

Обставини справи

Заявник Nikolay Sergeyevich Glukhin є громадянином росії, 1985 року народження, проживає в місті Москві.

23 серпня 2019 року заявник провів одиночний пікет на підтримку іншого політичного активіста – пана Kotov, проїхавшись в московському метро з картонною фігурою останнього в людський зріст та банером: «Ви мабуть жартуєте... Мені загрожує до п'яти років за 212.1 за мирні протести». Справа пана Kotov до того викликала суспільний резонанс і привернула широку увагу в ЗМІ.

Під час звичайного відслідковування мережі Інтернет поліція виявила фотографії та відео пікету заявника у метро, завантажені на загальнодоступному сайті соціальної мережі. За словами пана Glukhin, поліція ймовірно використовувала технологію розпізнавання обличчя. Щоб ідентифікувати його за скріншотами з сайту соціальної мережі, працівники поліції зібрали кадри з системи закритої трансляції телебачення – камер відеоспостереження, встановлених на станціях московського метро, через які він проїхав 23 серпня 2019 року, і через кілька днів використали технологію розпізнавання обличчя в реальному часі, щоб знайти та заарештувати його, коли він їхав у метро.

В подальшому заявник був визнаний винним у провадженні в справі про адміністративні правопорушення за неповідомлення органів влади про його одиночний пікет з використанням «предмета, який швидко розбирається». Скріншоти сайту соціальної мережі та відеозаписи з камер відеоспостереження були використані як докази проти нього.

30 жовтня 2019 року Московський міський суд в апеляційному порядку підтримав обвинувачення заявника, визнавши, зокрема, що мирний характер його демонстрації не мав значення, і що правопорушення було виявлено, а докази зібрані відповідно до Закону «Про поліцію».

У період з 2017 по 2022 рік у Москві було встановлено понад 220 000 камер відеоспостереження, у тому числі в московському метрополітені після набрання чинності указу уряду про транспортну безпеку (Указ № 410 від 5 квітня 2017 року). Всі вони оснащені технологією розпізнавання обличчя в реальному часі.

Заявник скаржився, що його визнання винним у вчиненні адміністративного правопорушення та використання технології розпізнавання обличчя при обробці його персональних даних порушило його права відповідно до статей 8 (право на повагу до приватного і сімейного життя) та 10 Конвенції (свобода вираження поглядів).

Крім того, посилаючись на статтю 6 Конвенції (право на справедливий суд), він скаржився, що провадження проти нього було несправедливим з причин відсутності сторони обвинувачення.

Оцінка Суду

Стаття 10 Конвенції

ЄСПЛ вважав, що заявник прагнув висловити свою думку з питання, що становить суспільний інтерес, і що було мало підстав для обмеження цього права відповідно до статті 10 Конвенції.

Органи влади, однак, не виявили терпимості до його одиночного пікету, який, безперечно, був мирним і не спричинив жодної небезпеки для громадського порядку чи безпеки. Дійсно, вони взагалі не надали оцінку, чи використання заявником картонної фігури з плакатом було вираженням його поглядів.

Таким чином, національні суди не надали «відповідних або достатніх підстав» для виправдання супроводу заявника до поліцейської дільниці, його арешту та обвинувачення, порушивши його право на свободу вираження поглядів відповідно до статті 10 Конвенції.

Стаття 8 Конвенції

(а) Існування втручання

(і) Загальні принципи

ЄСПЛ нагадав, що поняття «приватне життя» є широким поняттям, яке не піддається вичерпному визначенню. Воно може охоплювати множинні аспекти фізичної та соціальної ідентичності людини. Таке поняття не обмежується «найближчим оточенням», в якому індивід може жити власним особистим життям без втручання ззовні, але також включає в себе право вести «приватне соціальне життя», тобто можливість встановлення та розвитку відносин з іншими та зовнішнім світом. Воно не виключає діяльність, що відбувається в публічному контексті. Таким чином, існує площина взаємодії особи з іншими, навіть у публічному контексті, яка може підпадати під сферу «приватного життя» (див. *López Ribalda and Others v. Spain* [ВП]) (п. 64 рішення).

Саме лише зберігання даних, що стосуються приватного життя фізичної особи, є втручанням у розумінні статті 8 Конвенції. Подальше використання збереженої інформації не має жодного відношення до цього висновку. Однак при визначенні того, чи стосується особиста інформація, що зберігається органами влади, будь-якого з аспектів приватного життя, згаданих вище, Суд належним чином враховує конкретний контекст, в якому ця інформація була зафіксована та збережена, характер записів, спосіб використання та обробки цих записів та результати, які можуть бути отримані (див. *S. and Marper v. the United Kingdom* [ВП]) (п. 65 рішення).

Оскільки існують випадки, коли люди свідомо або навмисно беруть участь у заходах, які є або можуть бути записані чи про які повідомлялося публічно, обґрунтовані очікування особи щодо конфіденційності можуть бути значними, хоча і не обов'язково остаточним фактором у цій оцінці. **Що стосується моніторингу дій фізичної особи за допомогою фото або відеопристроїв, інституції Конвенції вважають, що моніторинг дій та переміщень фізичної особи в громадському місці за допомогою камери, яка не записувала візуальні дані, сам по собі не є формою втручання в**

приватне життя. Однак міркування щодо приватного життя можуть виникнути, як тільки з'явиться будь-який систематичний або постійний запис таких персональних даних, зокрема фотографії ідентифікованої особи. Образ людини є одним з головних атрибутів її особистості, оскільки він розкриває унікальні характеристики людини та відрізняє її від інших. Таким чином, право кожної особи на захист свого образу є однією з найважливіших складових розвитку особистості і передбачає право контролювати використання цього зображення. Хоча в більшості випадків право контролювати таке використання передбачає можливість для фізичної особи відмовитися від публікації свого зображення, воно також охоплює право фізичної особи заперечувати проти запису, збереження та відтворення зображення іншою особою (див. López Ribalda and Others, згадане вище, § 89, з подальшими посиланнями) (п. 66 рішення).

Як вже раніше зазначав ЄСПЛ, збір та зберігання органами влади даних про конкретних осіб становить втручання в приватне життя цих осіб, навіть якщо ці дані стосувалися виключно громадської діяльності особи (див. Amann v. Switzerland [ВП] та Rotaru v. Romania [ВП]), такі як участь в антиурядових демонстраціях (див. Association «21 December 1989» and Others v. Romania та Catt v. the United Kingdom). Суд також встановив, що наступні випадки збору даних у громадському місці становили втручання в приватне життя осіб: запис допиту в громадській зоні поліцейської дільниці (див. P.G. and J.H. v. the United Kingdom); запис камерами відеоспостереження в громадському місці та подальше розкриття відеоматеріалу засобом масової інформації (див. Peck v. the United Kingdom); запис відеоматеріалу в поліцейській дільниці та його подальше використання в кримінальному провадженні (див. Perry v. the United Kingdom (витяги)); збір за допомогою GPS-пристрою, прикріпленого до автомобіля особи, та зберігання даних про місцезнаходження та переміщення цієї особи в публічній сфері (див. Uzun v. Germany (витяги), та Ben Faiza v. France); реєстрація імені особи в поліцейській базі даних, яка автоматично збирала та обробляла інформацію про пересування цієї особи потягом або повітряним транспортом (див. Shimovolos v. Russia); і відеоспостереження за університетськими амфітеатрами в державному університеті (див. Antović and Mirković v. Montenegro) (п. 67 рішення).

(ii) Застосування до цієї справи

Уряд не заперечував, що фактичні обставини, описані вище, становлять «втручання» у право заявника на повагу до його приватного життя відповідно до статті 8 Конвенції. Зокрема, незважаючи на конкретне запитання Суду з цього питання, вони не прокоментували твердження заявника про те, що технологія розпізнавання обличчя була використана, по-перше, для ідентифікації його за фотографіями та відео, опублікованими в Telegram, і, по-друге, для визначення його місцезнаходження та арешту, коли він їздив у московському метро. Суд врахував труднощі, з якими зіткнувся заявник при доведенні своїх тверджень. Дійсно, національне законодавство, доступне Суду, не вимагало від поліції робити запис про використання ними технології розпізнавання обличчя або надавати відповідній особі доступ до будь-якого такого запису автоматично або за запитом (див. пункт

40, що описує практику використання технології розпізнавання обличчя без будь-якого офіційного запису) (п. 69 рішення).

На цьому тлі та беручи до уваги труднощі для заявника довести свої твердження, оскільки національне законодавство не передбачало офіційного запису або повідомлення про використання технології розпізнавання обличчя, відсутність будь-якого іншого пояснення швидкої ідентифікації заявника та неявне визнання Урядом використання технології розпізнавання обличчя в реальному часі, Суд погодився з тим, що в конкретних обставинах справи була використана технологія розпізнавання обличчя. Раніше Суд встановив, що зберігання фотографій поліцією в поєднанні з можливістю застосування до них методів розпізнавання обличчя є втручанням у право на приватне життя (див. *Gaughran v. the United Kingdom*) (п. 72 рішення).

ЄСПЛ дійшов висновку, що обробка персональних даних заявника в рамках провадження в справі про адміністративне правопорушення проти нього, включаючи використання технології розпізнавання обличчя – по-перше, для ідентифікації його за фотографіями та відео, опублікованими в Telegram, і, по-друге, для визначення його місцезнаходження та арешту пізніше, коли він пересувався у московському метро становило втручання у його право на повагу до його приватного життя в розумінні пункту 1 статті 8 Конвенції (п. 73 рішення).

(b) Обґрунтування втручання

(i) Загальні принципи

ЄСПЛ повторно зазначив, що будь-яке втручання може бути виправдане відповідно до пункту 2 статті 8 Конвенції лише в тому випадку, якщо воно відповідає закону, переслідує одну або кілька передбачених її положеннями законних цілей і є необхідним у демократичному суспільстві для досягнення будь-якої такої мети (див. *Roman Zakharov v. Russia* [ВП]).

Особисті дані, що розкривають політичні погляди, такі, як інформація про участь у мирних акціях протесту, підпадають під спеціальні категорії конфіденційних даних, що потребують підвищеного рівня захисту (див. *Catt*, цит. вище, §§ 112 та 123). Тому в контексті збору та обробки персональних даних важливо мати чіткі, детальні правила, що регулюють обсяг та застосування заходів, а також мінімальні гарантії, що стосуються, зокрема, тривалості, зберігання, використання, доступу третіх сторін, процедур збереження цілісності та конфіденційності даних та процедур їх знищення, що слугує належним запобіжником зловживань та свавілля (див. *S. and Marper*, цитовані вище, § 99, та *P.N. v. Germany*) (пункти 76, 77 рішення).

(ii) Застосування до цієї справи

На думку ЄСПЛ в цій справі питання законності та існування законної мети не могли бути відокремлені від питання про те, чи було втручання «необхідним у демократичному суспільстві» (див. *S. та Marper*, згадане вище, § 99; *Nemtsov v. Russia* та *Elvira Dmitriyeva v. Russia*). Тому Суд розглянув їх разом нижче (п. 78 рішення).

На думку національних органів влади та Уряду, заходи, вжиті проти заявника, мали правову основу в КпАП, Законі «Про оперативно-розшукову діяльність», Законі про поліцію та Указі № 410.

ЄСПЛ розпочав з того, що оперативно-розшукова діяльність може здійснюватися лише у зв'язку із правопорушенням, кваліфікованим як «кримінальне» відповідно до національного законодавства (див. пункт 24). Таким чином, Закон «Про оперативно-розшукову діяльність» не міг слугувати правовою підставою для заходів, вжитих у цій справі, яка стосувалася адміністративного правопорушення.

Як КпАП, так і Закон про поліцію надали поліції повноваження розслідувати адміністративні правопорушення та збирати докази, включаючи докази, що містять персональні дані (див. пункти 26-29). Указ № 410 передбачав встановлення камер відеоспостереження з функцією розпізнавання обличчя у московському метро, які були доступні для поліції (див. пункти 33-34). Таким чином, Суд визнав, що заходи, вжиті проти заявника, мали правову основу у національному законодавстві (п. 81 рішення).

Оскільки заявник стверджував, що національне законодавство не відповідає вимозі «якості закону», Суд вважав, що в контексті впровадження технології розпізнавання обличчя важливо мати детальні правила, що регулюють обсяг та застосування заходів, а також міцні гарантії від ризику зловживань та свавілля. Потреба в гарантіях буде ще більшою, коли мова йде про використання технології розпізнавання обличчя в реальному часі (п. 82 рішення).

ЄСПЛ зазначив про наявність серйозних сумнівів в тому, що національні правові положення відповідають вимозі «якості закону». Він вказав, зокрема, що національне законодавство дозволяє обробку біометричних персональних даних «у зв'язку зі здійсненням правосуддя» (див. пункт 31). Це правове положення сформульовано широко. Беручи до уваги, що Уряд не посилався на будь-яке авторитетне тлумачення цього положення Верховним або Конституційним судами та не подавав жодних прикладів його обмежувального тлумачення та застосування в адміністративній та судовій практиці, виявляється, що воно дозволяє обробку біометричних персональних даних – у тому числі за допомогою технології розпізнавання обличчя – у зв'язку з будь-яким судовим провадженням. Національне законодавство не містить жодних обмежень щодо характеру ситуацій, які можуть призвести до використання технології розпізнавання обличчя, цілей, категорій людей, які можуть бути ціллю, або щодо обробки конфіденційних персональних даних. Крім того, Уряд не послався на будь-які процедурні гарантії, що супроводжували б використання технології розпізнавання обличчя в росії, такі як процедури авторизації, процедури, яких слід дотримуватися для вивчення, використання та зберігання отриманих даних, механізми наглядового контролю та доступні засоби правового захисту (п. 83).

Суд вважав, що не підлягає сумніву, що боротьба зі злочинністю і, зокрема, з організованою злочинністю та тероризмом, яка є однією з проблем, з якими стикаються сучасні європейські суспільства, значною мірою залежить від

використання сучасних наукових методів розслідування та ідентифікації. Однак, хоча Суд визнав важливість таких методів у розкритті та розслідуванні злочинів, він повинен обмежити сферу свого розгляду. Питання не в тому, чи може обробка біометричних персональних даних за допомогою технології розпізнавання обличчя взагалі вважатися виправданою відповідно до Конвенції. Єдине питання, яке повинен розглянути Суд, полягало в тому, чи була обробка персональних даних заявника виправданою відповідно до пункту 2 статті 8 Конвенції в цій справі (порівняйте з рішенням у справі *S. and Marper*).

Визначаючи, чи була обробка персональних даних заявника «необхідною в демократичному суспільстві», Суд спочатку оцінив рівень фактичного втручання в право на повагу до приватного життя (див. *P.N. v. Germany*, згадане вище). Він зазначив, що поліція збирала та зберігала цифрові зображення заявника та використовувала їх для вилучення та обробки біометричних персональних даних заявника за допомогою технології розпізнавання обличчя: по-перше, щоб ідентифікувати його за фотографіями та відео, опублікованими в Telegram, а по-друге, щоб знайти та заарештувати його, коли він здійснював поїздки у московському метро. Суд визнав ці заходи особливо втручальними, особливо стосовно технології розпізнавання обличчя (див. пункт 37). Визнання таких заходів «необхідними в демократичному суспільстві» вимагало високого рівня обґрунтування, зокрема, особливо високого рівня обґрунтування потребувала необхідність застосування технології розпізнавання обличчя. Більше того, оброблені персональні дані містили інформацію про участь заявника у мирному протесті і тому розкривали його політичні погляди. Відповідно, вони потрапили до спеціальних категорій конфіденційних даних, що забезпечують підвищений рівень захисту (див. пункт 76) (п. 86 рішення).

При оцінці «необхідності в демократичному суспільстві» обробки персональних даних в контексті розслідувань, характер і тяжкість правопорушень, про які йдеться, є одним з елементів, які слід враховувати (див., *mutatis mutandis*, *P.N. v. Germany*, цитоване вище, § 72). Національне законодавство дозволяє обробку біометричних персональних даних у зв'язку з розслідуванням та обвинуваченням щодо будь-якого правопорушення, незалежно від його характеру та тяжкості (п. 87 рішення).

ЄСПЛ зауважив, що заявник був притягнутий до кримінальної відповідальності за незначне правопорушення, що полягало у проведенні одиночного пікету без попереднього повідомлення – правопорушення, кваліфіковане як адміністративне, а не кримінальне відповідно до національного законодавства. Його ніколи не звинувачували у вчиненні будь-яких недостойних дій під час пікету, таких як перешкоджання дорожньому руху, пошкодження майна або акти насильства. Ніколи не стверджувалося, що його дії становлять будь-яку небезпеку для громадського порядку або транспортної безпеки. Суд вже встановив, що провадження у справі про адміністративне правопорушення стосовно заявника порушило його право на свободу вираження поглядів (див. пункт 57). Він вважав, що використання особливо інтрузивних технологій розпізнавання обличчя для ідентифікації та арешту

учасників мирних акцій протесту може мати стримуючий ефект щодо прав на свободу вираження поглядів та зібрань (п. 88 рішення).

За таких обставин використання технології розпізнавання обличчя для ідентифікації заявника за фотографіями та відео, опублікованими в Telegram, а тим більше використання технології розпізнавання обличчя в реальному часі для визначення місцезнаходження та арешту заявника під час його поїздки в московському метро – не відповідало «нагальній соціальній потребі».

У світлі всіх вищезазначених міркувань ЄСПЛ виснував, що використання особливо інтрузивної технології розпізнавання обличчя в контексті реалізації заявником свого права на свободу вираження поглядів, передбаченого Конвенцією, є несумісним з ідеалами та цінностями демократичного суспільства, керованого верховенством права, яке Конвенція була покликана підтримувати та просувати. Обробка персональних даних заявника з використанням технології розпізнавання обличчя в рамках провадження в адміністративному правопорушенні – по-перше, для ідентифікації його за фотографіями та відео, опублікованими в Telegram, а по-друге, для визначення місцезнаходження та арешту під час поїздки в московському метро – не може вважатися «необхідною в демократичному суспільстві» (п. 90 рішення).

Відповідно, було порушення статті 8 Конвенції.

Висновок

Порушення статті 8 Конвенції (право на повагу до приватного і сімейного життя).

Порушення статті 10 Конвенції (свобода вираження поглядів).

Рішення в цій справі ухвалене Палатою 4 липня 2023 року й набуло статусу остаточного 4 жовтня 2023 року відповідно до пункту 2 статті 44 Конвенції.