

Обставини справи

Справа стосувалася законодавчої вимоги до «організаторів інтернет-комунікацій» зберігати всі дані про комунікації протягом 1 року та зміст усіх комунікацій протягом 6 місяців, а також надавати ці дані правоохоронним органам або службам безпеки у випадках, визначених законом, разом з інформацією, необхідною для розшифрування електронних повідомлень, якщо вони зашифровані.

Заявник, Подчасов Антон Валерійович, громадянин росії, 1981 року народження, проживає в місті Барнаул (росія). Заявник був користувачем Telegram, програми для обміну повідомленнями, яку можна безкоштовно використовувати на різних пристроях; відповідно до офіційного вебсайту додатку, Telegram не має наскрізного (клієнт-клієнт) шифрування за замовчуванням, а використовує спеціальну схему шифрування «сервер-клієнт» у своїх «хмарних чатах» за замовчуванням. Однак, можна перейти на наскрізне шифрування, активувавши функцію «секретний чат», зміст якого відомий лише адресату та отримувачу.

З червня 2017 року Telegram Messenger LLP було внесено до спеціального публічного реєстру як «інтернет організатора комунікацій» (організатор розповсюдження інформації в мережі Інтернет, далі – ICO). Це мало наслідком обов'язок збереження всіх комунікаційних даних протягом 1 року, змісту усіх повідомлень протягом 6 місяців і надання таких даних правоохоронним органам або службам безпеки у випадках, визначених законом, разом з інформацією, необхідною для розшифровки електронних повідомлень, якщо вони були зашифровані.

12 липня 2017 року Федеральна служба безпеки («ФСБ») вимагала від Telegram Messenger LLP розкрити технічну інформацію, яка сприяла б «дешифруванню повідомлень з 12 липня 2017 року стосовно користувачів Telegram, які підозрювалися в діяльності, пов'язаній з тероризмом». Наказ про розкриття посилався на статтю 10.1 (4.1) Закону про інформацію та наказ № 432 від 19 липня 2016 року. Він містив шість мобільних телефонних номерів, пов'язаних з обліковими записами Telegram Messenger, і посилався на шість судових рішень, винесених 10 липня 2017 року.

Telegram Messenger LLP відмовився виконувати наказ про розкриття інформації, стверджуючи, що це технічно неможливо без створення бекдору, який послабить механізм шифрування для всіх користувачів. У ньому, зокрема, пояснили, що шестеро користувачів, згаданих у наказі про розкриття інформації, увімкнули функцію «секретного чату» і тому використовували наскрізне шифрування. Мещанський районний суд Москви 12 грудня 2017 року

наклав на компанію штраф. Згодом, рішенням від 13 квітня 2018 року Таганський районний суд міста Москви постановив заблокувати додаток Telegram в росії. Обидва рішення після їх апеляційного оскарження були залишені без змін.

12 березня 2018 року заявник, разом із 34 іншими особами, оскаржили наказ про розголошення до суду. Скаржники стверджували, що надання ключів шифрування, як того вимагає ФСБ, дозволить розшифрувати повідомлення всіх користувачів. Таким чином, це порушить їх право на повагу до приватного життя та конфіденційності їх спілкування. Після отримання ключів шифрування ФСБ матиме технічну можливість отримати доступ до всіх комунікацій без судового дозволу, якого вимагає російське законодавство. Вони вказали на широку сферу застосування статті 10.1 Закону про інформацію як правової основи втручання та на відсутність гарантій від потенційно необґрунтованого розкриття їхньої особистої інформації.

22 березня 2018 року Мещанський районний суд відхилив скаргу як неприйнятну, встановивши, що оскаржуваний наказ про розкриття не вплинув на права скаржників. Рішення про неприйнятність не містило жодного додаткового обґрунтування.

22 травня 2018 року Московський міський суд залишив без змін рішення про неприйнятність у апеляційному порядку.

10 вересня 2018 року суддя Московського міського суду відмовив у направленні касаційної скарги, поданої заявником, для розгляду до Пленуму Московського міського суду, вказавши на відсутність істотних порушень норм матеріального та процесуального права, які вплинули на результат провадження.

Подальша касаційна скарга заявника була відхилена рішенням Верховного суду російської федерації 16 січня 2019 року. В свою чергу, додаток Telegram Messenger все ще доступний і працює в росії.

Заявник, посилаючись на статтю 8 Конвенції (право на повагу до кореспонденції) та статтю 13 (право на ефективний засіб правового захисту) скаржився на законодавчу вимогу для інтернет організаторів комунікацій (ICO) зберігати вміст всіх інтернет-комунікацій та пов'язаних із цим комунікаційних даних, а також надавати ці дані правоохоронним органам чи службам безпеки на їхню вимогу разом з інформацією, необхідною для розшифрування електронних повідомлень, якщо вони були зашифровані.

Оцінка Суду

Стаття 8 Конвенції

Суд вважав, що зберігання інтернет організатором комунікацій (ICO) заявника вмісту всіх його інтернет-комунікацій і пов'язаних з ним даних

порушило його право на повагу до приватного життя та кореспонденції (див. для порівняння рішення у справі *Breyer v. Germany*, № 50001/12, § 81, від 30 січня 2020 року, а також *Ekimdzhiev and Others v. Bulgaria*, № 70078/12, §§ 372 та 373, від 11 січня 2022 року). Таке зберігання становить втручання в його права, передбачені статтею 8 Конвенції, незалежно від того, чи отримали органи влади доступ до збережених даних. Зберігання, хоча й здійснюється приватними особами – ICO – вимагається законом; з цього випливає, що втручання можна віднести на рахунок російської федерації (див. згадане вище рішення у справі *Ekimdzhiev and Others*, згадане в цій справі, §§ 372 та 375) (пункт 52 рішення).

ЄСПЛ звернув увагу, що у справі *Roman Zakharov* Суд розглянув російське законодавство про таємне спостереження та встановив, що, беручи до уваги таємний характер заходів спостереження, широку сферу їх застосування, що впливає на всіх користувачів мереж зв'язку, і відсутність ефективних засобів для оскарження стверджуваного застосування заходів таємного спостереження на національному рівні, сама наявність законодавства, яке дозволяє таємне спостереження, є втручанням у приватне життя користувача (див. *Roman Zakharov v. Russia* ([GC], № 47143/06, §§ 170–79 від 4 грудня 2015 року). Суд не вбачив підстав вважати інакше у цій справі, оскільки Уряд підтвердив, що доступ до збережених Інтернет-комунікацій та пов'язаних із ними даних регулюється тим самим правовим режимом, який розглядався у справі *Roman Zakharov*. Таким чином, саме існування оскаржуваного законодавства само по собі становить втручання у реалізацію заявником прав за статтею 8 Конвенції (порівняйте, згадане вище рішення у справі *Ekimdzhiev and Others v. Bulgaria*, № 70078/12, §§ 383–84, від 11 січня 2022 року) (пункт 55 рішення).

Зрештою, щодо законодавчого зобов'язання ICO розшифровувати комунікації, якщо вони зашифровані, Суд відмітив, що зауваження сторін щодо цього питання обмежуються наскрізним шифруванням комунікацій, що у випадку Telegram є спілкуванням через «секретні чати». Сторони не надали жодних зауважень щодо схеми шифрування, яка використовується в «хмарних чатах», тому Суд не розглядав її (пункт 56 рішення).

Водночас, Суд дійшов висновку, що безперервне зберігання Інтернет комунікацій заявника та пов'язаних комунікаційних даних у Telegram, потенційний доступ органів влади до цих даних і зобов'язання Telegram розшифрувати їх, якщо вони зашифровані, відповідно до Закону про інформацію та прийнятих для його реалізації нормативно-правових актів, становило втручання в права заявника за статтею 8 Конвенції (пункт 58 рішення).

Крім того, ЄСПЛ зауважив, що в цій справі персональні дані зберігаються з метою надання компетентним національним органам влади можливості

проводити цілеспрямоване таємне спостереження за комунікаціями. Тому питання щодо зберігання персональних даних і таємного спостереження, тісно пов'язані між собою (пункт 58 рішення).

Суд вважав, що у даній справі питання законності та наявності легітимної мети не можна розглядати окремо від питання про те, чи було втручання «необхідним у демократичному суспільстві», тому він розглянув їх разом нижче (пункт 66 рішення).

Утримання і збереження інтернет-комунікацій і пов'язаних із ними даних у цій справі мало правову основу в Законі про інформацію, який слід розглядати в поєднанні з правовими положеннями, що регулюють доступ правоохоронних органів до даних, що зберігаються, та їх подальшого використання відповідно до Закону про інформацію, Кримінального процесуального кодексу та Закону про оперативно-розшукову діяльність (див. *Breyer v. Germany*, № 50001/12, § § 85 і 97, від 30 січня 2020 року) (пункт 67 рішення).

Суд також зазначив, що хоча технологічні можливості значно збільшили обсяг комунікацій, що проходять через глобальний Інтернет, загрози, з якими стикаються Договірні Держави та їхні громадяни, також поширилися. До них належать (але ними не обмежуються) глобальний тероризм, торгівля наркотиками, торгівля людьми та сексуальна експлуатація дітей. Багато з цих загроз походять від міжнародних мереж ворожих сторін, які мають доступ до все більш складних технологій, що дозволяє їм спілкуватися непоміченими. ЄСПЛ переконався, що оскаржувані законодавчі положення переслідували законні цілі захисту національної безпеки, запобігання заворушенням і злочинам, та захисту прав і свобод інших (пункт 68 рішення).

Таким чином, залишалося з'ясувати, чи містило національне законодавство адекватні та ефективні запобіжні заходи та гарантії, аби відповідати вимозі «якості закону» та «необхідності в демократичному суспільстві» (пункт 69 рішення).

Оскаржуване законодавство вимагало безперервного автоматичного зберігання та зберігання вмісту всіх інтернет-комунікацій протягом 6 місяців, а також відповідних даних комунікації протягом 1 року. Воно застосовувалося до всіх інтернет комунікаційних послуг, які використовуються для передачі голосових, текстових, візуальних, звукових, відео чи інших електронних повідомлень. Це впливає на всіх користувачів інтернет комунікацій, навіть за відсутності обґрунтованої підозри в причетності до злочинної діяльності чи діяльності, що загрожує національній безпеці, або будь-яких інших причин, які дають привід вважати, що збереження даних може сприяти боротьбі з серйозними злочинами чи захисту національної безпеки. ЄСПЛ був вражений надзвичайно широким обов'язком зберігання, передбаченим оскаржуваним законодавством, і дійшов висновку, що втручання є надзвичайно масштабним

і серйозним (порівняйте згадане вище рішення у справі *Ekimdzhiev and Others v. Bulgaria*, № 70078/12, § 394, від 11 січня 2022 року, що стосується лише збереження даних комунікацій) (пункт 70 рішення).

Відносно законодавчої вимоги надавати правоохоронним органам або службам безпеки доступ до збережених даних на їх запит, ЄСПЛ повторив, що доступ до даних в окремих випадках повинен супроводжуватися, *mutatis mutandis*, тими самими гарантіями, що й таємне спостереження (див. рішення у справі *Ekimdzhiev and Others v. Bulgaria*, згадане вище, § 395). Суд бере до уваги аргумент Уряду про те, що доступ має бути дозволений судом, однак зазначає, що згідно з національним законодавством росії, її правоохоронні органи не зобов'язані надавати постачальнику послуг зв'язку судовий дозвіл перед отриманням доступу до комунікацій особи. Дійсно, згідно з розпорядженнями уряду, ІСО повинні встановити обладнання, яке надає службам безпеки прямий доступ до збережених даних. Таким чином, правоохоронні органи мають прямий віддалений доступ до всіх інтернет-комунікацій і пов'язаних з ними комунікаційних даних (пункт 72 рішення).

Суд вважає, що вимога пред'явити дозвіл постачальнику послуг зв'язку перед отриманням доступу до комунікацій особи є важливою гарантією захисту від зловживань з боку правоохоронних органів, яка гарантує отримання належного дозволу в усіх випадках таємного спостереження. Спосіб організації доступу до збережених даних у росії дає службам безпеки технічні засоби для обходу процедури авторизації та доступу до збережених інтернет комунікацій і даних комунікацій без попереднього судового дозволу. Хоча ймовірність неналежних дій нечесної, недбалої чи надмірно старанної посадової особи ніколи не може бути повністю виключена незалежно від системи, ЄСПЛ вважав, що така система, як російська, яка дозволяє секретним службам отримувати прямий доступ до інтернет-комунікацій кожного громадянина, не вимагаючи від нього надання дозволу на перехоплення від постачальника послуг зв'язку або будь-кого іншого, особливо схильна до зловживань. Тому, потреба в гарантіях проти свавілля та зловживань видається особливо великою (див. згадане вище рішення у справі *Roman Zakharov v. Russia* ([GC], № 47143/06, §§ 269–70 від 4 грудня 2015 року) (пункт 73 рішення).

Уряд підтвердив, що доступ до збережених інтернет-комунікацій та пов'язаних із ними комунікаційних даних у контексті перехоплення мобільного телефонного зв'язку регулюється тим самим правовим режимом, який розглядався у справі *Roman Zakharov* (цит. в цій справі). У цій справі Суд визнав, що положення російського законодавства, які регулюють заходи таємного спостереження, не відповідали вимозі «якості закону», оскільки вони не передбачали адекватних та ефективних гарантій проти свавілля та ризику зловживань. Тому вони були не в змозі обмежити «втручання» в тому, що було

«необхідним у демократичному суспільстві». Суд, зокрема, встановив, що обставини, за яких державні органи були уповноважені вдаватися до заходів таємного спостереження з метою виявлення, запобігання та розслідування кримінальних правопорушень або захисту національної, військової, економічної чи екологічної безпеки росії, не були визначені достатньо чітко. Процедури дозволу не були здатні забезпечити те, щоб таємні заходи спостереження визначалися лише тоді, коли це «необхідно в демократичному суспільстві». Нагляд за перехопленням не відповідав вимогам незалежності, повноважень та компетенції, достатнім для здійснення ефективного та постійного контролю, громадського контролю та ефективності на практиці. Ефективність засобів правового захисту була порушена відсутністю повідомлення на будь-якому етапі таємного спостереження або належного доступу до документів, що стосуються таємного спостереження (див. рішення у справі *Roman Zakharov v. Russia* ([GC], № 47143/06, §§ 243–305) (пункт 74 рішення).

ЄСПЛ не вбачив жодних підстав дійти іншого висновку у цій справі. Тому він вважав, що національне законодавство не передбачає адекватних і достатніх гарантій проти зловживань, пов'язаних із доступом правоохоронних органів до інтернет-комунікацій та пов'язаних комунікаційних даних, які зберігаються ІСО відповідно до Закону про інформацію.

В свою чергу, стосовно вимоги подавати до служб безпеки інформацію, необхідну для розшифровки електронних повідомлень, якщо вони зашифровані, Суд зауважив, що міжнародні органи стверджували, що шифрування забезпечує потужні технічні гарантії проти незаконного доступу до вмісту повідомлень і тому широко використовується як засіб захисту права на повагу до приватного життя та конфіденційності листування в інтернеті (пункт 76 рішення).

З вищевикладеного ЄСПЛ зробив висновок, що оскаржуване законодавство передбачає збереження всіх інтернет-комунікацій усіх користувачів, прямий доступ служб безпеки до даних, що зберігаються без відповідних гарантій захисту від зловживань, і вимогу розшифровувати зашифровані повідомлення, що застосовуються до комунікації з наскрізним шифруванням не можна вважати необхідними в демократичному суспільстві. У тій мірі, в якій це законодавство дозволяє органам державної влади мати доступ на загальній основі та без достатніх гарантій до вмісту електронних комунікацій, в тій мірі воно порушує саму суть права на повагу до приватного життя згідно зі статтею 8 Конвенції. Отже, Держава-відповідач перевищила будь-які допустимі межі розсуду в цьому відношенні (пункт 80 рішення).

Заявник скаржився за статтею 13 Конвенції, що він не мав у своєму розпорядженні ефективного національного засобу правового захисту для своєї скарги за статтею 8 Конвенції. Беручи до уваги факти справи, доводи

сторін та висновки за статтею 8 Конвенції, Суд вважав, що немає необхідності виносити окреме рішення щодо прийнятності та суті скарги за статтею 13 (див. *Centre for Legal Resources on behalf of Valentin Câmpeanu v. Romania* [GC], № 47848/08, § 156, ECHR 2014).

Висновок

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

Рішення в цій справі ухвалено Палатою 13 лютого 2024 року та набуло статусу остаточного 13 травня 2024 року відповідно до пункту 2 статті 44 Конвенції.