіді на аргументи, які мали б вирішальне значення для результату провадження, порушеного заявницею, нехтуючи правом на справедливий судовий розгляд, гарантованим пунктом 1 статті 6 Конвенції.

356. У справі *«Кеннеді проти Сполученого Королівства» (Kennedy v. the United Kingdom)*, 2010 (§§ 185-191), політика влади «не підтверджувати і не заперечувати», що була проведена операція з перехоплення комунікацій, не була визнана несумісною з пунктом 1 статті 6. Таким чином, Трибуналу з питань слідчих повноважень, створеному для розгляду скарг осіб, які підозрюють, що їхні повідомлення були незаконно перехоплені органами влади, було достатньо просто повідомити заявників про те, що рішення на їхню користь не було прийнято, оскільки політику Уряду «ні підтвердити, ні заперечити» можна було б обійти, якби в результаті звернення до цього суду заявникові було повідомлено про те, чи мало місце перехоплення (*там само*, § 189).

iii. Використання як доказів персональних даних, зібраних незаконно або з порушенням статті 8

357. Питання використання як речових доказів у судовому провадженні персональних даних, зібраних у спосіб, що суперечить вимогам національного законодавства або вимогам статті 8, розглядалося Судом у кількох справах в контексті адміністративного судочинства (*«Вукота-Боїч проти Швейцарії» (Vukota-Bojic v. Switzerland)*, 2016, § 77, щодо використання у спорі із застрахованою особою інформації, таємно зібраної страховою компанією в межах її повноважень за схемою державного страхування); цивільного судочинства (*«Барбулеску проти Румунії» (Bărbulescu v. Romania)* [ВП], 2017, §§ 140-141, про використання даних, зібраних роботодавцем щодо використання працівником інтернету на робочому місці, з метою виправдання його звільнення; *«Флоріндо де Альмейда Васконселос Грамаксо проти Португалії» (Florindo de Almeida Vasconcelos Gramaxo v. Portugal)*, 2022, §§ 130-140, щодо використання даних GPS про пробіг, записаних на службовому автомобілі медичного представника, як підстави для його звільнення); та кримінальних проваджень (*«Буков проти Росії» (Bykov v. Russia)* [ВП], 2009, §§ 80-83, щодо перехоплення розмови в рамках негласної поліцейської операції та використання отриманих таким чином доказів як підстави для винесення обвинувального вироку).

358. Суд постановив, що прийняття та використання в судовому провадженні доказів такого характеру не призводить автоматично до висновку, що провадження було несправедливим, якщо це провадження в цілому було справедливим (*«Буков проти Росії» (Bykov v. Russia)* [ВП], 2009, §§ 89-91; *«Вукота-Боїч проти Швейцарії» (Vukota-Bojic v. Switzerland)*, 2016, §§ 91-100).

359. Суд встановив порушення пункту 1 статті 6 у справі, що стосувалася інформації, отриманої від поліцейського інформатора, який використовував прихований пристрій для запису розмов у камері заявника, що не було «відповідно до закону» (*«Еллен проти Сполученого Королівства» (Allan v. the United Kingdom)*, 2002, §§ 45-53). Зізнання заявника не були спонтанними, а були викликані наполегливими допитами інформатора, який з подачі поліції здійснював запис розмов за обставин, які можна розглядати як функціональний еквівалент допиту, без жодних гарантій, які були б притаманні офіційному допиту в поліції. Хоча між заявником та інформатором не було особливих стосунків і не було виявлено прямого примусу, заявник зазнав би психологічного тиску, який би вплинув на добровільність його зізнань. За таких обставин отриману інформацію можна було б вважати такою, що була отримана всупереч волі заявника, а її використання в судовому процесі — таким, що порушує його право зберігати мовчання та привілей не свідчити проти себе.

iv. Публічний судовий розгляд та публічне проголошення судового рішення і секретність даних¹³

360. У справі *«П. і Б. проти Сполученого Королівства» (P. and B. v. the United Kingdom)*, 2001 (§§ 38-41, 46-49), відсутність публічного судового розгляду і проголошення рішення в закритому режимі у справі про проживання дитини було визнано таким, що не суперечить пункту 1 статті 6. На думку Суду, провадження у справах про опіку над дітьми — це яскравий приклад випадків, коли недопущення преси та громадськості може бути виправданим з метою захисту персональних даних відповідної дитини і сторін, а також для уникнення шкоди інтересам правосуддя (*там само*, § 38). Той факт, що будь-хто, хто міг констатувати зацікавленість, міг проконсультуватися або отримати копію повного тексту наказів і рішень, а також те, що судові рішення зазвичай публікуються без зазначення імен зацікавлених осіб, був достатнім для компенсації відсутності публічного проголошення (*там само*, § 47).

361. У справі *«Кеннеді проти Сполученого Королівства» (Kennedy v. the United Kingdom)*, 2010 (§ 188), Суд підтвердив, що відповідно до пункту 1 статті 6 національна безпека може виправдовувати виключення громадськості з процесу. Він постановив, що характер питань, порушених перед Трибуналом з питань слідчих повноважень, які стосувалися незаконного перехоплення повідомлень, виправдовує відсутність публічного слухання.

362. Суд встановив подвійне порушення статті 6 у справі *«Василь Васильєв проти Болгарії» (Vasil Vasilev v. Bulgaria)*, 2021, щодо повної відсутності публічного доступу (виключення громадськості з усіх слухань і відсутність публічного оголошення рішення) у провадженні, яке заявник порушив з метою відшкодування збитків після перехоплення, запису й розшифровки телефонної розмови між ним і клієнтом, за яким велося приховане спостереження у кримінальній справі. Відсторонення громадськості від усіх слухань і винесення рішення ґрунтувалося виключно на наявності у справі інформації з обмеженим доступом (докази, отримані в результаті негласного перехоплення телефонних розмов заявника). На думку Суду, повна відсутність публічного доступу не могла бути виправдана необхідністю захисту засекреченої інформації, яка була предметом цієї справи. Характер питань, порушених під час провадження, які стосувалися відповідальності державних органів за передбачуване порушення прав за статтею 8, не мав високотехнічного характеру, і заявник не відмовився від свого права на публічний розгляд (*там само*, §§ 107-111). Коли справа стосується ймовірного порушення основоположного права державними органами, громадський контроль за ходом судового розгляду важливий для підтримки довіри до верховенства права. Наявність у матеріалах справи засекреченої інформації сама по собі не може бути підставою для того, щоб приховувати від громадськості все судові рішення. Якщо справа стосується засекреченої інформації, існують методи, які дозволяють певною мірою забезпечити доступ громадськості до рішень, що містяться в ній, зберігаючи при цьому секретність конфіденційної інформації (*там само*, §§ 116-118).

v. Тривалість судових проваджень щодо захисту даних

363. У справі *«Сатакуннан Марккінапорссі Ой та Сатамедіа Ой проти Фінляндії» (Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland)* [ВП], 2017 (§ 215), Суд постановив, що загальна тривалість — шість років і шість місяців на двох рівнях юрисдикції — провадження щодо відповідності національному законодавству та праву Європейського Союзу масової публікації даних про особисте оподаткування компаніями-заявниками не відповідала вимозі розумного строку, передбаченій пунктом 1 статті 6. Провадження в Суді справедливості

¹³ Див. також вище розділ цього Посібника, присвячений Розголошення даних в контексті судового провадження з точки зору статті 8 Конвенції.

Європейського Союзу щодо запиту про винесення попереднього рішення не може братися до уваги при оцінці тривалості, що покладається на національні органи (*там само*, § 208).

364. Навпаки у справі *«Суріков проти України» (Surikov v. Ukraine)*, 2017 (§§ 104-106), Суд визнав явно необґрунтованою скаргу щодо тривалості провадження, пов'язаного зі зберіганням роботодавцем конфіденційної та застарілої інформації про психічне здоров'я працівника та її використання при розгляді його заяви про підвищення на посаді. Суд постановив, що період менше шести років на трьох рівнях юрисдикції не порушує вимогу розумного строку, передбачену пунктом 1 статті 6 (*там само*, § 101).

б. Конкретні гарантії (пункти 2 і 3 статті 6 Конвенції)

365. У кримінальних справах кожній особі, якій висунуто звинувачення на основі її персональних даних, повинні бути надані певні конкретні гарантії.

і. Захист даних і право на презумпцію невинуватості (пункт 2 статті 6 Конвенції)

366. У справі *«Батіашвілі проти Грузії» (Batiashvili v. Georgia)*, 2019 (§§ 87-97), Суд визнав, що пункт 2 статті 6 може бути застосований в ситуації, коли влада маніпулювала записом телефонних розмов особи до її арешту і транслювала його на телебаченні. На думку Суду, втручання органів влади сприяло тому, що заявник сприймався як винний до того, як його провина була доведена в суді, а отже, становило порушення пункту 2 статті 6. Послідовність подій, розглянута в цілому, вказує на те, що на ситуацію заявника суттєво вплинула поведінка слідчих органів (*там само*, § 94). Хоча обвинувачення в неповідомленні про злочин було знято під час розгляду справи в першій інстанції, в обвинувальному акті, направленому до суду майже через чотири місяці після того, як запис став доступним для громадськості, все ще містилося посилання на це обвинувачення, навіть попри те, що органи прокуратури повинні були добре знати про фальшивість доказів, що лежали в основі цього обвинувачення (*там само*, § 95).

367. У справі *«Й.Б. та інші проти Туреччини» (Y.B. and Others v. Turkey)*, 2004 (§§ 43-51), заяви, зроблені поліцією для преси щодо підозрюваних, які були сфотографовані журналістами на пресконференції, що проходила в приміщенні поліції, були визнані такими, що порушують пункт 2 статті 6. Публікація фотографій підозрюваних у ході кримінального провадження сама по собі не становить порушення їхнього права на презумпцію невинуватості. Національні органи влади мають право інформувати громадськість про поточні кримінальні розслідування за умови, що це робиться з усією необхідною розсудливістю й обачністю. Проте, якщо вони оприлюднюють об'єктивну інформацію щодо кримінального провадження, ця інформація повинна бути вільною від будь-яких оцінок або упереджень щодо вини (*там само*, §§ 47-48). У цій справі позиція органів міліції, оскільки вона передбачала попередню оцінку звинувачень, які могли бути висунуті заявникам, і надавала пресі легкі фізичні засоби для їх ідентифікації, була несумісною з презумпцією невинуватості (*там само*, § 50).

368. У справі *«Пантелеєнко проти України» (Panteleyenko v. Ukraine)*, 2006 (§ 68-71), судові рішення про закриття кримінального провадження проти заявника були сформульовані таким чином, що не залишали жодних сумнівів у тому, що судді вважали заявника винним у вчиненні злочину, в якому його обвинувачували; тому Суд встановив порушення пункту 2 статті 6. Рішення про закриття провадження з «нереабілітуючих підстав» було прийнято на підставі доказів, що містили персональні дані заявника, нотаріуса за фахом, і були отримані в результаті обшуку його офісу, проведеного з порушенням встановленої законом вимоги про завчасне вручення ордеру на обшук особи, яка займає відповідне приміщення, і заборони

вилучати будь-які документи і предмети, які не мають безпосереднього відношення до справи, що розслідується (*там само*, § 70)¹⁴.

ii. Захист даних і право на захист (підпункт «b» пункту 3 статті 6 Конвенції)

369. У справі *«Рук проти Німеччини» (Rook v. Germany)*, 2019 (§ 69), Суд постановив, що період у три з половиною місяці для вивчення великого обсягу даних та електронних файлів про заявника, отриманих за допомогою телекомунікаційного спостереження, був достатнім з точки зору підпункту «b» пункту 3 статті 6 для того, щоб дати можливість його адвокату підготувати захист. З огляду на складність кримінального провадження, не було необхідності надавати адвокату заявника можливість читати і прослуховувати кожну одиницю даних спостереження, які включали 45 000 телефонних дзвінків і 34 000 інших наборів даних, зібраних в ході розслідування, а також 14 мільйонів електронних файлів, які поліція конфіскувала у квартирі заявника та в інших місцях (*там само*, §§ 7-8, 67-71).

370. У більш загальному плані Суд підкреслив, що сучасні методи розслідування дійсно можуть призвести до отримання величезних обсягів даних, інтеграція яких у кримінальне провадження не повинна спричиняти невинуватих затримок у цьому провадженні. Право заявника на розголошення інформації не слід плутати з його правом на доступ до всіх матеріалів, які органи влади вже визнали релевантними, що, як правило, вимагає, щоб зацікавлена особа була в змозі зрозуміти матеріал у повному обсязі (*там само*, § 67). Той факт, що судовий розгляд вже розпочався, коли адвокат отримав повну копію справи, не означає, що у нього не було достатньо часу для підготовки. Підпункт «b» пункту 3 статті 6 не вимагає, щоб підготовка до судового розгляду, який триває протягом певного періоду часу, була завершена до першого судового засідання (*там само*, § 72)¹⁵.

371. У справі *«Сігурдур Ейнарсон та інші проти Ісландії» (Sigurður Einarsson and Others v. Iceland)*, 2019 (§§ 88-93), Суд постановив, що не було порушення пункту 1 та підпункту «b» пункту 3 статті 6 щодо відсутності доступу захисту до величезної кількості даних, зібраних обвинуваченням і не включених до матеріалів розслідування, а також того факту, що захист не мав права голосу в електронному просіюванні цих даних обвинуваченням з метою виявлення інформації, що стосується розслідування. Що стосується «повного збирання даних», то сторона обвинувачення не знала про зміст масиву даних, і в цьому відношенні вона не мала жодних переваг перед захистом. Що стосується «помічених» даних, в принципі, було б доречно, якби захист отримав можливість провести пошук потенційно виправдовувальних доказів. Однак заявники на жодному етапі офіційно не клопотали про видачу відповідного судового наказу і не вказали, які саме докази вони шукали.

2. Право на ефективний засіб юридичного захисту (стаття 13 Конвенції)¹⁶

372. У справі *«Анне-Марі Андерсон проти Швеції» (Anne-Marie Anderson v. Sweden)*, 1997 (§§ 41-42), що стосувалася розголошення медичної документації, Суд не встановив порушення статті 13 у поєднанні зі статтею 8 щодо відсутності у пацієнтки можливості оскаржити цей захід до того, як медичний орган передав персональні та конфіденційні медичні дані органу соціального забезпечення. Серед іншого, заявниця була повідомлена про цей захід, він мав

¹⁴ Див. також [Посібник зі статті 6 Конвенції](#) (Право на справедливий судовий розгляд (кримінальний аспект)) щодо обґрунтованості судових рішень (пп. 168-176)

¹⁵ Див. також [Посібник зі статті 6 Конвенції](#) (Право на справедливий судовий розгляд (кримінальний аспект)) щодо можливостей, необхідних обвинуваченим для підготовки свого захисту.

¹⁶ Цей розділ слід читати у світлі та в поєднанні з [Посібник зі статті 13 Конвенції](#) (Право на ефективний засіб правового захисту, див., зокрема, стор. 49-51).

обмежений характер, оскільки відповідна інформація не була оприлюднена, але залишалася захищеною тим самим рівнем конфіденційності, який застосовувався до психіатричних записів.

373. У справі *«Мік і Джовановіч проти Сербії» (Mik and Jovanović v. Serbia)* (ухв.) заявники скаржилися за статтею 8 окремо і в поєднанні зі статтею 13 на триваюче ненадання Державою достовірної інформації про долю їхніх малолітніх синів, які, як стверджувалося, померли незабаром після народження і тіла яких ніколи не були показані заявникам, Суд зазначив, що нещодавно прийнятий законодавчий акт створив механізм (включаючи базу даних ДНК) щодо ситуації, з якою зіткнулися заявники та інші особи. Зокрема, нова законодавча база передбачає як судові, так і позасудові процедури, спрямовані на з'ясування справжнього статусу новонароджених дітей, які, як підозрюється, зникли з державних пологових будинків, і надання відшкодування батькам. Крім того, були зроблені певні важливі кроки для впровадження цієї системи, включаючи широке навчання суддів, а також призначення, в контексті позасудової процедури, членів (представники зареєстрованих батьківських асоціацій, які становлять більшість) комісії з широкими повноваженнями щодо розслідування, збору даних і звітності. Відзначивши, що заявники самі зробили вибір на користь використання нового механізму, Суд дійшов висновку, що продовжувати розгляд заяви у розумінні підпункту «с» пункту 1 статті 37 Конвенції більше не є виправданим.

374. У справі *«Пантелеєнко проти України» (Panteleyenko v. Ukraine)*, 2006 (§§ 82-84), Суд встановив порушення статті 13 у поєднанні зі статтею 8 у зв'язку з відсутністю ефективного засобу юридичного захисту, який би дозволив заявнику поскаржитися на розголошення конфіденційної інформації про його психічне здоров'я на публічному слуханні. На думку Суду, існуючі засоби правового захисту виявилися неефективними, оскільки вони не призвели до припинення розголошення конфіденційних психіатричних даних у матеріалах судової справи чи будь-якого присудження заявникові компенсації за шкоду, заподіяну внаслідок втручання в його особисте життя. Хоча слухання в закритому режимі запобігло б розголошенню інформації громадськості, це не завадило б їй стати відомою сторонам або бути включеною до матеріалів справи.

375. Стосовно розміщення в інтернеті судового рішення, яке розголошує інформацію про усиновлення дітей заявників, Суд постановив у справі *«Х та інші проти Росії» (X and Others v. Russia)*, 2020 (§§ 73-79), що мало місце порушення статті 13 у поєднанні зі статтею 8 у зв'язку з відсутністю будь-яких засобів судового захисту, за допомогою яких можна було б отримати компенсацію за моральну шкоду, заподіяну збоями у функціонуванні системи правосуддя.

376. У справі, що стосувалася внесення особи як «правопорушника» до поліцейських реєстрів після того, як вона була допитана у зв'язку зі зґвалтуванням, і збереження цього запису, попри те, що обвинувальний акт згодом не був пред'явлений, Суд встановив порушення статті 13 у поєднанні зі статтею 8, зазначивши, що заявник не мав жодного засобу правового захисту у відповідний час, за допомогою якого він міг би оскаржити цей захід (*«Дімітров-Казаків проти Болгарії» (Dimitrov-Kazakov v. Bulgaria)*, 2011, §§ 37-39).

377. Відсутність ефективного засобу правового захисту, який би дозволив заявнику вимагати вилучення його імені зі списку, доданого до Указу про рух «Талібан», становила порушення статті 13 у поєднанні зі статтею 8 у справі *«Нада проти Швейцарії» (Nada v. Switzerland)* [ВП], 2012 (§§ 209-214). Заявник мав можливість звернутися до національних судів, але вони не розглянули його скарги по суті.

378. Що стосується використання персональних даних у професійному контексті, Суд визнав порушення статті 13 у поєднанні зі статтею 8 у справі *«Сміт і Грейді проти Сполученого Королівства» (Smith and Grady v. the United Kingdom)*, 1999 (§§ 136-139), через відсутність ефективного засобу правового захисту щодо порушення приватного життя заявників в результаті інтрузивних розслідувань приватного життя гомосексуалістів, що призвело до їх звільнення зі збройних сил.

379. У справі *«Карабейоглу проти Туреччини» (Karabeyoğlu v. Turkey)*, 2016 (§§ 128-132), відсутність національного засобу правового захисту, за допомогою якого можна було б домогтися перегляду використання в дисциплінарному провадженні даних, отриманих за допомогою прослуховування телефонних розмов у кримінальному розслідуванні, призвело до того, що Суд визнав порушення статті 13 у світлі статті 8.

380. У справі *«Пек проти Сполученого Королівства» (Peck v. the United Kingdom)*, 2003 (§§ 101-114), Суд постановив, що заявник не мав ефективного засобу правового захисту, за допомогою якого можна було б поскаржитися на розголошення в засобах масової інформації записів камер відеоспостереження, на яких він намагається вчинити самогубство в громадському місці. Що стосується можливості судового оскарження, то оскільки єдиним питанням, яке розглядалося національними судами, було те, чи можна вважати політику щодо зображень, знятих камерами відеоспостереження в громадських місцях, «ірраціональною», будь-який розгляд питання про те, чи відповідало втручання в право заявника нагальній суспільній потребі або було пропорційним, був фактично виключений (*там само*, §§ 106-107). Що стосується комісій з питань ЗМІ, то відсутність у них повноважень присуджувати відшкодування збитків означало, що вони також не могли забезпечити ефективний засіб правового захисту (*там само*, §§ 108-109). Що стосується позову про порушення конфіденційності, то малоімовірно, що суди визнали б у відповідний час, що зображення мали «необхідну якість конфіденційності» або що інформація була «передана за обставин, які передбачають зобов'язання зберігати конфіденційність» (*там само*, § 111).

381. Що стосується таємного спостереження, то таємність заходів ускладнює, якщо не унеможлиблює, використання зацікавленою особою засобу правового захисту, особливо під час здійснення спостереження. «Ефективний засіб правового захисту» для цілей статті 13 має означати засіб правового захисту, який є настільки ефективним, наскільки це можливо, зважаючи на обмежені можливості звернення, що властиві будь-якій системі спостереження (*«Класс та інші проти Німеччини» Klass and Others v. Germany*, 1978, §§ 68-69). Об'єктивний наглядовий механізм може бути достатнім, якщо заходи залишаються таємними. Лише після того, як заходи були розголошені, протягом розумного періоду засоби правового захисту повинні стати доступними зацікавленій особі (*«Ротару проти Румунії» Rotaru v. Romania* [ВП], 2000, § 69).

382. Що стосується заходів цільового таємного спостереження, коли зловживання потенційно настільки легкі в окремих випадках і можуть мати такі шкідливі наслідки для демократичного суспільства в цілому, в принципі бажано довірити наглядовий контроль судді, судовий контроль пропонує найкращі гарантії незалежності, неупередженості та належної процедури. Після скасування заходу спостереження відповідні особи повинні бути проінформовані якнайшвидше, як тільки це стане можливим без шкоди для мети обмеження. Щоб дати можливість зацікавленій особі отримати перегляд провадження щодо втручання у здійснення її права на приватне життя, в принципі необхідно надати цій особі мінімальний обсяг інформації щодо рішення, яке можна оскаржити, наприклад, про дату його прийняття та суд, який його видав (*«Роман Захаров проти Росії» (Roman Zakharov v. Russia)* [ВП], 2015, §§ 233, 287 і 294; *«Ірфан Гюзель проти Туреччини» (İrfan Güzel v. Turkey)*, 2017, §§ 96 і 98-99).

383. У справі *«Класс та інші проти Німеччини» (Klass and Others v. Germany)*, 1978 (§§ 65-72), закон «G10» дозволяв органам влади відкривати й перевіряти пошту, читати телеграфні повідомлення та прослуховувати й записувати телефонні розмови з метою захисту країни від «неминучої небезпеки». Суд постановив, що сукупність засобів правового захисту, передбачених законодавством Німеччини, за конкретних обставин тієї справи задовольняла вимоги статті 13 у світлі статті 8 щодо поваги до приватного життя та листування. Хоча, згідно із Законом, рішення про застосування обмежувальних заходів не може бути оскаржене в суді, особам, які вважали, що вони перебувають під наглядом, були доступні різні інші засоби правового захисту. Згідно з рішенням Федерального конституційного суду від 1970 року

компетентний орган був зобов'язаний повідомити відповідну особу, щойно заходи спостереження були припинені, і повідомлення могло бути зроблено без шкоди для мети обмеження. З моменту такого повідомлення особам стають доступними різні засоби правового захисту в суді. Вони могли: подати позов про визнання, щоб домогтися розгляду адміністративними судами питання про те, чи були законно застосовані положення закону G10 у їхній справі і чи відповідали закону призначені заходи спостереження; подати позов про відшкодування збитків до цивільного суду, якщо їм було завдано шкоди; або подати позов про знищення або, якщо це доречно, про реституцію документів. Нарешті, якщо жоден із цих засобів не був успішним, вони могли звернутися до Федерального Конституційного Суду з проханням винести рішення щодо того, чи мало місце порушення Основного закону. Див., у тому ж ключі, справи *«Леандер проти Швеції» (Leander v. Sweden)*, 1987, §§ 78-84, що стосуються системи таємної перевірки кандидатів на важливі посади з точки зору національної безпеки, та *«Аманн проти Швейцарії» (Amann v. Switzerland)* [ВП], 2000, §§ 89-90, щодо перехоплення та запису телефонних розмов, а також зберігання персональних даних службами безпеки.

384. У зв'язку з відсутністю відповіді на побоювання обвинуваченого щодо законності прослуховування його телефонних розмов, Суд визнав порушення статті 13 у поєднанні зі статтею 8 у справі *«Ірфан Гюзель проти Туреччини» (İrfan Güzel v. Turkey)*, 2017 (§§ 100-109).

385. У справі *«Еллен проти Сполученого Королівства» (Allan v. the United Kingdom)*, 2002 (§ 55), Суд встановив порушення статті 13 у поєднанні зі статтею 8 на тій підставі, що у відповідний час не існувало законодавчої системи, яка б регулювала використання прихованих пристроїв для запису розмов у камері заявника та їх використання поліцією.

386. У справі, де загальний контроль над системою негласного спостереження був покладений виключно на Міністра внутрішніх справ (який брав безпосередню участь у запитах на використання спеціальних засобів спостереження для захисту національної безпеки), а не на незалежні органи, Суд встановив порушення статті 13 у світлі статті 8 у зв'язку з відсутністю ефективного засобу юридичного захисту (*«Асоціація за європейську інтеграцію і права людини та Екімджиев проти Болгарії» (Association for European Integration and Human Rights and Ekimdzhev v. Bulgaria)*, 2007, §§ 98-103).

387. З огляду на відсутність засобу правового захисту, за допомогою якого можна було б оскаржити збереження представниками Держави даних про приватне життя особи або правдивість такої інформації, Суд визнав порушення статті 13 у поєднанні зі статтею 8 у справі *«Ротару проти Румунії» (Rotaru v. Romania)* [ВП], 2000 (§§ 68-73). Він дійшов аналогічного висновку у справі *Зегерштедт-Віберг та інші проти Швеції» (Segerstedt-Wiberg and Others v. Sweden)*, 2006 (§§ 116-122), у зв'язку з відсутністю засобу правового захисту, який дозволив би заявникам переглянути в повному обсязі інформацію про них у файлах поліції безпеки, а також домогтися знищення файлів, що зберігалися на них поліцією безпеки, і видалення або виправлення особистої інформації, що міститься в цих файлах.

3. Право на свободу та особисту недоторканність (стаття 5 Конвенції)

400. У справі *«Акгюн проти Туреччини» (Akgün v. Turkey)*, 2021 (§§ 178-181), де на момент початкового досудового тримання під вартою заявника єдиним доказом, який був наданий для обґрунтування підозри за підпунктом «с» пункту 1 статті 5 у вчиненні ним злочину, пов'язаного з належністю до терористичної організації, був висновок про те, що він користувався зашифрованою системою обміну повідомленнями VuLock, Суд встановив порушення цього положення Конвенції. Потенційна злочинна діяльність заявника стосувалася організованої злочинності. Використання електронних доказів, які вказують на те, що особа користувалася сервісом зашифрованих повідомлень, який був спеціально розроблений і використовувався виключно злочинною організацією для цілей внутрішньої комунікації цієї організації, може

бути важливим інструментом у боротьбі з організованою злочинністю. Як наслідок, на підставі таких доказів підозрюваного можна затримати на самому початку провадження, оскільки вони можуть слугувати вагомим доказом приналежності особи до такої організації. Якщо такі докази становили єдину або виключну основу підозри проти особи, національний суд повинен був мати у своєму розпорядженні достатню інформацію про відповідні матеріали, перш ніж розглядати, з належною обачністю, їхню можливу доказову цінність відповідно до національного законодавства. У цій справі Уряд не зміг довести, що на дату взяття заявника під варту до суду докази, наявні у мирового судді, відповідали стандарту «обґрунтованої підозри», який вимагається підпунктом «с» пункту 1 статті 5 Конвенції, а саме, щоб задовольнити об'єктивного спостерігача в тому, що він міг вчинити злочини, за які його було затримано. На думку Суду, документ, в якому містився висновок про те, що заявник використовував *ByLock*, сам по собі не вказував і не описував жодної незаконної діяльності з боку заявника, оскільки в ньому не визначалися ні дати цієї передбачуваної діяльності, ні її частота, а також не містилося жодних додаткових пов'язаних з цим деталей. Крім того, ні в цьому документі, ні в постанові про обрання запобіжного заходу у вигляді досудового тримання під вартою не було зазначено, яким чином ця передбачувана діяльність заявника вказувала на його членство в терористичній організації.

IV. Сучасні виклики захисту даних

A. Технологічний прогрес, алгоритми та штучний інтелект¹⁷

401. У справах, що стосуються збирання та зберігання органами влади з метою запобігання злочинам відбитків пальців, біологічних зразків і профілів ДНК осіб, підозрюваних або засуджених за вчинення злочинів, Суд чітко зазначив, що використання сучасних наукових методів не може бути дозволено за будь-яку ціну і без ретельного балансу між потенційними перевагами широкого застосування таких методів і важливими інтересами приватного життя (*«С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom)* [ВП], 2008, § 112; *«Подчасов проти Росії» (Podchasov v. Russia)*, 2024, § 62). Будь-яка Держава, яка претендує на роль першопрохідця в розвитку нових технологій, несе особливу відповідальність за дотримання правильного балансу в цьому відношенні (*«С. і Марпер проти Сполученого Королівства» (S. and Marper v. the United Kingdom)* [ВП], 2008, § 112). Беручи до уваги швидкі темпи розвитку генетики та інформаційних технологій, можливість того, що в майбутньому інтереси приватного життя, пов'язані з генетичною інформацією, можуть зазнати негативного впливу у новий спосіб або у спосіб, який сьогодні неможливо точно передбачити (*там само*, § 71).

402. На думку Суду, стрімкий розвиток все більш досконалих технологій, що дозволяють, серед іншого, застосовувати до фотографій фізичних осіб методи розпізнавання обличчя і відображення обличчя, робить проблематичним фотографування осіб, а також зберігання і можливе поширення отриманих даних. Національні суди повинні враховувати ці фактори при оцінці необхідності втручання в приватне життя відповідної особи (*«Ґоґран проти Сполученого Королівства» (Gaughran v. the United Kingdom)*, 2020, § 70). У цій справі (*там само*, §§ 96-98), Суд наголосив, що сучасні технології більш складні, і що національні суди не приділили достатньої уваги цьому аспекту при розгляді необхідності втручання в право на повагу до

¹⁷ Цей розділ слід читати в поєднанні з розділами цього Посібника, присвяченими Зберігання персональних даних з метою боротьби зі злочинністю і Збирання даних органами влади за допомогою прихованого спостереження.

приватного життя заявника, фотографія якого була зроблена органами влади після незначного правопорушення і зберігалася навіть після того, як його судимість була видалена з обліку після спливу встановленого законом строку.

388. У справі *«Бреєр проти Німеччини» (Breyer v. Germany)*, 2020 (§ 88), Суд визнав, що в контексті боротьби з організованою злочинністю та тероризмом сучасні засоби телекомунікацій та зміни в комунікативній поведінці вимагають адаптації слідчих інструментів. На думку Суду, зобов'язання операторів мобільного зв'язку зберігати інформацію про абонентів і надавати її органам влади на їхній запит є, загалом, адекватною відповіддю на зміни в комунікаційній поведінці та в засобах телекомунікацій. Навпаки у справі *«Подчасов проти Росії» (Podchasov v. Russia)*, 2024 (§§ 70-79), національне законодавство вимагало від постачальників послуг інтернет-зв'язку зберігати зміст усіх інтернет-комунікацій протягом шести місяців, а пов'язані з ними комунікаційні дані — протягом одного року, а також надавати правоохоронним органам або службам безпеки доступ до збережених даних на їхню вимогу разом з інформацією, необхідною для розшифрування електронних повідомлень, якщо вони були зашифровані: Суд був вражений надзвичайно широким обов'язком зберігати інформацію та визнав таке втручання надзвичайно широкомасштабним і серйозним. Суд також зазначив, що згідно з національним законодавством, правоохоронні органи або служби безпеки не зобов'язані пред'являти судовий дозвіл відповідному постачальнику послуг зв'язку перед отриманням доступу до комунікацій певної особи. Фактично, постачальники послуг зв'язку були зобов'язані встановити обладнання, яке надавало б зазначеним органам прямий доступ до даних, що зберігаються. Хоча в такій системі потреба у захисті від свавілля та зловживань була особливо великою, національне законодавство не передбачало таких гарантій. Що стосується законодавчої вимоги розшифровувати повідомлення, то видається, що будь-які такі заходи не будуть обмежуватися конкретними особами й послаблять шифрування для всіх користувачів, таким чином впливаючи на всіх без винятку, включаючи осіб, які не становлять загрози законним інтересам; отже, такі заходи не можуть вважатися пропорційними (§§ 77-79).

389. У справі *«Шабо та Віссу проти Угорщини» (Szabó and Vissy v. Hungary)*, 2016 (§ 68), що стосується масового спостереження за комунікаціями, Суд визнав, що природним наслідком форм, яких набуває сучасний тероризм, є те, що уряди вдаються до новітніх технологій, включаючи масовий моніторинг комунікацій, з метою запобігання неминучим атакам. У цій справі Суд постановив, що законодавство, яке дозволяє масове спостереження, не забезпечує необхідних гарантій проти зловживань, оскільки нові технології дозволяють владі легко перехоплювати великі обсяги даних, що стосуються навіть людей, які не належать до категорії, на яку спочатку була спрямована операція. Більше того, заходи такого роду можуть бути призначені виконавчою владою без будь-якого контролю і без будь-якої оцінки того, чи були вони дійсно необхідними, а також за відсутності будь-якого ефективного судового або іншого засобу правового захисту (*там само*, §§ 73-89).

390. У справі *«Роман Захаров проти Росії» (Roman Zakharov v. Russia)* [ВП], 2015 (§§ 302-305), Суд постановив, що ризик зловживань, притаманний будь-якій системі таємного спостереження, був особливо високим у системі, де спецслужби та поліція мали прямий доступ за допомогою технічних засобів до всіх мобільних телефонних комунікацій. Суд визнав порушення статті 8, вважаючи, що російське законодавство, яке дозволяє загальне перехоплення комунікацій, не забезпечує адекватних та ефективних гарантій проти свавілля і ризику зловживань, притаманних будь-якій системі таємного спостереження.

391. У справі *«Акгюн проти Туреччини» (Akgün v. Turkey)*, 2021 (§§ 178-181), де під час початкового досудового ув'язнення заявника висновок про те, що він використовував зашифровану систему обміну повідомленнями ByLock, був єдиним доказом, який був наданий для обґрунтування підозри, для цілей підпункту «с» пункту 1 статті 5, у вчиненні ним злочину, Суд підкреслив, що використання таких доказів як єдиної підстави для підозри може викликати ряд делікатних питань, оскільки за своєю природою процедура і технології, застосовані при

зборі цих доказів, були складними і, відповідно, могли зменшити здатність національних судів встановити їх автентичність, точність і цілісність (див. п. 373 вище).

392. У справах *«Центр правосуддя проти Швеції» (Centrum för rättvisa v. Sweden)* [ВП], 2021, § 261, та *«Біг Бразер Вотч та інші проти Сполученого Королівства» (Big Brother Watch and Others v. the United Kingdom)* [ВП], 2021, §§ 322-323, Суд прямо визнав, що використання режиму масового перехоплення саме по собі не суперечить статті 8, зважаючи на поширення загроз, з якими наразі стикаються Держави від мереж міжнародних суб'єктів, що використовують інтернет для спілкування, а також на існування сучасних технологій, що дають змогу цим суб'єктам уникати виявлення. Однак, Суд наголосив, що з огляду на постійний розвиток сучасних комунікаційних технологій, його звичайний підхід до режимів цільового спостереження повинен бути адаптований для відображення специфічних особливостей режиму масового перехоплення з огляду на ризик зловживання повноваженнями на масове перехоплення і законну необхідність дотримання таємниці в таких операціях. Зокрема, цей процес повинен був підпадати під дію «наскрізних гарантій», що означає, що на національному рівні на кожному етапі процесу повинна проводитися оцінка необхідності та пропорційності вжитих заходів; що на масове перехоплення з самого початку має надаватися незалежний дозвіл, якщо об'єкт і масштаби операції визначені; і що за операцією має здійснюватися нагляд і незалежний розгляд *ex post facto*.

393. У справі *«Глухін проти Росії» (Glukhin v. Russia)*, 2023, Суд вперше розглянув питання про використання поліцією технології розпізнавання обличчя. Ця технологія була використана, по-перше, для ідентифікації заявника за фотографіями та відео, опублікованими на публічному каналі Telegram, і, по-друге, для його розшуку й арешту під час поїздки в міському метрополітені. Суд відзначив дуже інтрузивний характер цих заходів, наголосивши, що, аби такі заходи вважалися «необхідними в демократичному суспільстві», потрібен високий рівень обґрунтування, причому найвищий рівень обґрунтування вимагається для використання технології розпізнавання обличчя у реальному часі (*там само*, § 86). У зв'язку з цим Суд зазначив, що заявника було притягнуто до відповідальності за незначне правопорушення, яке полягало у проведенні одиночної демонстрації без попереднього повідомлення. Його ніколи не звинувачували у вчиненні будь-яких засуджуваних дій під час демонстрації (таких як перешкоджання руху транспорту, пошкодження майна або акти насильства). Ніколи не стверджувалося, що його дії становили будь-яку небезпеку для громадського порядку або безпеки на транспорті. За таких обставин Суд вирішив, що використання технології розпізнавання обличчя для ідентифікації заявника, а отже, і використання технології розпізнавання обличчя в реальному часі для його розшуку та арешту, не відповідало «нагальній суспільній потребі», а отже, не могло вважатися «необхідним у демократичному суспільстві» (*там само*, §§ 88-90).

В. Інтернет та пошукові системи

394. Інтернет-сайти — це інформаційно-комунікаційний інструмент, який особливо відрізняється від друкованих засобів масової інформації, особливо щодо здатності зберігати й передавати інформацію (*«Венгжиновський і Смольчевський проти Польщі» (Węgrzynowski and Smolczewski v. Poland)*, 2013, § 58; *«М.Л. та В.В. проти Німеччини» (M.L. and W.W. v. Germany)*, 2018, § 91; *«Гурбейн проти Бельгії» (Hurbain v. Belgium)* [ВП], 2023, § 236). У світлі своєї доступності та здатності зберігати і передавати величезні обсяги інформації інтернет відіграє важливу роль у розширенні доступу громадськості до новин і сприянні поширенню інформації в цілому (*«Таймз Ньюзпейперс Лтд проти Сполученого Королівства» (№№ 1 і 2) (Times Newspapers Ltd v. the United Kingdom (nos. 1 і 2))*, 2009, § 27).

395. Ризик шкоди, яку контент і комунікації в інтернеті становлять для здійснення та реалізації прав і свобод людини, зокрема права на повагу до приватного життя, безумовно, вищий, ніж

ризик, який становить преса, особливо з огляду на важливу роль пошукових систем (*«Гурбейн проти Бельгії» (Hurbain v. Belgium)* [ВП], 2023, § 236; *«М.Л. та В.В. проти Німеччини» (M.L. and W.W. v. Germany)*, 2018, § 91 та наведені там посилання).

396. Інформація, що містить персональні дані, якою володіють засоби масової інформації, може бути легко знайдена користувачами інтернету за допомогою пошукових систем. Через цей посилюючий вплив на поширення інформації та характер діяльності, що лежить в основі публікації інформації, зобов'язання пошукових систем перед фізичною особою, яка є суб'єктом інформації, можуть відрізнятися від зобов'язань суб'єкта, який первісно опублікував інформацію (*«Гурбейн проти Бельгії» (Hurbain v. Belgium)* [ВП], 2023, § 207; *«М.Л. та В.В. проти Німеччини» (M.L. and W.W. v. Germany)*, 2018, § 97). З огляду на відмінність між діяльністю та обов'язками операторів пошукових систем і видавців новин, суб'єкти даних, які звертаються за захистом своїх персональних даних у цьому контексті, не зобов'язані попередньо або одночасно звертатися до вебсайту-оригіналу, щоб реалізувати свої права щодо пошукових систем, оскільки це дві різні форми обробки, кожна з яких має свої підстави для легітимності та має різний вплив на права та інтереси особи. Аналогічно, розгляд позову проти видавця новинного вебсайту не може бути поставлений в залежність від попереднього запиту про виключення з переліку (*«Гурбейн проти Бельгії» (Hurbain v. Belgium)* [ВП], 2023, § 208). Див. також пп. **Error! Reference source not found.-Error! Reference source not found.** цього Посібника вище, щоб отримати додаткову інформацію про «право на забуття»

397. На думку Суду, інтернет-архіви сприяють збереженню та доступності новин та інформації (*«Таймз Ньюспейперс Лтд проти Сполученого Королівства» (№№ 1 і 2) (Times Newspapers Ltd v. the United Kingdom (nos. 1 і 2))*, 2009, § 45). Такі архіви становлять важливе джерело для освіти та історичних досліджень, особливо тому, що вони легко доступні для громадськості і, як правило, безкоштовні (*«Гурбейн проти Бельгії» (Hurbain v. Belgium)* [ВП], § 180). Свобода розсуду, надана Державам у встановленні балансу між конкуруючими правами, є більшою, коли йдеться про архіви новин про минулі події, а не про репортажі про поточні події (*«Таймз Ньюспейперс Лтд проти Сполученого Королівства» (№№ 1 і 2) (Times Newspapers Ltd v. the United Kingdom (nos. 1 і 2))*, § 45). Обов'язок преси діяти відповідно до принципів відповідальної журналістики, забезпечуючи точність опублікованої довготривалої, а не односторонньої інформації, більш суворий за відсутності терміновості в публікації матеріалу (*там само*, § 45).

398. У справі *«Гурбейн проти Бельгії» (Hurbain v. Belgium)* [ВП], 2023 (§§ 180-185) Суд відзначив появу консенсусу в Європі щодо важливості архівів, які, за загальним правилом, повинні залишатися автентичними, достовірними та повними, щоб преса могла виконувати свою місію. Відповідно, цілісність архівів преси має бути керівним принципом при розгляді будь-якого запиту на видалення або зміну всієї або частини архівної статті, особливо якщо її законність ніколи не ставилася під сумнів. Такі запити вимагають особливої пильності та ретельного вивчення з боку національних органів влади.

С. Передача даних і потоки даних

399. У справі *«Сатакуннан Марккінапорссі Ой та Сатамедіа Ой проти Фінляндії» (Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland)* [ВП], 2017, що стосувалася масових потоків персональних даних, персональні податкові дані про 1,2 млн осіб були опубліковані в журналі, а згодом поширені за допомогою служби текстових повідомлень. На думку Суду існування суспільного інтересу в наданні доступу до великих обсягів податкових даних і дозволу на їх збір у журналістських цілях не обов'язково або автоматично означало, що також існував суспільний інтерес у масовому поширенні таких необроблених даних у незміненому вигляді без будь-якого аналітичного втручання. Необхідно розрізняти обробку даних у журналістських цілях і поширення необроблених даних, до яких журналісти мали

привілейований доступ (*там само*, § 175). У цьому контексті факт заборони масової публікації даних про особисте оподаткування у спосіб, несумісний з фінськими та європейськими правилами захисту даних, сам по собі не був санкцією, незважаючи на те, що на практиці обмеження, накладені на обсяг інформації, що підлягає оприлюдненню, могли зробити деякі з видів діяльності компаній-заявників менш прибутковими (*там само*, § 197).

400. У справі «*Біз Бразер Вотч та інші проти Сполученого Королівства*» (*Big Brother Watch and Others v. the United Kingdom*) [ВП], 2021, серед іншого, було порушено питання про сумісність зі статтею 8 Конвенції обміну даними, перехопленими іноземними спецслужбами, в цьому випадку Агентством національної безпеки США (NSA). Суд постановив, що обмін даними повинен регулюватися чіткими докладними правилами, які дають громадянам адекватне уявлення про обставини й умови, за яких влада уповноважена звертатися з таким запитом і які забезпечують ефективні гарантії проти використання цих повноважень в обхід внутрішнього законодавства та/або зобов'язань Держав за Конвенцією. Після отримання матеріалів перехоплення Держава-одержувач повинна забезпечити належні гарантії для їх вивчення, використання та зберігання; для їх подальшої передачі та для їх видалення і знищення. Ці гарантії в рівній мірі застосовуються до отримання Державою-учасницею запитуваних матеріалів перехоплення від іноземної розвідувальної служби. Якщо Держави не завжди знають, чи є матеріали, отримані від іноземних розвідувальних служб, результатом перехоплення, то Суд вважає, що ті ж стандарти повинні застосовуватися до всіх матеріалів, отриманих від іноземних розвідувальних служб, які можуть бути результатом перехоплення. Зрештою, за будь-яким режимом, який дозволяє розвідувальним службам запитувати перехоплення чи надання перехоплених матеріалів у Держави, які не є учасницями Конвенції, або отримання прямого доступу до таких матеріалів, має здійснюватися незалежний нагляд, а також має бути можливість незалежного розгляду *ex post facto* (*там само*, §§ 498-499).

Перелік цитованих справ

Цитована в цьому Посібнику судова практика включає винесені Судом рішення або ухвали, а також рішення або доповіді Європейської комісії з прав людини (надалі — «Комісія»).

Якщо не вказано інше, усі посилання стосуються рішення по суті справи, що були постановлені Палатою Суду. Скорочення «(ухв.)» вказує на те, що наводиться цитата з ухвали Суду, а аббревіатура «[ВП]» — на те, що справа розглядалася Великою Палатою.

Рішення Палати, які не є остаточними у розумінні статті 44 Конвенції, позначені зірочкою у переліку нижче. У пункті 2 статті 44 Конвенції зазначено: «Рішення Палати стає остаточним: (а) якщо сторони заявляють, що вони не звертатимуться з клопотанням про передання справи на перегляд Великої Палати; або (b) через три місяці від дати постановлення рішення, якщо клопотання про передання справи на перегляд Великої Палати не було заявлено; або (c) якщо колегія Великої Палати відхиляє клопотання про передання справи на перегляд Великої Палати згідно зі статтею 43». У випадках, коли клопотання про передання справи приймається колегією Великої Палати, рішення Палати не стає остаточним і, отже, не має законної сили; остаточним стає подальше рішення Великої Палати.

Гіперпосилання на цитовані справи в електронній версії Посібника ведуть до бази даних HUDOC (<http://hudoc.echr.coe.int>), яка забезпечує доступ до практики Суду (Великої Палати, рішень та ухвал Палати та Комітету, комунікованих справ, консультативних висновків і правових оглядів з Інформаційного бюлетеня про судову практику) і Комісії (рішення і доповіді), а також резолюцій Комітету міністрів.

Суд виносить свої рішення та ухвали англійською та/або французькою мовою — двома офіційними мовами Суду. База даних HUDOC також містить переклади багатьох важливих справ на більш ніж тридцять неофіційних мов, а також посилання на близько сотню онлайн-зібрань судової практики, підготовлених третіми сторонами. Усі мовні версії, що доступні для наведених справ, доступні через вкладку «мовні версії» у базі даних HUDOC, вкладку, яку можна знайти після натискання на гіперпосилання на справу.

—А—

- «*А.Б. проти Нідерландів*» (*A.B. v. the Netherlands*), № 37328/97, 29 січня 2002 року
«*А.П., Гарсон і Ніко проти Франції*» (*A.P., Garçon and Nicot v. France*), №№ 79885/12 та 2 інших, ЄСПЛ 2017
«*А. П. проти Вірменії*» (*A.P. v. Armenia*), № 58737/14, 18 червня 2024 року
«*Авілкіна та інші проти Росії*» (*Avilkina and Others v. Russia*), № 1585/09, 06 червня 2013 року
«*Адомайтис проти Литви*» (*Adomaitis v. Lithuania*), № 14833/18, 18 січня 2022 року
«*Ай. проти Сполученого Королівства*» (*I. v. The United Kingdom*) [ВП], № 25680/94, 11 липня 2006
«*Айсагуер проти Франції*» (*Aysaquer v. France*), № 8806/12, 22 червня 2017 року
«*Акгюн проти Туреччини*» (*Akgün v. Turkey*), № 19699/18, 20 липня 2021 року
«*Аксель Шпрінгер АГ проти Німеччини*» *Axel Springer AG v. Germany* [ВП], № 39954/08, 07 лютого 2012 року
«*Аксель Шпрінгер СЕ та РТЛ Телевізійон ГмБХ проти Німеччини*» (*Axel Springer SE and RTL Television GmbH v. Germany*), № 51405/12, 21 вересня 2017
«*Александрідіс проти Греції*» (*Alexandridis v. Greece*), № 19516/06, 21 лютого 2008 року
«*Алкая проти Туреччини*» (*Alkaya v. Turkey*), № 42811/06, 09 жовтня 2012 року

«Альфа Дорифорікі Тілеорасі Анонімі Етайріа проти Греції» (*Alpha Doryforiki Tileorasi Anonymi Etairia v. Greece*), № 72562/10, 22 лютого 2018 року
«Аманн проти Швейцарії» (*Amann v. Switzerland*) [ВП], № 27798/95, ЄСПЛ 2000-II
«Андре та інші проти Франції» (*André and Others v. France*), № 18603/03, 24 липня 2008 року
«Антовіч і Мірковіч проти Чорногорії» (*Antović and Mirković v. Montenegro*), № 70838/13, 28 листопада 2017 року
«Антонета Тудор проти Румунії» (*Antoneta Tudor v. Romania*) (*Antoneta Tudor v. Romania*), № 23445/04, 24 вересня 2013 року
«Анчев проти Болгарії» (*Anchev v. Bulgaria*) (ухв.), №№ 38334/08 та 68242/16, 05 грудня 2017 року
«Апосту проти Румунії» (*Apostu v. Romania*), № 22765/12, 03 лютого 2015 року
«Армонієне проти Литви» (*Armonienė v. Lithuania*), № 36919/02, 25 листопада 2008 року
«Асоціація «21 грудня 1989» та інші проти Румунії» (*Association «21 December 1989» and Others v. Romania*), №№ 33810/07 і 18817/08, 24 травня 2011 року
«Асоціація за європейську інтеграцію і права людини та Екімджієв проти Болгарії» (*Association for European Integration and Human Rights and Ekimdzhiiev v. Bulgaria*), № 62540/00, 28 червня 2007 року

—Б—

«Б.Б. проти Франції» (*B.B. v. France*), № 5335/06, 17 грудня 2009 року
«Барбулеску проти Румунії» (*Bărbulescu v. Romania*) [ВП], № 61496/08, 05 вересня 2017 (витяги)
«Батіашвілі проти Грузії» (*Batiashvili v. Georgia*), № 8284/07, 10 жовтня 2019 року
«Беґгал проти Сполученого Королівства» (*Beghal v. the United Kingdom*), № 4755/16, 28 лютого 2019 року
«Бедат проти Швейцарії» (*Bédat v. Switzerland*) [ВП], № 56925/08, ЄСПЛ 2016
«Бен Файза проти Франції» (*Ben Faiza v. France*), № 31446/12, 08 лютого 2018 року
«Бенедік проти Словенії» (*Benedik v. Slovenia*), № 62357/14, 24 квітня 2018 року
«Берн Ларсен Голдінг АС та інші проти Норвегії» (*Bernh Larsen Holding AS and Others v. Norway*), № 24117/08, 14 березня 2013 року
«Биков проти Росії» (*Vukov v. Russia*) [ВП], № 4378/02, 10 березня 2009 року
«Біг Бразер Вотч та інші проти Сполученого Королівства» (*Big Brother Watch and Others v. the United Kingdom*) [ВП], №№ 58170/13 та 2 інших, 25 травня 2021 року
«Бірюк проти Литви» (*Biriuk v. Lithuania*), № 23373/03, 25 листопада 2008 року
«Богомолова проти Росії» (*Bogomolova v. Russia*), № 13812/09, 20 червня 2017 року
«Болевіч проти Сербії» (*Boljević v. Serbia*), № 47443/14, 16 червня 2020 року
«Бреєр проти Німеччини» (*Breyer v. Germany*), № 50001/12, 30 січня 2020 року
«Брунет проти Франції» (*Brunet v. France*), № 21010/10, 18 вересня 2014
«Бук проти Німеччини» (*Buck v. Germany*), № 41604/98, ЄСПЛ 2005-IV
«Бутуруга проти Румунії» (*Buturugă v. Romania*), № 56867/15, 11 лютого 2020 року
«Бьянкарді проти Італії» (*Biancardi v. Italy*), № 77419/16, 25 листопада 2021 року

—В—

«В. проти Нідерландів» (*W. v. the Netherlands*) (ухв.), № 20689/08, 20 січня 2009 року
«Валашінас проти Литви» (*Valašinas v. Lithuania*), № 44558/98, ЄСПЛ 2001-VIII
«Валензуела Контрерас проти Іспанії» (*Valenzuela Contreras v. Spain*), № 2767/95, Збірник рішень та ухвал 1998-V
«Ван Вондель проти Нідерландів» (*Van Vondel v. the Netherlands*), № 38258/03, 25 жовтня 2007 року

- «Ван дер Вельден проти Нідерландів» (*Van der Velden v. the Netherlands*) (ухв.), № 29514/05, ЄСПЛ 2006-XV
- «Василь Васильєв проти Болгарії» (*Vasil Vasilev v. Bulgaria*), № 7610/15, 16 листопада 2021 року
- «Васильчук проти України» (*Vasylychuk v. Ukraine*), № 24402/07, 13 червня 2013 року
- «Вебер і Саравія проти Німеччини» (*Weber and Saravia v. Germany*) (ухв.), № 54934/00, ЄСПЛ 2006-XI
- «Венгжиновський і Смольчевський проти Польщі» (*Węgrzynowski and Smolczewski v. Poland*), № 33846/07, 16 липня 2013 року
- «Веттер проти Франції» (*Vetter v. France*), № 59842/00, 31 травня 2005 року
- «Візер енд Бікос Бетейлігунген ГмБХ проти Австрії» (*Wieser and Bicos Beteiligungen GmbH v. Austria*), № 74336/01, ЄСПЛ 2007-IV
- «Віллемс проти Нідерландів» *Willems v. the Netherlands* (ухв.), № 57294/16, 9 листопада 2021 року
- «Вінчі Констракшен та ДжіТіЕм Жені Сівіл енд Сервісіс проти Франції» (*Vinci Construction and GTM Génie Civil and Services v. France*), №№ 63629/10 і 60567/10, 02 квітня 2015 року
- «Віртшафтс-Тренд Цайтшріфтс-Ферлагсгезельшафт мБХ проти Австрії» (№ 2) (*Wirtschafts-Trend Zeitschriften-Verlagsgesellschaft mbH v. Austria (no. 2)*) (ухв.), № 62746/00, ЄСПЛ 2002-X
- «Вісент Дель Кампо проти Іспанії» (*Vicent Del Campo v. Spain*), № 25527/13, 06 листопада 2018 року
- «Віси проти Словаччини» (*Visy v. Slovakia*), № 70288/13, 16 жовтня 2018 року
- «Віссе проти Франції» (*Wisse v. France*), № 71611/01, 20 грудня 2005 року
- «Володіна проти Росії» (№ 2) (*Volodina v Russia (no. 2)*), № 40419/19, 14 вересня 2021 року
- «Вукота-Боїч проти Швейцарії» (*Vukota-Bojić v. Switzerland*), № 61838/10, 18 жовтня 2016 року
- «Вучина проти Хорватії» (*Vučina v. Croatia*) (ухв.), № 58955/13, 24 вересня 2019 року



- «Г.С.Б. проти Швейцарії» (*G.S.B. v. Switzerland*), № 28601/11, 22 грудня 2015 року
- «Гайовський проти Словаччини» (*Hájovský v. Slovakia*), № 7796/16, 01 липня 2021 року
- Галдіманн та інші проти Швейцарії (*Haldimann and Others v. Switzerland*), № 21830/09, ЄСПЛ 2015
- «Гараламбіє проти Румунії» (*Haralambie v. Romania*), № 21737/03, 27 жовтня 2009 року
- «Гардель проти Франції» (*Gardel v. France*), № 16428/05, ЄСПЛ 2009
- «Гарнага проти України» (*Garnaga v. Ukraine*), № 20390/07, 16 травня 2013 року
- «Гассін проти Румунії» (*Hassine v. Romania*), № 36328/13, 09 березня 2021 року
- «Гаф'юк проти Румунії» (*Gafiuc v. Romania*), № 59174/13, 13 жовтня 2020 року
- «Гашчак проти Словаччини» (*Haščák v. Slovakia*), №№ 58359/12 та 2 інших, 23 червня 2022 року
- «Гелфорд проти Сполученого Королівства» (*Halford v. the United Kingdom*), 25 червня 1997 року, *Збірник рішень та ухвал 1997-III*
- «Гемелеїнен проти Фінляндії» (*Hämäläinen v. Finland*) [ВП], № 37359/09, ЄСПЛ 2014
- «Генрі Кісмон проти Франції» (*Henry Kismoun v. France*), № 32265/10, 05 грудня 2013 року
- «Гійо проти Франції» (*Guillot v. France*), 24 жовтня 1996 року, *Збірник рішень та ухвал 1996-V*
- «Гірлеану проти Румунії» (*Gîrleanu v. Romania*), № 50376/09, 26 червня 2018 року
- «Гісбер та інші проти Франції» (*Giesbert and Others v. France*), №№ 68974/11 і 2 інших, 01 червня 2017 року
- «Глухін проти Росії» (*Glukhin v. Russia*), № 11519/20, 04 липня 2023 року
- «Говен-Фурні і Сілію проти Франції» (*Gauvin-Fournis and Silliau v. France*), №№ 21424/16 і 45728/17, 07 вересня 2023 року
- «Годеллі проти Італії» (*Godelli v. Italy*), № 33783/09, 25 вересня 2012 року

«Горлов та інші проти Росії» (*Gorlov and Others v. Russia*), №№ 27057/06 та 2 інших, 02 липня 2019 року
«Гоулік проти Ліхтенштейну» (*Gawlik v. Liechtenstein*), № 23922/19, 16 лютого 2021 року
«Гройтер проти Нідерландів» (*Greuter v. the Netherlands*) (ухв.), № 40045/98, 19 березня 2002 року
«Гувіг проти Франції» (*Huvig v. France*), 24 квітня 1990 року, серія А № 176-В
«Гуерра та інші проти Італії» (*Guerra and Others v. Italy*), № 14967/89, Збірник рішень та ухвал 1998-I
«Гуіоргуї Ніколаїшвілі проти Грузії» (*Guiorgui Nikolaïchvili v. Georgia*), № 37048/04, 13 січня 2009 року
«Гурбейн проти Бельгії» (*Hurbain v. Belgium*), [ВП], № 57292/16, 04 липня 2023 року
«Гьормюш та інші проти Туреччини» (*Görmüş and Others v. Turkey*), № 49085/07, 19 січня 2016 року
«Гюзель Ердагьоз проти Туреччини» (*Güzel Erdagöz v. Turkey*), № 37483/02, 21 жовтня 2008 року

—Г—

«Гаскін проти Сполученого Королівства» (*Gaskin v. the United Kingdom*), 07 липня 1989 року, Серія А № 160
«Гілан і Квінтон проти Сполученого Королівства» (*Gillan and Quinton v. the United Kingdom*), № 4158/05, ЄСПЛ 2010 (витяги)
«Гоґран проти Сполученого Королівства» (*Gaughran v. the United Kingdom*), № 45245/15, 13 лютого 2020 року
«Грант проти Сполученого Королівства» (*Grant v. the United Kingdom*), № 32570/03, ЄСПЛ 2006-VII

—Д—

«Д.Г. та інші проти Північної Македонії» (*D.H. and Others v. North Macedonia*), № 44033/17, 18 липня 2023 року
«Д.Л. проти Болгарії» (*D.L. v. Bulgaria*), № 7472/14, 19 травня 2006 року
«Даджеон проти Сполученого Королівства» (*Dudgeon v. the United Kingdom*), 22 жовтня 1981 року, Серія А № 45
«Далеа проти Франції» (*Dalea v. France*) (ухв.), № 964/07, 02 лютого 2010 року
«Девечі проти Туреччини» (*Deveci v. Türkiye*) (ухв.), № 42785/11, 28 червня 2022 року
«ДЕЛЬТА ПЕКАРНИ а.с. проти Чеської Республіки» (*DELTA PEKÁRNY a.s. v. Czech Republic*), № 97/11, 02 жовтня 2014 року
«Деміртепе проти Франції» (*Demirtepe v. France*), № 34821/97, ЄСПЛ 1999-IX (витяги)
«Дж.Л. проти Італії» (*J.L. v. Italy*), № 5671/16, 27 травня 2021 року
«Дж.П.Д. проти Франції» (*J.P.D. v. France*) (ухв.), № 55432/10, 16 вересня 2016 року
«Дж.С. проти Сполученого Королівства» (*J.S. v. the United Kingdom*) (ухв.), 445/10, 03 березня 2015 року
«Джекер проти Швейцарії» (*Jecker v. Switzerland*), № 35449/14, 06 жовтня 2020 року
«Дімітрас та інші проти Греції» (*Dimitras and Others v. Greece*), №№ 42837/06 та 4 інших, 03 червня 2010 року
«Дімітров-Казаків проти Болгарії» (*Dimitrov-Kazakov v. Bulgaria*), № 11379/03, 10 лютого 2011 року
«Доєрга проти Нідерландів» (*Doerga v. the Netherlands*), № 50210/99, 27 квітня 2004 року
«Драган Петровіч проти Сербії» (*Dragan Petrovic v. Serbia*), № 75229/10, 14 квітня 2020 року

«Драгоєвіч проти Хорватії» (*Dragojević v. Croatia*), № 68955/11, 15 січня 2015 року
«Дракшас проти Литви» (*Drakšas v. Lithuania*), № 36662/04, 31 липня 2012 року
«Дрелон проти Франції» (*Drelon v. France*), №№ 3153/16 і 27758/18, 08 вересня 2022 року
«Друкарня та видавництво проти Франції» (*Société de conception de presse et d'édition v. France*), № 4683/11, 25 лютого 2016 року
«Думітру Попеску проти Румунії» (№ 2) (*Dumitru Popescu v. Romania (no. 2)*), № 71525/01, 26 квітня 2007 року
«Дюпюї та інші проти Франції» (*Dupuis and Others v. France*), № 1914/02, 07 червня 2007 року

—Е—

«Егеланд і Гансайд проти Норвегії» (*Egeland and Hanseid v. Norway*), № 34438/04, 16 квітня 2009 року
«Едісьон Плон проти Франції» (*Éditions Plon v. France*), № 58148/00, ЄСПЛ 2004-IV
«Екімджиев та інші проти Болгарії» (*Ekimdzhiiev and Others v. Bulgaria*), № 70078/12, 11 січня 2022 року
«Еллен проти Сполученого Королівства» (*Allan v. the United Kingdom*), № 48539/99, ЄСПЛ 2002-IX
«Ельберте проти Латвії» (*Elberte v. Latvia*), № 61243/08, ЄСПЛ 2015
«Ем-Джі-Ен Лімітед проти Сполученого Королівства» (*MGN Limited v. the United Kingdom*), № 39401/04, 18 січня 2011 року
«Ердем проти Німеччини» (*Erdem v. Germany*), № 38321/97, ЄСПЛ 2001-VII (витяги)
«Ернст та інші проти Бельгії» (*Ernst and Others v. Belgium*), № 33400/96, 15 липня 2003 року
«Етерніт проти Франції» (*Eternit v. France*) (ухв.), № 20041/10, 27 березня 2012 року

—Ж—

«Жулук проти Сполученого Королівства» (*Szuluk v. the United Kingdom*), № 36936/05, ЄСПЛ 2009

—З—

«Зегерштедт-Віберг та інші проти Швеції» (*Segerstedt-Wiberg and Others v. Sweden*), № 62332/00, ЄСПЛ 2006-VII
«Z проти Фінляндії» (*Z v. Finland*), 25 лютого 1997, Збірник рішень та ухвал 1997-I
«Золтан Варга проти Словаччини» (*Zoltán Varga v. Slovakia*), №№ 58361/12 та 2 інших, 20 липня 2021
«Зоммер проти Німеччини» (*Sommer v. Germany*), № 73607/13, 27 квітня 2017 року

—І—

«І. проти Фінляндії» (*I. v. Finland*), № 20511/03, 17 липня 2008 року
«Івашченко проти Росії» (*Ivashchenko v. Russia*), № 61064/10, 13 лютого 2018 року
«Івон Шаве, в дівоцтві Жульєн, проти Франції» (*Yvonne Chave née Jullien v. France*), № 14461/88, ухвала Комісії від 9 липня 1991 року
«Х та інші проти Росії» (*X and Others v. Russia*), №№ 78042/16 і 66158/14, 14 січня 2020 року
«Іордачі та інші проти Молдови» (*Iordachi and Others v. the Republic of Moldova*), № 25198/02, 10 лютого 2009 року

«Ірфан Гюзель проти Туреччини» (*irfan Guzel v. Turkey*), № 35285/08, 07 лютого 2017 року

—Й—

«Й. проти Туреччини» (*Y. v. Turkey*) (ухв.), № 648/10, 17 лютого 2015 року

«Й.Б. та інші проти Туреччини» (*Y.B. and Others v. Turkey*), №№ 48173/99 і 48319/99, 28 жовтня 2004 року

«Й.Г. проти Росії» (*Y.G. v. Russia*), № 8647/12, 30 серпня 2022 року

«Й.Й. проти Росії» (*Y.Y. v. Russia*), № 40378/06, 23 лютого 2016 року

«Йарнеа проти Румунії» (*Jarnea v. Romania*), № 41838/05, 19 липня 2011

«Йеггі проти Швейцарії» (*Jäggi v. Switzerland*), № 58757/00, ЄСПЛ 2006-Х

«Йоанна Шульц проти Польщі» (*Joanna Szulc v. Poland*), № 43932/08, § 13 листопад 2012

«Йончев проти Болгарії» (*Yonchev v. Bulgaria*), № 12504/09, 07 грудня 2017 року

—К—

«К.Г. та інші проти Словаччини» (*K.H. and Others v. Slovakia*), № 32881/04, ЄСПЛ 2009 (витяги)

«К.К. проти Іспанії» (*C.C. v. Spain*), № 1425/06, 06 жовтня 2009 року

«К.С. та М.С. проти Німеччини» (*K.S. and M.S. v. Germany*), № 33696/11, 06 жовтня 2016 року

«К.У. проти Фінляндії» (*K.U. v. Finland*), № 2872/02, ЄСПЛ 2008

«Какісісой та інші проти Кіпру» (*Cakicisoy and Others v. Cyprus*) (ухв.), № 6523/12, 23 вересня 2014 року

«Кан проти Німеччини» (*Kahn v. Germany*), № 16313/10, 17 березня 2016 року

«Канонн проти Франції» (*Canonne v. France*) (ухв.), № 22037/13, 02 червня 2015 року

«Карабейоглу проти Туреччини» (*Karabeyoğlu v. Turkey*), № 30083/10, 07 червня 2016 року

«Каруана проти Мальти» (*Caruana v. Malta*) (ухв.), № 41079/16, 15 травня 2018 року

«Качмарек проти Польщі» (*Kaczmarek v. Poland*), № 16974/14, 22 лютого 2024 року

«Квасніца проти Словаччини» (*Kvasnica v. Slovakia*), № 72094/01, 09 червня 2009 року

«Кеват Озель проти Туреччини» (*Cevat Özel v. Turkey*), № 19602/06, 07 червня 2016 року

«Кемалеттін Канлі проти Туреччини» (*Cemalettin Canli v. Turkey*), № 22427/04, 18 листопада 2008 року

«Кеннеді проти Сполученого Королівства» (*Kennedy v. the United Kingdom*), № 26839/05, 18 травня 2010 року

«Кетт проти Сполученого Королівства» (*Catt v. the United Kingdom*), № 43514/15, 24 січня 2019 року

«Кіннунен проти Фінляндії» (*Kinnunen v. Finland*), № 18291/91, ухвала Комісії, 13 жовтня 1993 року

«Кіннунен проти Фінляндії» (*Kinnunen v. Finland*), № 24950/94, ухвала Комісії, 15 травня 1996 року

«Кірдьок та інші проти Туреччини» (*Kirdök and Others v. Turkey*), № 14704/12, 3 грудня 2019 року

«Кіютін проти Росії» (*Kiyutin v. Russia*), № 2700/10, ЄСПЛ 2011

«Класс та інші проти Німеччини» (*Klass and Others v. Germany*), 06 вересня 1978 року, Серія А № 28

«Кобан проти Іспанії» (*Coban v. Spain*) (ухв.), № 17060/02, 25 вересня 2006 року

«Коновалова проти Росії» (*Konovlova v. Russia*), № 37873/04, 09 жовтня 2014 року

«Копленд проти Сполученого Королівства» (*Copland v. the United Kingdom*), № 62617/00, ЄСПЛ 2007-I

«Коссі проти Сполученого Королівства» (*Cossey v. the United Kingdom*), 27 вересня 1990, Серія А № 184

- «Котілайнен та інші проти Фінляндії» (*Kotilainen and Others v. Finland*), № 62439/12, 17 вересня 2020 року
- «Краксі проти Італії (№ 2)» (*Craxi v. Italy (no. 2)*), № 25337/94, 17 липня 2003
- «Крістін Гудвін проти Сполученого Королівства» (*Christine Goodwin v. the United Kingdom*) [ВП], № 28957/95, ЄСПЛ 2002-VI
- «Кроне Ферлаг ГмбХ унд Ко. КГ проти Австрії» (*Krone Verlag GmbH & Co. KG v. Austria*), № 34315/96, 26 лютого 2002 року
- «Круглов та інші проти Росії» (*Kruglov and Others v. Russia*), №№ 11264/04 та 15 інших, 04 лютого 2020 року
- «Круслін проти Франції» (*Kruslin v. France*), 24 квітня 1990 року, серія А № 176-A
- «Кур'єр Цайтунгсферлаг унд Друкерай ГмбХ проти Австрії» (*Kurier Zeitungsverlag und Druckerei GmbH v. Austria*), № 3401/07, 17 січня 2012 року
- «Кхан проти Сполученого Королівства» (*Khan v. the United Kingdom*), № 35394/97, ЄСПЛ 2000-V
- «Кьопке проти Німеччини» (*Körke v. Germany*) (ухв.), № 420/07, 05 жовтня 2010 року

—Л—

- «Л.Б. проти Угорщини» (*L.B. v. Hungary*) [ВП], № 36345/16, 09 березня 2023 року
- «Л.Г. проти Латвії» (*L.H. v. Latvia*), № 52019/07, 29 квітня 2014 року
- «Л.Л. проти Франції» (*L.L. v. France*), № 7508/02, ЄСПЛ 2006-XI
- «Л.Ф. проти Франції» (*L.F. v. France*) (ухв.), №№ 3866/20 і 9292/20, 13 лютого 2024 року
- «Лабіта проти Італії» (*Labita v. Italy*) [ВП], № 26772/95, ЄСПЛ 2000-IV
- «Лавенц проти Латвії» (*Lavents v. Latvia*), № 58442/00, 28 листопада 2002 року
- «Ламберт проти Франції» (*Lambert v. France*), № 23618/94, Збірник рішень та ухвал 1998-V
- «Леандер проти Швеції» (*Leander v. Sweden*), 26 березня 1987 року, серія А № 116
- «Ліберт проти Франції» (*Libert v. France*), № 588/13, 22 лютого 2018 року
- «Ліберті та інші проти Сполученого Королівства» (*Liberty and Others v. the United Kingdom*), № 58243/00, 1 липня 2008
- «Ліблік та інші проти Естонії» (*Liblik and Others v. Estonia*), № 173/15 та 5 інших, 28 травня 2019 року
- «Лібшер проти Австрії» (*Liebscher v. Austria*), № 5434/17, 06 квітня 2021 року
- «Лопез Рібалда та інші проти Іспанії» (*López Ribalda and Others v. Spain*) [ВП], №№ 1874/13 і 8567/13, 17 жовтня 2019 року
- «Лупкер та інші проти Нідерландів» (*Lupker and Others v. the Netherlands*), 18395/91, ухвала Комісії, 07 грудня 1992 року
- «Люді проти Швейцарії» (*Lüdi v. Switzerland*), № 12433/86, Серія А № 238

—М—

- «М.Б. проти Франції» (*M.B. v. France*), № 22115/06, 17 грудня 2009 року
- «М.Г. проти Сполученого Королівства» (*M.G. v. the United Kingdom*), № 39393/98, 24 вересня 2002 року
- «М.Д. та інші проти Іспанії» (*M.D. and Others v. Spain*), № 36584/17, 28 червня 2022 року
- «М.К. проти Сполученого Королівства» (*M.C. v. the United Kingdom*), № 51220/13, 30 березня 2021 року
- «М.К. проти Франції» (*M.K. v. France*), № 19522/09, 18 квітня 2013 року
- «М.Л. та В.В. проти Німеччини» (*M.L. and W.W. v. Germany*), №№ 60798/10 і 65599/10, 28 червня 2018 року

- «М.М. проти Сполученого Королівства» (*M.M. v. the United Kingdom*), № 24029/07, 13 листопада 2012 року
- «М.Н. та інші проти Сан-Марино» (*M.N. and Others v. San Marino*), № 28005/12, 7 липня 2015
- «М.П. проти Португалії» (*M.P. v. Portugal*), № 27516/14, 7 вересня 2021 року
- «М.С. проти Швеції» (*M.S. v. Sweden*), 27 серпня 1997 року, *Доповіді про рішення та ухвали* 1997-IV
- «Мадяр Гельсінкі Бізотцаг проти Угорщини» (*Magyar Helsinki Bizottság v. Hungary* [ВП], № 18030/11, ЄСПЛ 2016
- «Маквей, Оніл та Еванс проти Сполученого Королівства» (*McVeigh, O'Neill and Evans v. the United Kingdom*), №№ 8022/77 і два інших, звіт Комісії, 18 березня 1981 року
- «Макгінлі та Еган проти Сполученого Королівства» (*McGinley and Egan v. the United Kingdom*), 09 червня 1998 року, *Збірник рішень та ухвал* 1998-III
- «Маланічева проти Росії» (*Malanicheva v. Russia*) (ухв.), № 50405/06, 31 травня 2016 року
- «Малоун проти Сполученого Королівства» (*Malone v. the United Kingdom*), 02 серпня 1984 року, Серія А № 82
- «Маргарі проти Греції» (*Margari v. Greece*), № 36705/16, 20 червня 2023 року
- «Маркіані проти Франції» (*Marchiani v. France*) (ухв.), № 30392/03, 27 травня 2008 року
- «Матерон проти Франції» (*Matheron v. France*), № 57752/00, 29 березня 2005 року
- «Медіенгруппе Остеррайх ГмБХ проти Австрії» (*Mediengruppe Österreich GmbH v. Austria*), № 37718/18, 26 квітня 2022 року
- «Ментзен проти Латвії» (*Mentzen v. Latvia*) (ухв.), № 71074/01, ЄСПЛ 2004-XII
- «Мессіна проти Італії» (№ 2) (*Messina v. Italy (no. 2)*), № 25498/94, ЄСПЛ 2000-X
- «Мехмедович проти Швейцарії» (*Mehmedovic v. Switzerland*) (ухв.), № 17331/11, 11 грудня 2018 року
- «Мік і Джовановіч проти Сербії» (*Mik and Jovanovic v. Serbia*) (ухв.), №№ 9291/14 і 63798/14, 23 березня 2021 року
- «Мікуліч проти Хорватії» (*Mikulić v. Croatia*), № 53176/99, ЄСПЛ 2002-I
- «Мітов та інші проти Болгарії» (*Mitov and Others v. Bulgaria*) (ухв.), № 80857/17, 28 лютого 2023 року
- «Мітянін і Леонов проти Росії» (*Mityanin and Leonov v. Russia*), №№ 11436/06 і 22912/06, 07 травня 2018 року
- «Міфсуд проти Мальти» (*Mifsud v. Malta*), № 62257/15, 29 січня 2019 року
- «Мішоод проти Франції» (*Michaud v. France*), № 12323/11, ЄСПЛ 2012
- «Модесту проти Греції» (*Modestou v. Greece*), № 51693/13, 16 березня 2017 року
- «Мозлі проти Сполученого Королівства» (*Mosley v. the United Kingdom*), № 48009/08, 10 травня 2011 року
- «Моккуте проти Литви» (*Mockutė v. Lithuania*), № 66490/09, 27 лютого 2018 року
- «Молдован проти України» (*Moldovan v. Ukraine*), № 62020/14, 14 березня 2024 року
- «Молодіжна ініціатива за права людини проти Сербії» (*Youth Initiative for Human Rights v. Serbia*), № 48135/06, 25 червня 2013 року
- «Монтера проти Італії» (*Montera v. Italy*) (ухв.), № 64713/01, 09 липня 2002 року
- «Москальов проти Росії» (*Moskalev v. Russia*), № 44045/05, 07 листопада 2017 року
- «Муртазалиєва проти Росії» (*Murtazaliyeva v. Russia*) [ВП], № 36658/05, 18 грудня 2018 року
- «Мустафа Сезгін Танрікулу проти Туреччини» (*Mustafa Sezgin Tanrikulu v. Turkey*), № 27473/06, 18 липня 2017 року
- «Мюррей проти Сполученого Королівства» (*Murray v. the United Kingdom*) [ВП], 28 жовтня 1994 року, Серія А № 300-A

—Н—

- «Н.Ф. та інші проти Росії» (*N.F. and Others v. Russia*), № 3537/15 і 8 інших, 12 вересня 2023 року
- «Н.Ш. проти Хорватії» (*N.Š. v. Croatia*), № 36908/13, 10 вересня 2020 року
- «Нагла проти Латвії» (*Nagla v. Latvia*), № 73469/10, 16 липня 2013 року
- «Нада проти Швейцарії» (*Nada v. Switzerland*) [ВП], № 10593/08, ЄСПЛ 2012
- «Національна федерація асоціацій і спілок спортсменів та інші проти Франції» (*National Federation of Sportspersons' Associations and Unions (FNASS) and Others v. France*), №№ 48151/11 і 77769/13, 18 січня 2018 року
- «Негру проти Республіки Молдова» (*Negru v. the Republic of Moldova*), № 7336/11, 27 червня 2023 року
- «Недбала проти Польщі» (*Niedbala v. Poland*), № 27915/95, 4 липня 2000 року
- «Нух Узун та інші проти Туреччини» (*Nuh Uzun and Others v. Turkey*), №№ 49341/18 і далі, 29 березня 2022 року
- «Ньюз Ферлагс ГмБХ і Ко. КГ проти Австрії» (*News Verlags GmbH & Co.KG v. Austria*), № 31457/96, ЄСПЛ 2000-I

—О—

- «Одієвре проти Франції» (*Odièvre v. France*) [ВП], № 42326/98, ЄСПЛ 2003-III
- «Олейнік проти Росії» (*Oleynik v. Russia*), № 23559/07, 21 червня 2016 року

—П—

- «П. і Б. проти Сполученого Королівства» (*P. and B. v. the United Kingdom*), № 36337/97 і 35974/97, ЄСПЛ 2001-III
- «П. і С. проти Польщі» (*P. and S. v. Poland*), № 57375/08, 30 жовтня 2012 року
- «П.Г. і Дж.Г. проти Сполученого Королівства» (*P.G. and J.H. v. the United Kingdom*), № 44787/98, ЄСПЛ 2001-IX
- «П.Н. проти Німеччини» (*P.N. v. Germany*), № 74440/17, 11 червня 2020 року
- «П.Т. проти Республіки Молдова» (*P.T. v. the Republic of Moldova*), № 1122/12, 26 травня 2020 року
- «Пантелеєнко проти України» (*Panteleyenko v. Ukraine*), № 11901/02, 29 червня 2006 року
- «Пеерс проти Греції» (*Peers v. Greece*), № 28524/95, ЄСПЛ 2001-III
- «Пек проти Сполученого Королівства» (*Peck v. the United Kingdom*), № 44647/98, ЄСПЛ 2003-I
- «Пендов проти Болгарії» (*Pendov v. Bulgaria*), № 44229/11, 26 березня 2020 року
- «Перрі проти Сполученого Королівства» (*Perry v. the United Kingdom*), № 63737/00, ЄСПЛ 2003-IX (витяги)
- «Перуззо і Мартенс проти Німеччини» (*Peruzzo and Martens v. Germany*) (ухв.), №№ 7841/08 і 57900/12, 04 червня 2013 року
- «Петрова проти Латвії» (*Petrova v. Latvia*), № 4605/05, 24 червня 2014 року
- «Пінто Коельйо проти Португалії» (№ 2) (*Pinto Coelho v. Portugal (no. 2)*), № 48718/11, 22 березня 2016 року
- «Подчасов проти Росії» (*Podchasov v. Russia*), № 33696/19, 13 лютого 2024 року
- «Поланко Торрес і Мовілла Поланко проти Іспанії» (*Polanco Torres and Movilla Polanco v. Spain*), № 34147/06, 21 вересня 2010 року
- «Прадо Бугалло проти Іспанії» (*Prado Bugallo v. Spain*), № 58496/00, 18 лютого 2003 року
- «Прутеану проти Румунії» (*Pruteanu v. Romania*), № 30181/05, 03 лютого 2015 року

«Пьотржак і Бичавська-Синярьська та інші проти Польщі» (*Pietrzak and Bychawska-Siniarska and Others v. Poland*), №№ 72038/17 та 25237/18, 18 травня 2024 року

— P —

«Р.Е. проти Сполученого Королівства» (*R.E. v. the United Kingdom*), № 62498/11, 27 жовтня 2015 року

«Радіо Твіст а.с. проти Словаччини» (*Radio Twist a.s. v. Slovakia*), № 62202/00, ЄСПЛ 2006-XV

«Раду проти Республіки Молдова» (*Radu v. the Republic of Moldova*), № 50073/07, 15 квітня 2014 року

«Рамадан проти Франції» (*Ramadan v. France*) (ухв.), № 23443/23, 09 січня 2024 року

«Редакція «Правоє діло» і Штекель проти України» (*Editorial Board of Pravoye Delo and Shtekel v. Ukraine*), № 33014/05, ЄСПЛ 2011 (витяги)

«Реклос та Давурліс проти Греції» (*Reklos and Davourlis v. Greece*), № 1234/05, 15 січня 2009 року

«Різ проти Сполученого Королівства» (*Rees v. the United Kingdom*), № 9532/81, Серія А № 106

«Річчі проти Італії» (*Ricci v. Italy*), № 30210/06, 08 жовтня 2013 року

«Робатін проти Австрії» (*Robathin v. Austria*), № 30457/06, 03 липня 2012 року

«Роемен і Шміт проти Люксембургу» (*Roemen and Schmit v. Luxembourg*), № 26419/10, ЄСПЛ 2003-IV

«Роман Захаров проти Росії» (*Roman Zakharov v. Russia*) [ВП], № 47143/06, ЄСПЛ 2015

«Ротару проти Румунії» (*Rotaru v. Romania*) [ВП], № 28341/95, ЄСПЛ 2000-V

«Роше проти Сполученого Королівства» (*Roche v. the United Kingdom*) [ВП], № 32555/96, ЄСПЛ 2005-X

«Рук проти Німеччини» (*Rook v. Germany*), № 1586/15, 25 липня 2019 року

— C —

«С. і Марпер проти Сполученого Королівства» (*S. and Marper v. the United Kingdom*) [ВП], №№ 30562/04 і 30566/04, ЄСПЛ 2008

«С.В. проти Італії» (*S.V. v. Italy*), № 55216/08, 11 жовтня 2018 року

«Самойлова проти Росії» (*Samoylova v. Russia*), № 49108/11, 14 грудня 2021 року

«Саномат Уйтгеверс Б.В. проти Нідерландів» (*Sanoma Uitgevers B.V. v. the Netherlands*) [ВП], № 38224/03, 14 вересня 2010 року

«Сарбу проти Румунії» (*Sârbu v. Romania*), № 34467/15, 28 березня 2023 року

«Сатакуннан Марккінапорссі Ой та Сатамедіа Ой проти Фінляндії» (*Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*) [ВП], № 931/13, ЄСПЛ 2017 (витяги)

«Свідки Єгови проти Фінляндії» (*Jehovah's Witnesses v. Finland*), № 31172/19, 09 травня 2023 року

«Седлецька проти України» (*Sedletska v. Ukraine*), № 42634/18, 01 квітня 2021 року

«Сексешен Крестен Фільтенборг Мортесен проти Данії» (*Succession Kresten Filtenborg Mortensen v. Denmark*) (ухв.), № 1338/03, ЄСПЛ 2006-V

«Сервуло енд Ассосіадос — Сосьєдад де Адвогадос, РЛ та інші проти Португалії» (*Sérvulo & Associados - Sociedade de Advogados, RL and Others v. Portugal*), № 27013/10, 03 вересня 2015 року

«Сергава проти Естонії» (*Särgava v. Estonia*), № 698/19, 16 листопада 2021 року

«Сілвер та інші проти Сполученого Королівства» (*Silver and Others v. the United Kingdom*), 25 березня 1983 року, Серія А № 61

«Сінан Ішик проти Туреччини» (*Sinan Işık v. Turkey*), № 21924/05, ЄСПЛ 2010

«Смірнов проти Росії» (*Smirnov v. Russia*), № 71362/01, 07 червня 2007 року

«Сміт і Грейді проти Сполученого Королівства» (*Smith and Grady v. the United Kingdom*), № 33985/96 і 33986/96, Збірник рішень та ухвал 1999-VI
«Соро проти Естонії» (*Sõro v. Estonia*), № 22588/08, 03 вересня 2015 року
«Столкоса проти Польщі» (*Stolkosa v. Poland*) (ухв.), № 68562/14, 14 вересня 2021 року
«Супруненко проти Росії» (*Suprunenko v. Russia*) (ухв.), № 8630/11, 19 червня 2018 року
«Суріков проти України» (*Surikov v. Ukraine*), № 42788/06, 26 січня 2017 року
«Сціацца проти Італії» (*Sciacca v. Italy*), № 50774/99, ЄСПЛ 2005-I
«Сьодерман проти Швеції» (*Söderman v. Sweden*) [ВП], № 5786/08, ЄСПЛ 2013

—Т—

«Таймз Н'юзпейперс Лтд проти Сполученого Королівства» (№№ 1 і 2) (*Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2)*), №№ 3002/03 і 23676/03, ЄСПЛ 2009
«Тейлор-Саборі проти Сполученого Королівства» (*Taylor-Sabori v. the United Kingdom*), № 47114/99, 22 жовтня 2002 року
«Телеграф Медіа Недерланд Ланделійке Медіа Б.В. та інші проти Нідерландів» (*Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*), № 39315/06, 22 листопада 2012 року
«Тена Аррегуї проти Іспанії» (*Tena Arregui v. Spain*), № 42541/18, 11 січня 2024 року
«Тіллак проти Бельгії» (*Tillack v. Belgium*), 20477/05, 27 листопада 2007 року
«Тома проти Люксембургу» (*Thoma v. Luxembourg*), № 38432/97, ЄСПЛ 2001-III
«Тома проти Румунії» (*Thoma v. Romania*), № 42716/02, 24 лютого 2009 року
«Тонсбергс Блад А.С. і Гауком проти Норвегії» (*Tønsbergs Blad A.S. and Haukom v. Norway*), № 510/04, 01 березня 2007 року
«Тончев проти Болгарії» (*Tonchev v. Bulgaria*), № 40519/15, 16 квітня 2024 року
«Трабайо Руеда проти Іспанії» (*Trabajo Rueda v. Spain*), № 32600/12, 30 травня 2017 року
«Трайковські та Чіповські проти Північної Македонії» (*Trajkovski and Chipovski v. North Macedonia*), №№ 53205/13 і 63320/13, 13 лютого 2020 року

—у—

«Узун проти Німеччини» (*Uzun v. Germany*), № 35623/05, ЄСПЛ 2010 (витяги)
«Унгвари енд Іродалом Кфт. проти Угорщини» (*Ungváry and Irodalom Kft. v. Hungary*), № 64520/10, 03 грудня 2013 року

—Ф—

«Файненшіал Таймз Лтд та інші проти Сполученого Королівства» (*Financial Times Ltd and Others v. the United Kingdom*), № 821/03, 15 грудня 2009 року
«Ферлагсгруппе Дрьомер Кнаур ГмбХ унд Ко. КГ проти Німеччини» (*Verlagsgruppe Droemer Knauer GmbH & Co. KG v. Germany*), № 35030/13, 19 жовтня 2017 року
«Флоріндо де Альмейда Васконселос Грамаксо проти Португалії» (*Florindo de Almeida Vasconcelos Gramacho v. Portugal*), № 26968/16, 13 грудня 2022 року
«Фокслі проти Сполученого Королівства» (*Foxley v. the United Kingdom*), № 33274/96, 20 червня 2000 року
«Фон Ганновер проти Німеччини» (№ 2) (*Von Hannover v. Germany (no.2)*) [ВП], №№ 40660/08 і 60641/08, ЄСПЛ 2012
«Фон Ганновер проти Німеччини» (*Von Hannover v. Germany*), № 59320/00, ЄСПЛ 2004-VI
«Францу проти Румунії» (*Frâncu v. Romania*), № 69356/13, 13 жовтня 2020 року

[«Фрідл проти Австрії» \(Friedl v. Austria\)](#), № 15225/89, доповідь Комісії, 19 травня 1994 року

—X—

[«Хадіджа Ісмаїлова проти Азербайджану» \(Khadija Ismayilova v. Azerbaijan\)](#), №№ 65286/13 і 57270/14, 10 січня 2019 року

[«Хеглас проти Чеської Республіки» \(Heglas v. Czech Republic\)](#), № 5935/02, 01 березня 2007 року

[«Хелілі проти Швейцарії» \(Khelili v. Switzerland\)](#), № 16188/07, 18 жовтня 2011 року

[«Хмель проти Росії» \(Khmel v. Russia\)](#), № 20383/04, 12 грудня 2013 року

[«Хужин та інші проти Росії» \(Khuzhin and Others v. Russia\)](#), № 13470/02, 23 жовтня 2008 року

—Ц—

[«Центр демократії та верховенства права проти України» \(Centre for Democracy and the Rule of Law v. Ukraine\)](#), № 10090/16, 26 березня 2020 року

[«Центр правосуддя проти Швеції» \(Centrum för rättvisa v. Sweden\)](#) [ВП], № 35252/08, 25 травня 2021 року

—Ч—

[«Чаботару проти Молдови» \(Ciubotaru v. Moldova\)](#), № 27138/04, 27 квітня 2010 року

—Ш—

[«Шабо та Вісси проти Угорщини» \(Szabó and Vissy v. Hungary\)](#), № 37138/14, 12 січня 2016 року

[«Шантаре та Лабазніковс проти Латвії» \(Šantare and Labazņikovs v. Latvia\)](#), № 34148/07, 31 березня 2016 року

[«Шер та інші проти Сполученого Королівства» \(Sher and Others v. the United Kingdom\)](#), № 5201/11, ЄСПЛ 2015 (витяги)

[«Шерр'єр проти Франції» \(Cherrier v. France\)](#), № 18843/20, 30 січня 2024 року

[«Шеффілд і Горшем проти Сполученого Королівства» \(Sheffield and Horsham v. the United Kingdom\)](#), 30 липня 1998, *Збірник рішень та ухвал 1998-V*

[«Шимоволос проти Росії» \(Shimovolos v. Russia\)](#), № 30194/09, 21 червня 2011 року

[«Шмідт проти Німеччини» \(Schmidt v. Germany\)](#) (ухв.), № 32352/02, 05 січня 2006 року

[«Штандард Ферлагсгезельшафт мБХ проти Австрії» \(№ 3\) \(Standard Verlagsgesellschaft mbH v. Austria \(no. 3\)\)](#), № 39378/15, 07 грудня 2021 року