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

© Переклад з доповненнями адвокатів, кандидатів юридичних наук Олександра Дроздова та Олени Дроздової

Офіційне цитування:
CASE OF BENEDIK v. SLOVENIA
(Application no. 62357/14)

Офіційний текст англійською мовою: http://hudoc.echr.coe.int/eng?i=001-182455

ЧЕТВЕРТА СЕКЦІЯ

СПРАВА БЕНЕДІК проти СЛОВЕНІЇ

(Заява №. 62357/14)

РІШЕННЯ

СТРАСБУРГ

24 квітня 2018 року

Це рішення набуде статусу остаточного відповідно до умов, визначених пунктом 2 статті 44 Конвенції. Воно може підлягати редакційним виправленням.

У справі Бенедік проти Словенії

Європейський суд з прав людини (четверта секція) засідаючи Палатою у складі:

Ганна Юдківська, *голова,*
Вінсент А. Де Гаетано,
Карло Ранзоні
Георгес Раварані
Марко Бошняк,
Пітер Пакзолей, *судді,*
і Андреа Тамієтті, *Секретар секції,*

Після обговорення за зачиненими дверима 20 травня 2018 року,

Постановляє таке рішення, що було ухвалене у той день:

ПРОЦЕДУРА

1. Справа було розпочато за заявою (№ 62357/14) проти Республіки Словенії, поданої до Суду відповідно до статті 34 Конвенції з прав людини та основних свобод (далі - Конвенція) Ігорем Бенедіком .

2. Заявника представляв у Суді пан М. Єленіч Новак, адвокат, який практикував у Любляні. Уряд Словенії ("Уряд") був представлений їх представником, пані Дж. Морела, державний прокурор.

3. Заявник стверджував, зокрема, що його право відповідно до статті 8 Конвенції було порушене, оскільки поліція незаконно отримала інформацію, яка викликала встановлення його особи, від інтернет-провайдера.

4. 8 квітня 2015 року уряд був повідомлений про заяву.

ФАКТИ

I. ОБСТАВИНИ СПРАВИ

5. Заявник народився в 1977 році і мешкає в м. Крань.

A. Розслідування

6. У 2006 році правоохоронні органи кантону Вале провели моніторинг користувачів так званої мережі "Razorback". Поліція Швейцарії встановила, що деякі користувачі володіли і обмінювалися дитячим порнографією у вигляді зображень або відеозаписів. Файлами, які містять незаконний контент, обмінювалися за допомогою так званої «p2p» (peer-to-peer) мережі обміну файлами, в якій кожен з підключених комп'ютерів діяв як клієнт і сервер. Отже, кожен користувач міг отримати доступ до всіх файлів, доступних для обміну іншими користувачами мережі та завантажити їх для використання. Серед

динамічних адрес Інтернет-протоколу ("IP"), стосовно яких подала запит поліція Швеції, також була певна динамічна IP-адреса, яка згодом була пов'язана з заявником .

7. На підставі даних, отриманих поліцією Швеції, 7 серпня 2006 року поліція Словенії не отримавши судового наказу подала запит до компанії S., інтернет-провайдер Словенії (далі «ISP») розкрити дані про користувача, якому була призначена вищезазначена IP адреса о 13:28 20 лютого 2006 року. Поліція засновувала свій запит на розділі 149b (3) Кримінально-процесуального Кодексу (далі "КПК" , дивіться пункт 36 нижче), який вимагав від операторів електронних мереж комунікацій розкривати поліції інформацію про власників або користувачів певних засобів електронного зв'язку, подробиці про яких не були доступні у відповідному довіднику. У відповідь, 10 серпня 2006 року ISP надав поліції ім’я та адресу батька заявника, який був клієнтом інтернет-провайдера, що стосувався відповідної IP-адреси.

8. 12 грудня 2006 року поліція запропонувала Районній державній прокуратурі м. Крань подати запит слідчому судді Районного суду м. Крань видати наказ вимагаючи від інтернет-провайдера розкрити персональні дані про абонента і трафік, пов'язаний з IP-адресою, про яку йде мова. 14 грудня 2006 року такий наказ суду був отриманий на підставі статті 149b (1)КПК, а Інтернет-провайдер надав поліції необхідні дані.

9. 12 січня 2007 року суддя, який веде слідство районного суду м. Крань видав наказ про проведення обшуку в будинку родини заявника. В наказі батько заявника був зазначений як підозрюваний. Під час обшуку будинку поліція та суддя, який веде слідство районного суду м. Крань вилучили чотири комп'ютера, а згодом зробили копії жорстких дисків.

10. На основі розмови з членами сім'ї заявника, записи про яких недоступні, поліція змінила підозрюваного на заявника.

11. Під час огляду жорстких дисків поліція виявила, що на одному з них містилися файли з порнографічними матеріалами за участю неповнолітніх. Поліція встановила , що заявник встановив eMule, програму для обміну файлами, на одному з комп'ютерів , за допомогою якої він мав можливість завантажувати різні файли в інших користувачів програми, а також автоматично пропонував та ділився своїми власними файлами з ними. Серед файлів, завантажених заявником, невеликий відсоток складав дитячу порнографію.

12. 26 листопада 2007 року окружний прокурор м. Крань подав запит про відкриття розслідування проти заявника.

13. На свій захист перед слідчим суддею заявник стверджував, *зокрема,* що йому не було відомо про зміст файлів, про які йде мова. Він також стверджував, що ISP незаконно, без судового ордера, передав поліції його дані, в тому числі його адресу.

14. 5 березня 2008 року суддя, який веде слідство, районного суду м. Крань відкрив судове слідство проти заявника на підставі обґрунтованої підозри, що він скоїв кримінальний злочин показу, створення, зберігання та розповсюдження порнографічного матеріалу відповідно до розділу 187 (3) Кримінального кодексу. Суддя зазначив, серед

іншого, що батько заявника був власником визначеної IP-адреси ,а заявник, як стверджувалося, зареєструвався в відповідній програмі під іменем "Benet".

15. 17 березня 2008 року адвокат заявника подав апеляцію на рішення про відкриття судового слідства. Він стверджував, *зокрема* , що докази стосовно особи користувача відповідної IP-адреси були отримані незаконно. Ця інформація стосувалася даних про трафік, тому її неможливо було отримати без судового ордера .

16. 21 березня 2008 року тимчасова колегія суду відхилила апеляцію виявивши, що, незважаючи на те, що адвокат стверджував, що особа користувача IP-адреси була отримана незаконно, він не вимагав, щоб певні документи були вилучені з матеріалів справи.

B. Судовий процес

17. 29 травня 2008 року районна державна прокуратура м. Крань подала звинувачувальний акт проти заявника за вищезазначений кримінальний злочин.

18. На засіданні 8 жовтня 2008 року заявник подав письмове прохання про вилучення доказів, отриманих незаконно, в тому числі інформації стосовно користувача відповідної IP-адреси, отриманої без наказу суду.

19. 5 грудня 2008 року суд відхилив запит заявника, виявивши, що дані стосовно користувача відповідної IP-адреса були отримані відповідно до розділу 149b (3) КПК.

20. 5 грудня 2008 року районний суд м. Крань визнав заявника винним у скоєнні кримінального правопорушення , в якому його обвинувачували. На основі думки експерта в сфері комп'ютерної науки окружний суд постановив, що заявникові повинно було бути відомо про 630 порнографічних зображень і 199 відео за участі неповнолітніх, які він завантажив за допомогою мережі p2p і зробив доступними для спільного використання іншим користувачам. Заявник був засуджений до восьми місяців умовного ув’язнення з випробувальним терміном в два роки.

C. Провадження Верховному Суді м. Любляна

21. Заявник і окружний прокурор оскаржили рішення суду першої інстанції. Заявник оскаржував факти, встановлені окружним судом. Він також стверджував, що інформація про абонента, яку поліція Словенії отримала незаконно, повинна бути вилучена з доказів. Отже, всі докази, засновані на таких незаконно отриманих даних, також повинні були бути вилучені.

22. 4 листопада 2009 року Верховний суд м. Любляна частково задовольнив апеляцію окружного прокурора змінивши умовне засудження заявника на тюремного ув'язнення на термін шість місяців. Апеляція заявника була відхилена як необґрунтована. Верховний суд підтвердив, що суд першої інстанції були правильно встановив факти справи; крім того суд

постановив, що дані стосовно користувача IP-адреси були отримані на законних підставах, оскільки для такої мети не потрібен був наказ суду.

D. Провадження у Верховному суді

23. Заявник подав апеляцію з питань прав до Верховного суду повторюючи, що динамічну IP-адресу неможливо було порівнювати з телефонним номером, який не був внесений в телефонний довідник, оскільки нова IP-адреса була призначена для комп'ютера кожного разу, коли користувач входив в систему Відповідно, такі дані необхідно було розглядати як дані про трафік, які складають обставини та факти, пов'язані з електронним зв'язком, та залучали захист конфіденційності спілкування. Заявник стверджував, що поліція Швейцарії не повинна була отримати відповідну динамічну IP-адресу без судового наказу, а також поліція Словенії не повинна отримати дані про особу абонента, пов'язаного з IP-адресою без такого наказу.

24. 20 січня 2011 року Верховний суд відхилив апеляцію заявника з питань права вважаючи, що з огляду на загальнодоступність веб-сайтів, а також з огляду на той факт, що поліція Швейцарії могла перевіряти обміни в мережі p2p просто за допомогою моніторингу користувачів, які обмінюються певним контентом, тобто без будь-якого певного втручання в інтернет-трафік, таке спілкування неможливо вважати приватним і таким чином, захищеним статтею 37 Конституції. Крім того, на думку Верховного суду, поліція не отримала дані про електронне спілкування заявника, але лише дані, які стосуються користувача певного комп'ютера, з допомогою якого був отриманий доступ до мережі інтернет.

E. Провадження в Конституційному Суді

25. Заявник подав конституційну скаргу до Конституційного Суду повторюючи скарги, подані до судів нижчої інстанції.

26. Конституційний суд подав запит до Уповноваженого з питань інформації для висловлення своєї думки з цього питання. Уповноважений з питань інформації вважала, що причиною отримання інформації про особу окремого користувача електронного спілкування було саме те, що він або вона спілкувалися за допомогою більш-менш загальнодоступних веб-сайтів. На думку Уповноваженого з питань інформації було неможливо відокремити дані про трафік від даних про абонентів, оскільки дані про трафік самостійно не мають ніякого значення, якщо не з'ясувати, яка особа стояла за цими даними - таким чином ця остання інформація вважалася надзвичайно важливим елементом конфіденційності спілкування. Уповноважена з питань інформації також зазначила, що положення Закону про електронне спілкування, чинні у відповідний час, вимагали наказу суду стосовно всіх даних, пов’язаних з електронним спілкуванням незалежно від того, чи були вони пов'язані з даними про трафік або особу. На думку Уповноваженого з питань інформації розділ 149b (3) КПК, який вимагав лише письмового запиту від поліції для отримання даних про осіб, які спілкуються, був конституційно проблематичним.

27. 13 лютого 2014 року Конституційний суд відхилив скаргу заявника постановивши , що його конституційні права не були порушені. Рішення Конституційного суду було прийняте сімома голосами проти двох. Суддя Дж. Совдат та суддя Д. Джадек Пенса написали окремі думки. Рішення було вручене заявникові 11 березня 2014 року.

1 Рішення Конституційного суду

28. Конституційний Суд з самого початку зазначив, що, окрім змісту повідомлень, стаття 37 Конституції також захищала дані про трафік, тобто будь-які дані, оброблені для передачі повідомлень у мережі електронних комунікацій. Суд вважав, що IP-адреси були включені в такі дані про трафік. Проте Конституційний Суд дійшов висновку, що заявник, не намагався сховати у будь-який спосіб IP-адресу, за допомогою якої він отримав доступ до інтернет, свідомо відкривав себе для публіки і не міг законно очікувати конфіденційності. Як наслідок, дані щодо особи користувача IP-адреси не були захищені конфіденційністю зв'язку відповідно до статті 37 Конституції, але лише як конфіденційність інформації відповідно до статті 38 Конституції , а також не був необхідний наказ суду для того, щоб розкрити їх в справі заявника.

29. Найбільш доречні частини рішення Конституційного суду є наступними (в перекладі на англійську мову на веб-сайті Конституційному суду):

«Перегляд заперечень щодо доступу до IP-адреси позивача поліцією Швейцарії

11 Другий параграф статті 37 Конституції передбачає більш високий рівень захисту, ніж стаття 8 ЄКПЛ, оскільки він вимагає наказу суду щодо будь-якого втручання у право на конфіденційність спілкування... Право на конфіденційність спілкування, визначене першим параграфом статті 37 Конституції, насамперед захищає зміст переданого повідомлення. ... Окрім змісту повідомлення також захищаються обставини та факти, пов'язані з спілкуванням. Відповідно до цієї точки зору, у рішенні № Up-106/05 від 2 жовтня 2008 (Офіційний вісник РС, № 100/08, та OdlUS XVII, 84) Конституційний Суд продовжив захист, передбачений статтею 37 Конституції, також на такі дані, які стосуються телефонних дзвінків, які за своїм характером є невід'ємною частиною спілкування, для того, щоб такі дані не могли бути отримані без судового наказу. Наведене рішення посилається на телефонний зв'язок, але такий самий висновок можливо застосовувати *mutatis mutandis* до інших видів зв'язку на відстані. Вирішальний тест на конституційність перегляду для перегляду Конституційним Судом питання стосовно того, чи певне спілкування є захищеним відповідно до статті 37 Конституції є перевіркою законного очікування конфіденційності.

12. Зв'язок через Інтернет відбувається, в принципі, в анонімній формі, яка необхідна для вільного розвитку особистості, свободи слова та вираження ідей, а отже, для розвитку вільного та демократичного суспільства .Тому конфіденційність зв'язку, захищена суворими умовами, визначеними в другому параграфі статті 37 Конституції, є дуже важливим правом людини, яке стає все більш важливим завдяки технологічним досягненням та пов'язаними з цим зростаючими можливостям моніторингу. Це викликає законне очікування фізичних осіб того, що держава залишить їх у спокої і в

їх спілкуванні за допомогою сучасних каналів зв'язку, а також того, що вони не обов'язково повинні захищати себе за те, що вони роблять, говорять, пишуть або думають. Якщо існує підозра в кримінальному правопорушенні, поліція повинна мати можливість ідентифікувати осіб, які брали участь у певному спілкуванні, пов'язаному з передбачуваним злочином, оскільки за злочинцями складніше простежити у зв'язку з цим принципом анонімності в Інтернеті. Умови, відповідно до яких поліція може проводити слідчі дії, а також питання стосовно необхідності наказу суду залежать від того, чи може таке втручання вплинути на право на конфіденційність інформації.

13. Як було зазначено вище, на додаток до змісту повідомлень стаття 37 Конституції також захищає дані про трафік. Дані про трафік означають будь-які дані, оброблені для передачі повідомлень в мережі електронних комунікацій або для їх оплати. Це означає, що IP-адреса є даними про трафік. Отже, Конституційний Суд повинен відповісти на питання, чи позивач законно очікував конфіденційності щодо цих даних.

14. У зв'язку з цим переглядом необхідно враховувати два фактори: очікування конфіденційності щодо IP-адреси та законності цього очікування, коли останнє повинне мати такий характер, щоб суспільство бажало визнати його законним. Позивач в справі, про яку йде мова, спілкувався з іншими користувачами мережі Razorback за допомогою програми eMule для обміну різними файлами, в тому числі такими, які містять дитячу порнографію. З урахуванням загальної анонімності користувачів Інтернету, а також змісту файлів, Конституційний Суд не сумнівався в тому, що заявник очікував, що його повідомлення будуть залишатися конфіденційними, а також він також безумовно очікував, що його особистість не буде розкрита. Отже, питання полягало в тому, чи було таке очікування конфіденційності законним. Позивач не встановив, що IP-адреса, за допомогою якої він отримував доступ до Інтернету, була прихована убудь-який спосіб і, таким чином, непомітним для інших користувачів, або те, що доступ до мережі Razorback (а отже, до змісту файлів) був у будь-який спосіб обмеженим , наприклад, за допомогою паролів або інших засобів. ... На відміну від цього , в справі позивача будь-яка особа, зацікавлена в обміні таких даними, мала можливість отримати доступ до оскаржених файлів, і заявник не продемонстрував, що його IP- адреса була у будь-який спосіб прихованою або недоступною для інших користувачів цієї мережі. Це наводить на висновок, що була викликана відкрита лінія зв'язку з раніше невизначеним колом незнайомих осіб, які користуються інтернетом у всьому світі, які виявили інтерес до спільного використання певних файлів, при цьому доступ до IP-адрес інших користувачів не обмежувався для користувачів цієї мережі. Тому, на думку Конституційного Суду, очікування заявником конфіденційності не було законним; оскільки якщо особа свідомо відкриває себе для публіки, навіть з домашнього комп'ютера, притулок свого власного будинку не може бути предметом захисту, передбаченим статтею 37 Конституції. З огляду на вищезазначене, оскаржена позиція Верховного Суду не викликає занепокоєння щодо конституційного права. Отримання даних про динамічну IP-адресу не втручається в його право на конфіденційність зв'язку, визначене першим параграфом статті 37 Конституції з урахуванням всіх обставин справи, тому наказ суду не був необхідним для цього оцінювання. Заявник сам відмовився від свого права на

конфіденційність приватного життя і тому не міг мати законного очікування конфіденційності приватного життя.

...

Перегляд заперечень щодо доступу до даних користувача певної IP-адреси

16. Заявник також оскаржує точку зору Верховного Суду, згідно з якою своїм запитом до інтернет-провайдера відповідно до третього параграфу Статті 149.b КПК поліція не отримала даних про трафік, а лише дані щодо певного користувача визначеного засобу комунікації ...

17. У справі, яка розглядається, 7 червня 2006 року на підставі третього параграфу Статті 149.b КПК поліція надіслала запит постачальнику послуг щодо даних про користувача, якому 20 лютого 2006 року о 13:28була призначена IP-адреса 195.210.223.200. У відповідь вони отримали дані про користувач ім'я, прізвище та адресу, а час спілкування, встановлений з точністю до секунди, вже був відомим. Потім 14 грудня 2006 року поліція також отримала наказ судді, який веде слідство, на підставі першого параграфа 149.b КПК, а постачальник послуг також надавав дані про трафік на основі цього наказу. Тому головним питанням для Конституційного Суду було те, чи є отримання даних про особу користувача певної IP-адреси знаходяться в межах конфіденційності зв'язку.

18. Відповідно до позиції Конституційного суду у рішенні № -106 / 05, стаття 37 Конституції також захищає дані про трафік, тобто дані, які стосуються, наприклад, того, хто, коли, з ким і як часто спілкувалася особа. Особистість особи, яка спілкується, є одним з важливих аспектів конфіденційності зв'язку , тому необхідно отримати судовий наказ про її розголошення відповідно до другого параграфу статті 37 Конституції. Незважаючи на цю точку зору Конституційний Суд вирішив, що твердження заявника про порушення статті 37 Конституції є необґрунтованим в справі, про яку йде **мова.** Своєю поведінкою заявник сам відмовився від захисту приватності, публічно розкриваючи як свою власну IP-адресу, так і зміст своїх повідомлень, і тому не може більше покладатися на неї стосовно розкриття своєї ідентичності. Оскільки таким шляхом він також відмовився від законного сподівання конфіденційності, дані про ідентичність користувача IP-адреси більше не користувалися захистом з точки зору конфіденційності інформації, але тільки з точки зору конфіденційності інформації, визначеної статтею 38 Конституції. Тому, отримавши дані про ім'я, прізвище та адресу користувача динамічної IP-адреси, за допомогою якої спілкувався позивач, поліція не втрутилася в конфіденційність спілкування і тому не вимагала наказу суду для розкриття його особи. З урахуванням вищезазначеного, оскаржена позиція Верховного суду не суперечить статті 37 Конституції, а також скарги позивача в цій частині є необґрунтованими. "

II. ВІДПОВІДНЕ НАЦІОНАЛЬНЕ ЗАКОНОДАВСТВО І ПРАКТИКА

A. Конституція

35. Статті 37 та 38 Конституції, які передбачають захист конфіденційності листування та інших засобів спілкування та захисту персональних даних, відповідно, передбачають:

Стаття 37

"Конфіденційність кореспонденції та інших засобів зв'язку повинна гарантуватися.

Лише закон може встановлювати, що на підставі судового наказу захист конфіденційності листування та інших засобів спілкування та недоторканність приватності повинен бути призупинений на певний час, якщо це є необхідним для відкриття або здійснення кримінального провадження або з міркувань національної безпеки ".

Стаття 38

"Захист персональних даних повинен бути гарантований. Використання персональних даних всупереч цілям, для яких вони були зібрані, заборонено.

Збір, обробка, цільове використання, контроль і захист конфіденційності персональних даних повинні бути передбачені законом.

Кожен має право на доступ до зібраних персональних даних стосовно нього, а також право на судовий захист у випадку будь-якого зловживання такими даними ".

B. Закон про кримінальне судочинство

36. Розділ 149b Закону про кримінальне судочинство (Офіційний бюлетень № 8/06), в розділі, який регулює заходи, вжиті поліцією під час досудового провадження, передбачає:

«(1) Якщо існують підстави підозрювати , що кримінальний злочин , за який злочинець притягується до відповідальності *ex officio* було скоєно, здійснюється або готується або організовується, а інформація про спілкування з використанням електронних мереж спілкування повинна бути отримана для розкриття цього злочину або його виконавця суддя, який веде слідство на запит прокурора, який подає обґрунтовані підстави, може наказати оператору електронної мережі спілкування надати йому інформацію про учасників, обставини та факти електронних повідомлень , такі як: номер або інша форма ідентифікації користувачів послуг електронних комунікацій; тип, дата, час і тривалість дзвінка або іншої форми електронних служб спілкування; кількість переданих даних; а також місце, в якому здійснювалося обслуговування електронного спілкування.

(2) Запит і наказ повинні бути в письмовій формі і повинні містити інформацію , яка дозволяє визначити засоби електронного зв'язку, вказівку на обґрунтовані підстави, період часу, для якого необхідна інформація, і інші важливі обставини , які пропонують використання заходу

(3) Якщо існують підстави для підозр в тому, що кримінальний злочин, за яке злочинця притягують до відповідальності *ex officio,* був скоєний або готується, і інформацію про власника або користувача певних засобів електронного зв'язку , дані

про якого не доступні в відповідному каталозі, а також інформацію про час, протягом якого спосіб комунікації був або використовується, необхідно отримати для того, щоб розкрити цей злочин або його виконавця, поліція може подати запит до оператора мережі електронного спілкування для отримання цієї інформації за їх письмовим запитом та навіть без згоди особи, якої стосується інформація.

(4) Оператор мереж електронного спілкування може не розголошувати своїм клієнтам або третій стороні той факт, що він надав певну інформацію судді, який веде слідство (перший параграф цього розділу) або поліції (попередній пункт), або той факт, що він має намір зробити це.

C. Закон про електронні комунікації

37. На той час, коли були отримані дані, про які йде мова (серпень 2006 року), Закон про електронні комунікації («ECA», Офіційний вісник № 43/04 і 86/04) був чинним. Цей закон запроваджував, серед іншого, Директиву 2002/58 / ЕС (дивіться пункт 56 нижче). Наступні положення були доречними:

Розділ 1

Зміст закону

«Цей Закон регулює умови для надання електронних мереж зв'язку, а також надання послуг електронного зв'язку ... визначає права користувачів ... регулює захист таємності і конфіденційності електронного спілкування і регулює інші питання , пов'язані з електронним спілкуванням ".

стаття 3

Умови використання

« Умови, які використовується в цьому Законі мають наступне значення:

...

25. Дані про трафік - це будь-які дані, оброблені з метою передачі повідомлень в мережі електронних комунікацій або для виставлення рахунку.

... "

стаття 103

Конфіденційність засобів зв’язку

" (1) Конфіденційність засобів зв’язку :

1 Зміст повідомлень ;

2 Дані про трафік та дані про місцезнаходження, пов'язані з повідомленням, зазначеним у пункті (1) 1 вище ;

3. Факти та обставини, пов'язані з невдалою спробою встановлення зв'язку.

(2) Оператор та будь-яка особа, залучена в забезпечення та здійснення своєї діяльності, повинні продовжувати зберігати конфіденційність повідомлень після припинення діяльності, для яких вони повинні були захищати конфіденційність.

(3) Ці суб'єкти, відповідальні відповідно до підпункту (2) вище, можуть отримувати інформацію, яка стосується повідомлень, зазначених в підпункті 1 вище, лише в тому обсязі, який є необхідним для надання спеціальних загальнодоступних послуг зв'язку , і можуть використовувати або передавати [*posreduje*] цю інформацію іншим суб'єктам для надання цих послуг.

(4) Якщо оператори отримують інформацію про зміст повідомлень або записують або зберігають повідомлення та дані про трафік, пов'язані з ними відповідно до підпункту (3) вище , вони повинні повідомити користувача про це, коли підписується угода, або під час початку надання загальнодоступних послуг зв'язку та видалити інформацію про зміст повідомлень або саме спілкування як тільки це стане технічно можливим, і коли інформація вже не буде необхідною для надання певних загальнодоступних послуг зв'язку.

(5) Всі форми спостереження або перехоплення, такі як прослуховування, підключення до мережі, запис, збереження і передача [*posredovanje*] повідомлень , зазначені у пункті (1) вище , повинні бути заборонені, якщо це не дозволено відповідно до підрозділу (4) вище або відповідно до підпунктів 107 цього Закону, або якщо ця форма спостереження або перехоплення необхідна для відправки повідомлень (наприклад , факсимільний зв'язок, електронна пошта, електронні поштові скриньки, голосова пошта і SMS послуги).

... "

стаття 104

Дані про трафік

" (1) Дані про трафік, які стосуються абонентів та користувачів , оброблені та збережені оператором , повинні бути видалені або створені анонімними, як тільки вони більше не є необхідними для передачі повідомлень.

(2) Без шкоди для положень підпункту (1) вище оператор може до повної сплати послуги, але не пізніше, ніж до закінчення терміну давності, зберігати та обробляти дані про трафік, необхідні для цілей обчислення та оплати, пов'язаних з взаємозв'язку.

(3) З метою маркетингу послуг електронного спілкування або надання послуг з доданою вартістю, постачальник публічно доступної служби електронного зв'язку може обробляти дані, зазначені в підпункті 1 вище, в обсязі та протягом часу, необхідного для таких послуг або маркетингу, але лише в тому випадку, якщо абонент або користувач, яких стосуються дані, надали свою попередню згоду. Абоненти і користувачі повинні бути поінформовані, до надання згоди, про типи даних про трафік , які обробляються, а також тривалість такої обробки. Користувач або абонент має право відкликати свою згоду у будь-який час.

(4) Для цілей , зазначених в пункті (2) вище , постачальник послуг повинен вказати в загальних умовах дані про трафік, які будуть збережені і оброблені , а також їх тривалість , та оголосити , що вони будуть оброблені відповідно до Закону про захист даних.

(5) Дані про трафік можуть оброблятися лише відповідно до підпунктів (1) - (4) вище особами, які діють під керівництвом оператора та займаються виставленням рахунку або управлінням трафіком відповідаючи на запити клієнтів, виявленням шахрайства, маркетингом послуг електронного зв'язку або наданням послуги з доданою вартістю, і ця обробка повинна обмежуватися тим, що необхідно для цілей такої діяльності.

(6) Без шкоди для положень підпунктів (1), (2), (3) та (5) вище , оператор після письмового запиту компетентного органу, створеного з метою врегулювання спорів, зокрема, спорів щодо взаємозв'язку або виставлення рахунку, а також відповідно до чинного законодавства , передавати дані про трафік такому органу. "

стаття 107

Законне перехоплення спілкування

« ... (2) Оператор повинен надати можливість здійснювати законне перехоплення повідомлень в певній точці мережі зв'язку загального користування, як тільки він отримає копію оперативної частини наказу компетентного органу з зазначенням точки ... в якій повинне відбуватися законне перехоплення повідомлень та інших даних, які стосуються засобів, обсягу та тривалості цього заходу. "

38. Наступні поправки до ЕСА, а саме ЕСА-А, які були прийняті 28 листопада 2006 року, тобто після того, як були вжиті оскаржені заходи в цій справі (Офіційний вісник № 129/06), регулювали збереження даних про трафік для цілей, *зокрема* , кримінального провадження. Вони містили дані, необхідні для ідентифікації джерела повідомлення, такі як ім'я та адреса абонента, якому була призначена певна IP-адреса, дані, необхідні для ідентифікації напрямку повідомлень, і дані, необхідні для визначення дати, часу і тривалості спілкування (розділи 107.a і 107.b). У зв'язку з цим не існувало жодного розрізнення статичною і динамічної IP-адреси. Крім того, поправка , запроваджена секцією 107.č , передбачала , що оператор мав зобов'язання надати доступ або передати збережені дані негайно і не пізніше ніж через три дні після отримання копії «наказу» виданого "компетентним органом". Розділ 107.e виправленого Закону передбачав, що «суду , який наказав оцінити деякі дані, повинен зберігати записи стосовно наказів про доступ і передачі збережених даних ». Він також регулює d процедури звітування про доступ до збережених даних - від судів до Міністерства юстиції, а потім від Міністерства до Європейської комісії.

39. 20 грудня 2012 року був прийнятий новий Закон про електронні засоби зв'язку ("ЕСА-1", " Офіційний вісник № 109/2012"). Його розділи з 166 до 168 передбачають наступне:

стаття 166

Передача збережених даних компетентним органам

« (1) оператор повинен негайно або без неналежних затримок передавати збережені дані як тільки він отримує копію резолютивної частини наказу компетентного органу з зазначенням всіх необхідних даних про масштаби доступу.

...

(4) Оператор не може розкрити наказ особам, яких стосується наказ, або третім сторонам, а також не розголошувати те, що він передав або буде передавати збережені дані компетентному орган відповідно до цього розділу.

...

(7) Уповноважений з питань інформації здійснює моніторинг виконання зобов'язань провайдерами відповідно до цього розділу, оскільки вони не підпорядковуються нагляду інших компетентних органів на підставі інших законів ".

стаття 168

Дані про накази про надання доступу та дані про передачу

" (1) Суд, який видав наказ про надання доступу до даних, повинен вести облік наказів про надання доступу та передачі даних, збережених відповідно до розділу 166 цього Закону, який складається з:

1. кількості справ , в яких був виданий наказ про надання доступу до збережених даних;

2. витягів про дату або період, за який був поданий запит для отримання даних, дату, коли компетентний орган видавав наказ про надання доступу до даних та дату передачі даних;

3. кількість справ, в яких накази про надання доступу до даних не можуть бути виконані.

(2) Компетентний суд передає міністерству відповідальному за правосуддя , не пізніше 31 січня наступного року запис, зазначений у підпункті (1) вище, за поточний рік.

(3) Міністерство , відповідальне за правосуддя, повинне, на підставі записів , отриманих від усіх судів, підготувати спільний звіт про доступ до збережених даних по не пізніше 20 лютого кожного року за попередній рік. Він передає його міністерству, яке повинне, в свою чергу , передати його без затримки Європейській Комісії та Комітету національних зборів, відповідальному за нагляд за службою розвідки і службою безпеки.

(4) Міністерство, відповідальне за правосуддя, повинне, після отримання попередньої думки Голови Верховного суду Республіки Словенії, видати вказівки з використанням форм звітності відповідно до цього розділу. "

D. Закон про захист персональних даних

40. Крім того, для того, щоб Словенія стала членом Європейського Союзу, Парламент Словенії ухвалив15 липня 2004 рок новий Закон про захист персонаьних даних (Офіційний вісник №. 86/ 04), підкріплений Директивою 95/46 / ES (дивіться пункт 53 нижче) Він, наскільки це є доречним, передбачає:

стаття 1

Зміст закону

"Цей Закон визначає права, обов'язки, принципи та заходи для запобігання неконституційних, незаконних та необґрунтованих посягань на недоторканість та гідність особи (далі - особа) під час обробки персональних даних".

стаття 6

Значення термінів

«Терміни, які використовуються в цьому Законі, мають наступне значення:

1. Персональні дані - це будь-які дані, що стосуються особи незалежно від форми, в якій вони виражені.

2. Особа - це ідентифікована або фізична особа, яку можливо ідентифікувати та якої стосуються персональні дані; фізична особа, яку можливо ідентифікувати, є особою, яка може бути ідентифікована безпосередньо або побічно, зокрема, за посиланням на ідентифікаційний номер або на один або більше факторів, характерних для його фізичної, фізіологічної, психічної, економічної, культурної або соціальної ідентичності, а метод ідентифікації не викликає значні витрати або непропорційно великі зусилля, чи вимагає великої кількості часу.

...

18. Анонімізація - це зміна форми персональних даних у такий спосіб, що вони вже не були пов'язані з особою або такий зв'язок мін бути встановлений за непропорційних зусиль, витрат або кількості часу.

19. Конфіденційні персональні дані - це дані про расове, національне або етнічне походження, політичні, релігійні або філософські переконання, членство в профспілках, стан здоров'я, сексуальне життя ... "

41. Розділ 2 Закону про захист персональних даних передбачає, що персональні дані повинні оброблятися законно та справедливо. Розділ 8 передбачав, що персональні дані можуть бути оброблені , якщо закон передбачав це або на основі згоди потерпілої особи. Відповідно до статті 12 персональні дані можуть бути оброблені без будь-якої іншої правової онови , якщо це терміново необхідно для захисту життя і здоров’я особи.

42. Закон про захист персональних даних також передбачав , що дані можуть бути зібрані лише для визначених і законних цілей, та оброблені у відповідний спосіб (розділ 16) і лише за умови , що це було необхідно для досягнення цих цілей (розділ 21). Після цього вони повинні бути видалені, знищені, заблоковані або анонімізовані (в тому ж місці). В Закону також викладені заходи і процедури , які повинні бути вжиті операторами і обумовленими угодою особами, які обробляють дані, для захисту персональних даних, а

також для запобігання випадкового або умисного несанкціонованого знищення даних, їх зміну, втрати або несанкціонованої обробки (розділи 24 і 25).

E. Кримінальний кодекс

43. Кримінальний кодекс, застосовний у відповідний час, забороняв в своїй статті 187 презентацію порнографічних матеріалів неповнолітніх у віці до чотирнадцяти років, а також створення та розповсюдження порнографічних матеріалів з зображенням неповнолітніх. Відповідні положення мають наступний зміст:

" ...

(2) Будь-яка особа, як експлуатує неповнолітніх для виготовлення порнографічних зображень, аудіовізуальних та інших об'єктів порнографічного змісту, або використовує неповнолітнього для здійснення порнографічного виступу, засуджується на термін ув'язнення від шести місяців до п'яти років ув’язнення.

(3) Будь-яка особа, яка створює, розповсюджує, продає, імпортує або експортує порнографічні або інші матеріали сексуального характеру з зображенням неповнолітніх, поставляє його за допомогою іншого способу, або володіє таким матеріалом з наміром створення, розповсюдження, продажу, імпорту, експорту або пропонування його за допомогою будь-якого іншого способу, підлягає такому ж покаранню, як і в підпункті 2 вище .

... "

F. Рішення Конституційного суду № Up-106/05 від 2 жовтня 2008 року

44. Справа Up-106/05 стосувався заявника, який був визнаний винним в незаконному виготовленні та торгівлі наркотиками на основі даних (список телефонних номерів та текстових повідомлень), отриманих з його SIM-карти без рішення суду. Він скаржився на те, що його засудження було засноване на незаконно отриманих доказах, оскільки поліція слідкувала за його мобільним телефонним зв'язком без наказу суду. Конституційний суд задовольнив скаргу і скасував рішення судів нижчої інстанції.

45. Конституційний Суд виявив, що захисту підлягали не лише зміст повідомлення, а й обставини і факти, пов'язані з цим, в тому числі дані, збережені в пам'яті телефону, які були невід'ємним елементом конфіденційності спілкування. Таким чином, отримання даних про останні набрані і неприйняті виклики викликає вивчення змісту і обставин спілкування, і отже, складало втручання в права, визначені в першому параграфі статті 37 Конституції. Суд зазначив, що таке втручання відповідно до статті 37§2 Конституції було прийнятним, якщо виконувалися наступні умови: (1) втручання було передбачене законом ; (2) втручання було дозволено на підставі наказу суду; (3) тривалість втручання була точно визначена; і (4) втручання було необхідним для відкриття або здійснення кримінального провадження, або з міркувань національної безпеки.

III. ВІДПОВІДНЕ МІЖНАРОДНЕ ПРАВО

A. Конвенція про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних

46. Конвенція про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних (відкрита для підписання 28 січня 1981 року ETS № 108, далі «Конвенція від 1981 року») була ратифікована всіма державами-членами Ради Європи і набула чинності щодо Словенії 1 вересня 1994 року[1]. В статті 1 викладені об'єкт і мета Конвенції, якою є «забезпечення на території кожної Сторони для кожної особи, незалежно від її громадянства або місця проживання, дотримання її прав й основоположних свобод, зокрема її права на недоторканість приватного життя, у зв'язку з автоматизованою обробкою персональних даних, що її стосуються (далі - захист даних)». Конвенція від 1981 року, серед іншого, захищає осіб від зловживань і застосовується до всієї обробки даних, що здійснюється як в приватному і державному секторах, таких як обробка даних по судовими і правоохоронними органами. У статті 2 «персональні дані» означають будь-яку інформацію, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною. Стаття 5 вимагає, щоб персональні дані, що піддаються автоматизованій обробці, повинні отримуватися та оброблятися сумлінно та законно.

B. Конвенція про кіберзлочинність

---

1 Законом України «Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних (Відомості Верховної Ради України (ВВР), 2010, N 46, ст.542) {Із змінами, внесеними згідно із Законом N 383-VII від 03.07.2013, ВВР, 2014, N 14, ст.252 } ратифіковано Конвенцію про захист осіб у зв'язку з автоматизованою обробкою персональних даних, вчинену 28 січня 1981 року в м. Страсбурзі (додається), та Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних, вчинений 8 листопада 2001 року в м. Страсбурзі (додається), які набирають чинності для України в перший день місяця, що настає після закінчення тримісячного періоду від дати здачі Україною на зберігання її ратифікаційної грамоти, з такими заявами:

до підпункту "a" пункту 2 статті 3 Конвенції: "Україна не буде застосовувати цю Конвенцію до персональних даних, які обробляються фізичними особами виключно для непрофесійних особистих чи побутових потреб";

до підпункту "b" пункту 2 статті 3 Конвенції: "Україна буде застосовувати цю Конвенцію до інформації, яка стосується груп осіб, асоціацій, фондів, компаній, корпорацій та будь-яких інших організацій, що безпосередньо чи опосередковано складаються з окремих осіб, незалежно від того, мають чи не мають такі установи статус юридичної особи";

до підпункту "c" пункту 2 статті 3 Конвенції: "Україна буде застосовувати цю Конвенцію до файлів персональних даних, які не обробляються автоматизовано";

до пункту 2 статті 13 Конвенції (994_326): "Органом, на який покладаються повноваження згідно з пунктом 2 статті 13 Конвенції (994_326), є Уповноважений Верховної Ради України з прав людини". {Абзац дев'ятий статті 1 із змінами, внесеними згідно із Законом N 383-VII від 03.07.2013 }.

Цей Закон набирав чинності одночасно з набранням чинності Законом України "Про захист персональних даних" (крім статті 3 цього Закону, яка набирала чинності з дня опублікування цього Закону).

47. Конвенція про кіберзлочинність (відкрита для підписання 23 листопада 2001 року, набула чинності 1 липня 2004 року, ETS № 185, далі "Конвенція про кіберзлочинність")[2] в Словенії стала чинною 1 січня 2005 року.

48. Конвенція про кіберзлочинність - це перша міжнародна угода про злочини, скоєні через Інтернет, яка є відкритою для всіх держав. Вона вимагає від держав визнання кримінальними правопорушеннями, зокрема, дитячу порнографію.

49. Стаття 1 визначає для цілей Конвенції про кіберзлочинність "дані про рух інформації" означає будь-які комп'ютерні дані, пов'язані з комунікацією за допомогою комп'ютерної системи, які були створені комп'ютерною системою, що складала частину ланцюга комунікації, і які зазначають походження, кінцевий пункт, маршрут, час, дату, розмір і тривалість комунікації або тип основної послуги.". Пояснювальний звіт у відповідній частині передбачає наступне (§ 30) :

> «Походження» стосується номера телефону, адреси Інтернет-протоколу (IP-адреса), або подібне визначення об'єкта зв'язку, яку постачальник послуг надає послуги. «Кінцевий пункт» стосується порівняльної вказівки на об'єкт зв'язку, якому передаються повідомлення. Термін «тип основної послуги» стосується типу послуги, яка використовується в мережі, наприклад, передача файлів, електронна пошта або обмін миттєвими повідомленнями ".

50. Відповідно до Конвенції про кіберзлочинність для органів влади повинні бути доступні наступні заходи для боротьби зі злочинами, про які йде мова:

Стаття 18 – Порядок представлення

"1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для надання повноважень своїм компетентним органам видавати ордери:

---

2 Законом України «Про ратифікацію Конвенції про кіберзлочинність» 7 вересня 2005 року N 2824-IV (Із змінами, внесеними згідно із Законом N 2532-VI (від 21.09.2010)) Конвенцію про кіберзлочинність, підписану від імені України 23 листопада 2001 року в м. Будапешті, ратифіковано з такими застереженнями і заявами:

до пункту 1 статті 6: Україна залишає за собою право не застосовувати пункт 1 статті 6 Конвенції в частині встановлення кримінальної відповідальності за виготовлення, придбання для використання, надання для використання іншим чином предметів, зазначених у підпункті 1.a.i, та виготовлення і придбання для використання предметів, зазначених у підпункті 1.a.ii статті 6 Конвенції;

до пункту 1 статті 9: Україна залишає за собою право не застосовувати повністю підпункти 1.d та 1.e статті 9 Конвенції;

відповідно до підпункту 7.a статті 24: в Україні органами, на які покладаються повноваження згідно з пунктом 7 статті 24 Конвенції, є Міністерство юстиції України (щодо запитів судів) і Генеральна прокуратура України (щодо запитів органів досудового слідства);

відповідно до підпункту 2.c статті 27: в Україні органами, відповідальними за надсилання запитів про взаємну допомогу, надання на них відповідей, їх виконання або передачу уповноваженим органам, є Міністерство юстиції України (щодо доручень судів) та Генеральна прокуратура України (щодо доручень органів досудового слідства);

відповідно до пункту 1 статті 35: {Закон доповнено абзацом згідно із Законом N 2532-VI від 21.09.2010} в Україні органом, на який покладаються повноваження щодо створення та функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі, є Міністерство внутрішніх справ України. {Закон доповнено абзацом згідно із Законом N 2532-VI від 21.09.2010}.

...

b) постачальнику послуг, який пропонує свої послуги на території Сторони - про надання інформації про користувача послуг, пов'язаної з такими послугами, яка знаходиться у власності або під контролем такого постачальника послуг.
2. Повноваження і процедури, на які містяться посилання у цій статті, регулюються положеннями статей 14 і 15.
3. Для цілей цієї статті термін "інформація про користувача послуг" означає будь-яку інформацію, у формі комп'ютерних даних чи у іншій формі, яка знаходиться у постачальника послуг, відноситься до користувачів його послуг, не є даними про рух даних або власне даними змісту інформації, та за допомогою якої можна встановити:

a. тип комунікаційної послуги, яка використовувалася, її технічні положення і період користування послугою;

b. особистість користувача послуг, поштову або географічну адресу, телефони та інший номер доступу, інформацію про рахунки і платежі, яку можна отримати за допомогою угоди або домовленості про постачання послуг;

c. будь-яку іншу інформацію про місце встановлення комунікаційного обладнання, яку можна отримати за допомогою угоди або домовленості про постачання послуг".

Стаття 20 - Збирання даних про рух інформації у реальному масштабі часу

"1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для надання своїм компетентним органам повноважень:

a. збирати або записувати технічними засобами на території такої Сторони, та

b. зобов'язувати постачальника послуг, в межах його існуючих технічних можливостей:

i. збирати або записувати технічними засобами на території такої Сторони; або

ii. співробітничати і допомагати компетентним органам у зборі або запису даних про рух інформації у реальному масштабі часу, які пов'язані з визначеною передачею інформації на її території, яка передається за допомогою комп'ютерних систем.

...

4. Повноваження і процедури, на які містяться посилання у цій статті, регулюються положеннями статей 14 і 15."

Стаття 21 - Перехоплення даних змісту інформації

" 1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними стосовно певних серйозних злочинів, які визначаються внутрішньодержавним законодавством, для надання повноважень своїм компетентним органам:

a. збирати або записувати технічними засобами на території такої Сторони, або

b. зобов'язувати постачальника послуг, в межах його існуючих технічних можливостей:

i. збирати або записувати технічними засобами на території такої Сторони; або

ii. співробітничати і допомагати компетентним органам у зборі або запису даних змісту інформації у реальному масштабі часу, які належать до визначеної передачі інформації на її території, яка здійснюється за допомогою комп'ютерних систем.

...

4. Повноваження і процедури, на які містяться посилання у цій статті, регулюються положеннями статей 14 і 15".

51. Стосовно порядку подання, в Пояснювальному звіті до Конвенції про кіберзлочинність (Будапешт, 23 листопада 2001 року, ETS № 185) зазначено, що під час кримінального розслідування інформація про абонентів може знадобитися переважно у двох ситуаціях. По-перше для того, щоб визначити, які послуги та відповідні технічні заходи були використані або використовуються абонентом, наприклад тип використовуваного телефонного зв'язку, тип інших пов'язаних засобів зв'язку, які використовуються (наприклад, переадресація викликів, голосова пошта) або номер телефону чи інша технічна адреса (наприклад, адреса електронної пошти). По-друге, якщо відома технічна адреса, інформація про абонента необхідна для того, щоб допомогти ідентифікувати особу, про яку йде мова. Згідно з пояснювальним звітом порядок подання забезпечує менш нав'язливі і менш обтяжливі заходи , які правоохоронні органи можуть застосовувати замість таких заходів як перехоплення даних про зміст і збір даних про трафік в режимі реальному часі, які повинні або можуть бути обмежені лише серйозними правопорушеннями.

52. Конвенція про кіберзлочинність вимагає , щоб вищезазначені заходи , передбачені статтями 18, 20 і 21 підпорядковувалися умовам, викладеним в статтях 14 і 15, які, наскільки це є доречним, мають наступний зміст:

Стаття 14 – Сфера процедурних положень

"1. Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для визначення повноважень і процедур, передбачених цією частиною, з метою конкретних кримінальних розслідувань або переслідувань.

... "

Стаття 15 - Умови і запобіжні заходи

"1. Кожна Сторона забезпечує, щоб встановлення, імплементація і застосування повноважень і процедур, передбачених цією частиною, регулювалися умовами і запобіжними заходами, передбаченими її внутрішньодержавним правом, які б забезпечували адекватний захист прав і свобод людини, включаючи права, що випливають із зобов'язань за Конвенцією Ради Європи про захист прав людини і основних свобод 1950 р., Міжнародною Хартією ООН про громадянські і політичні права 1966 р., та інших відповідних міжнародних угод з прав людини, і які б включали в себе принцип пропорційності.
2. Такі умови і запобіжні заходи включатимуть, між іншим, як це є доречним з огляду на природу відповідного повноваження або процедури, судовий або інший незалежний нагляд, підстави, які виправдовують застосування, і обмеження сфери застосування і терміну таких повноважень або процедур".

IV. ВІДПОВІДНЕ ЗАКОНОДАВСТВО ЄС

A. Директива 95/46/ЄС та Регламент (ЄС) 2016/679

53. Стаття 2 (1) (a) Директиви Європейського Парламенту та Ради Європейського Союзу 95/46/ЄС від 24 жовтня 1995 року «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» (OJ 1995 L 281, стор. 31, далі «Директива

про захист даних») передбачає, що «персональні дані означають будь-яку інформацію, що стосується встановленої фізичної особи чи фізичної особи, яку можна встановити ("суб'єкт даних")». Крім того, згідно з вищезазначеними положеннями «особою, яку можна встановити, є така, яка може бути встановленою прямо чи непрямо, зокрема, за допомогою ідентифікаційного коду або одного чи більше факторів, притаманних фізичним, фізіологічним, розумовим, економічним, культурним чи соціальним аспектам її особистості". Директива про захист даних не застосовується до сфери поліції та кримінального правосуддя.

54. Пункт 26 цієї Директиви передбачає, що під час визначення того, чи можливо ідентифікувати особу, «повинні враховуватися всі засоби, які, ймовірно, є обґрунтованим використовувати ... для ідентифікації зазначеної особи»; принципи захисту не застосовуються до даних, що надані анонімно таким чином, що суб'єкт даних не може бути встановлений.

55. Регламент 2016/679 Європейського Парламенту та Ради (ЄС) від 27 квітня 2016 року про захист фізичних осіб у зв’язку з опрацюванням персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) набули чинності 24 травня 2016 року[3]. Після набуття чинності (25 травня 2018 року) воно замінило Директиву про захист даних. Стаття 4 визначає " фізичну особу, яку можна ідентифікувати" як "особу, є такою особою, яку можна ідентифікувати, прямо чи опосередковано, зокрема, за такими ідентифікаторами як ім’я, ідентифікаційний номер, дані про місцеперебування, онлайн-ідентифікатор..". У пункті 26 цього Регламенту далі передбачено, що під час з'ясування того, чи можливо обґрунтовано використовувати засоби для визначення фізичної особи «необхідно враховувати всі об'єктивні фактори, такі як витрати та період часу, необхідні для ідентифікації з огляду на доступної технології, наявні станом на час опрацювання, а також технологічні розробки ". У цьому пункті також пояснюється, що «принципи захисту даних не повинні застосовуватися до анонімної інформації, а саме інформації, яка не стосується фізичної особи, яку ідентифіковано або можливо ідентифікувати, або персональних даних, що стали анонімними у такий спосіб, що суб'єкта даних неможливо чи більше неможливо ідентифікувати.»

B. Директива 2002/58/ЄС

56. Крім того, спеціально для сфери електронних засобів зв'язку, Директива 2002/58/ЄС Європейського Парламенту та Ради від 12 липня 2002 року щодо обробки персональних даних та захисту конфіденційності в секторі електронних засобів спілкування (Директива про приватне життя та електронні засоби зв'язку) (OJ 2002 L 201) була прийнята 12 липня 2002 року. Вона не застосовується до сфери поліції та кримінального правосуддя, але гармонізує положення держав-членів, які повинні забезпечити однаковий рівень захисту основних прав та свобод, зокрема, права на конфіденційність приватного життя стосовно обробки особистих даних у секторі електронних засобів спілкування. Стаття 2 передбачає визначення "користувача" як "будь-яку фізичну особу, яка використовує загальнодоступну послугу електронних засобів зв’язку для приватних або ділових цілей без обов'язкової попередньої підписки на надання такої послуги". Вона далі визначає «дані про трафік" як "будь-які дані, оброблені з метою здійснення передачі повідомлення мережею

3 Для України цей Регламент набрав чинності 25 травня 2018 року.

електронного зв’язку або в цілях формування формування рахунку за користування послугами електронного зв’язку". Крім того, вона визначає "повідомлення" як "будь-яку інформацію, якою обмінюються або яку передають між обмеженим колом осіб за допомогою загальнодоступної послуги електронного зв'язку".

C. Рамкове Рішення Ради 2008/977/JHA та Директива (ЄС) 2016/680

57. Рамкове Рішення Ради 2008/977 / JHA від 27 листопада 2008 року про захист персональних даних, які обробляються в рамках співпраці поліції та судової влади у кримінальних справах (OJ 2008 L 350, p. 60, далі " Рамкове рішення про захист даних ") спрямоване на забезпечення захисту особистих даних фізичним особам, коли їх особисті дані обробляються з метою запобігання, розслідування, виявлення або переслідування кримінального злочину чи виконання кримінального покарання. Рамкове рішення про захист даних в значній мірі посилається на принципи та визначення, які містяться у Конвенції від 1981 року та Директиві про захист даних.

58. Директива ЄС (ЄС) 2016/680 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб стосовно обробки особистих даних компетентними органами влади з метою запобігання, розслідування, виявлення та переслідування кримінального злочину або виконання кримінальних покарань, а також щодо вільного переміщення таких даних та скасування Рамкового рішення Ради 2008/977 / JHA (OJ 2016 L 119, p. 89) регулює обробку даних компетентними органами влади, такими як поліція та органи кримінального правосуддя, з метою, *зокрема* , розслідування та переслідування кримінального злочину. Стаття 3 (1) містить те саме визначення "фізичної особи, яку можливо ідентифікувати", а пункт 21 - те саме пояснення щодо засобів ідентифікації як в Загальному регламенті про захист даних (дивіться пункт 55 вище). Крім того, стаття 4 вимагає, щоб особисті дані, *зокрема*, обробляли законно та справедливо. Стаття 1 (3) передбачає , що держава-учасниця може передбачати більш високі гарантії, ніж гарантії, які містяться в Директиві.

59. Директива замінює Рамкове Рішення 2008/977/JHA та набуває чинності 6 травня 2018 року.

D. Відповідні рішення Суду Європейського Союзу

60. Стосовно концепції "персональних даних " згідно зі статтею 2 (a) Директиви про захист даних, Суд Європейського Союзу (CJEU) у своєму рішенні від 24 листопада 2011 року у справі «*Scarlet Extended*» (C-70/10) ЄС: C: 2011: 771, пункт 51, виявив, що IP – адреси користувачів були «захищеними персональними даними, оскільки вони дозволяють точно визначити особи цих користувачів».

61. У своєму рішенні від 19 жовтня 2016 в *Брейер,* C-582/14, ЄС : C: 2016: 779, CJEU розглядав питання про особливий характер динамічних IP-адрес. Суд зазначає наступне:

> "[15] IP-адреси є серією цифр, призначених комп'ютерам в мережі для полегшення їх зв'язку через Інтернет. Коли отримується доступ до веб-сайту IP-адреса комп'ютера,

який намагається отримати доступ, повідомляється серверу, на якому зберігається веб-сайт, до якого звертаються за довідкою. Це з'єднання необхідно для того, щоб дані, до яких отримується доступ, могли бути передані правильному одержувачу.

[16] Крім того, з наказу про посилання та документів Суді очевидно, що провайдери інтернет-послуг призначають комп'ютерам користувачів Інтернету як "статичну" IP-адресу, або " динамічну " IP-адресу, тобто IP-адреса, яка змінюється кожного разу, коли з'являється нове підключення до Інтернету. На відміну від статичних IP-адрес, динамічні IP-адреси не дозволяють встановлювати зв'язок між файлами, доступними для громадськості, між даним комп'ютером та фізичним з'єднанням із мережею, яке використовується провайдером інтернет послуг ».

62. CJEU вважав, що динамічна IP-адреса не складала інформацію, яка стосується «фізичної особи, яку можливо ідентифікувати», оскільки така адреса безпосередньо не виявляла ідентичність фізичної особи, яка володіла комп'ютером, з якого був отриманий доступ до веб-сайту, або іншої особи, яка могла б використати цей комп'ютер (в тому ж місці, § 38). CJEU продовжував визначати, чи динамічна IP-адреса в цій справі, зареєстрована постачальником онлайн засобів масової інформації, може розглядатися як дані, які стосуються «фізичної особи, яку можливо ідентифікувати» в значенні статті 2 (a) Директиви про захист даних. З цією метою CJEU посилаючись на виклад 26 розглянув, чи можливість поєднання динамічної IP-адреси, яка у справі, про яку йде мова, знаходилася в руках постачальника послуг онлайн засобів масової інформації з додатковими даними, які належать інтернет-провайдеру, складало засіб, який можливо було обґрунтовано використовувати для ідентифікації суб'єкта даних (§§ 41 і 45). ECJU дійшов наступного висновку з цього питання:

"[49] З огляду на всі вищезазначені міркування відповідь на перше питання полягає в тому, що стаття 2 (a) Директиви 95/46 повинна тлумачитися як так, яка означає, що динамічна IP-адреса, зареєстрована постачальником послуг онлайн засобів масової інформації, коли особа отримує доступ до веб-сайту, який провайдер робить доступним для громадськості, складає персональні дані у значенні цього положення стосовно цього провайдера, якщо останній має законні засоби, які дозволяють йому ідентифікувати суб'єкта даних за допомогою додаткових даних, які має інтернет-провайдер про цю особу ".

V. ПОРІВНЯЛЬНЕ ПРАВО

A. Федеральний конституційний суд Німеччини

63. Заявник посилався на рішення Федерального конституційного суду Німеччини («GFCC») від 24 січня 2012 року, BVerfG, 1 BvR 1299/05. GFCC частково задовольнили скарги, які стосуються, *зокрема*, неавтоматичного пошуку інформації про динамічні IP-адреси, які зберігають провайдери телекомунікаційних послуг.

64. Відповідно до розділу 113 Закону про телекомунікації («TCA») провайдери телекомунікаційних послуг були зобов'язані поставляти, на запит компетентних органів (в

тому числі правоохоронних), інформацію про деякі зібрані дані з метою, *зокрема*, переслідування кримінальних злочинів або нормативних правопорушень. Оскаржене законодавче положення було створене для того, щоб надати можливість, якщо це є здійсненним, привласнити всі номери телекомунікацій своїм відповідним абонентам (і додатково, в кінцевому підсумку, якщо можливо, їх користувачам). Як виявив GFCC, це положення не надавало жодних певних порогів вторгнення, які б визначало його обсяг більш докладно. Натомість, воно завжди надавало дозвіл на інформацію в кожній окремій справі, якщо це було необхідно для виконання вищезазначених обов'язків. GFCC не визнав це неконституційним. Проте, питання, яке також виникло, полягало в тому, чи оскаржене положення також охоплювало інформацією про власника з динамічної IP-адреси. Спочатку GFCC розглянув питання про зв'язок між інформацією абонента та попередньою інформацією про зміст, яка може бути приписана йому. Він виявив наступне (§ 113, цитата з перекладу, наданому на веб-сайті GFCC):

> " ... конфіденційність телекомунікацій [Стаття 10.1 Основного Закону] не захищає конфіденційність обставин кожного надання послуг телекомунікацій, таких як, наприклад, присвоєння номерів телекомунікацій, що надаються постачальниками послуг для певних абонентів. "

65. GFCC далі зазначив відмінність між статичними і динамічними IP-адресами, виявивши наступне (§§ 115 і 116):

> " ... присвоєння статичної IP-адреси певному абоненту - точніше мережевому інтерфейсу абонента - як правило, також надає непряму інформацію про певну телекомунікаційну подію, пов'язану з цією особою, оскільки такі адреси, навіть якщо вони статичні, є зареєстрованими і стають предметом приписувань, які ідентифікують особу майже лише у зв'язку з певними подіями спілкування. Проте в цій справі також передача інформації у зв'язку з цим обмежується винятково абстрактним присвоєнням номера та абонента.
>
> ... На противагу цьому ситуація відрізняється, коли динамічні IP-адреси приписуються ідентифікованим особам, оскільки такі адреси особливо тісно пов'язані з певними телекомунікаційними подіями. Це віднесення підпадає під сферу захисту статті 10.1 Основного закону. Проте в цій справі з цього факту автоматично не витікає, що присвоєння динамічної IP-адреси обов'язково завжди пов'язане з певною подією телекомунікацій, про яку побічно також надається інформація. Бо у зв'язку з цим також інформація стосується лише даних, абстрактно віднесених до абонента. Отже, не існує принципових відмінностей від присвоєння статичних IP-адрес. Проте застосування Статті 10.1 Основного Закону полягає в тому, що коли телекомунікаційні підприємства ідентифікують динамічну IP-адресу, вони повинні зробити проміжний крок, в якому вони вивчають відповідні дані про з'єднання своїх клієнтів, тобто [вони] повинні мати певні телекомунікаційні події. Ці телекомунікаційні зв’язки, які окремо зберігаються провайдерами послуг, підпорядковуються конфіденційності телекомунікацій незалежно від того, чи повинні вони залишатися доступними постачальникам послуг відповідно до законодавства ... або вони зберігаються ними на договірній основі. Оскільки законодавчий орган покладає на телекомунікаційні

підприємства обов’язок доступу до цих даних і оцінювання їх в інтересах виконання державою своїх зобов'язань, це є порушенням статті 10.1 Основного закону. Це відбувається не лише у випадку, коли постачальники послуг повинні самостійно надавати дані про з'єднання, а також, якщо вони повинні використовувати дані як попередній запит для отримання інформації. "

66. GFCC дійшов висновку, що розділ 113,1 TCA порушував статтю 10.1 Основного закону тому, що він був основою для надання інформації про динамічну IP-адресу.

67. Крім того, незважаючи на те, зо GFCC не виявив автоматичний пошук даних (розділ 12 TCA) щодо статичної IP-адреси неконституційним, такий висновок був зроблений стосовно обмеженого використання таких адрес в наступному контексті (§§ 160 і 161) :

" ... Виділення статичних IP-адрес, виділення яких в цій справі було публічно доступним на практиці, суттєво обмежується установами та великими користувачами. Можливість отримання таких цифр мала невелике значення за цих обставин .

Проте § 112 TKG [TCA] може набувати набагато більше значення порушення, якщо статичні IP-адреси в майбутньому - наприклад, на основі Інтернет-протоколу версії 6 - повинні більш широко використовуватися як основа інтернет-зв'язку. Питання про значення вторгнення в ідентифікацію IP-адреси переважно не залежить від того (навіть якщо в цій справі застосовується ряд фундаментальних прав), чи IP-адреса технічно є динамічною або статичною, але від фактичного значення створення обов'язку щодо інформації у зв’язку з цим. Але якщо на практиці статичні IP-адреси значною мірою призначаються також і приватним особам, це може означати, що ідентичність користувачів Інтернету широко або принаймні значно визначена, а події зв'язку в інтернеті деанонімізуються не лише на обмежений проміжок часу, але назавжди. Така далекоглядна можливість деанонімізації спілкування в інтернеті виходить за межі впливу традиційного реєстру номерів телефону. ... Значення для особи, яка постраждала від призначення IP-адреси абоненту, не може бути прирівняне до ідентифікації номера телефону, оскільки перший дає змогу отримувати доступ до інформації, сфери та змісту, що суттєво є більш далекосяжним.... З огляду на цей підвищений інформаційний потенціал загальна можливість ідентифікації IP-адреси буде конституційно прийнятною лише за умови більш вузьких обмежень ... "

B. Канадський Верховний Суд

68. Справа *R проти Спенсера* (2014 SCC 43, [2014] 2 SCR 212) стосувалася пошуку без попереднього судового дозволу інформації про абонента, поєднаного з динамічною IP-адресою, сестри заявника, яку поліція отримала у зв'язку з онлайн обміном файлів із дитячою порнографією. На основі інформації про абонента, отриманої від провайдера, поліція отримала ордер на обшук проти позивача по апеляції. Останній намагався вилучити докази, знайдені в його комп'ютері, на підставі того, що дії поліції щодо отримання його адреси у провайдера без попереднього судового дозволу складало необґрунтований пошуку, який суперечить Хартії прав і свобод Канади. Рішення

Верховного суду Канади («SCC ») від 13 червня 2014 року на користь позивача по апеляції було прийняте суддею Кромвель.

69. Посилаючись на попереднє прецедентне право з цього питання суд зазначив, що обґрунтоване очікування стандартів конфіденційності було нормативним, а не лише дескриптивним, а також те, що воно неминуче було "наповнене цінними суб'єктивним оцінюванням, яке було зроблене з незалежної точки зору розсудливою і проінформованою особою, яка була занепокоєна довгостроковими наслідками дії уряду щодо захисту конфіденційності" (§ 18). SCC всупереч думці суду першої інстанції, виявив, що суб'єктивне очікування конфіденційності позивача по апеляції було обґрунтоване тим фактом, що він був особою, яка використовує мережеве з'єднання для передачі конфіденційної інформації. Суд продовжив визначати, чи суб'єктивне очікування конфіденційності позивача по апеляції було обґрунтованим. З цією метою в рішенні були розглянуті дві обставини: характер інтересів конфіденційності, які є головними в цій справі, і нормативно-договірної бази, яка регулює розкриття інформації про абонентів Інтернет-провайдерами". Стосовно попереднього, суддя Кромвел дійшов наступних висновків:

> " [31] Таким чином, зрозуміло, що тенденція отримання інформації, яка спрямована на підтримку висновків стосовно іншої особистої інформації, повинна враховуватися під час оцінювання предмета пошуку.
>
> [36] ... Аналіз містить конфіденційність сфери або речі, які шукають, а також вплив пошуку на його ціль, а не законний чи незаконний характер елементів, які намагаються отримати ...
>
> [41] Існує також третя концепція конфіденційності інформації, яка є особливо важливою в контексті використання Інтернету. Це - розуміння конфіденційності як анонімності. На мою думку, концепція конфіденційності потенційно захищена р. 8 [право бути захищеним від необґрунтованого обшуку або конфіскації] повинна містити це розуміння конфіденційності.
>
> [50] ... За обставин цієї справи запит поліції про зв'язок певної IP-адреси з інформацією про абонента фактично є запитом про встановлення зв'язку певної особи (або обмеженої кількості осіб у випадку спільних Інтернет-послуг) з певними заходами в Інтернеті. Цей вид запиту зачіпає аспект анонімності інтересу конфіденційності інформації намагаючись встановити зв'язок підозрюваного з анонімно здійснюваною діяльністю в Інтернеті, діяльністю, яка була визнана Судом за інших обставин як залучення значних інтересів конфіденційності ... .
>
> [51] Таким чином, я дійшов висновку, що запит поліції до Shaw [ISP] щодо інформації про абонента, яка відповідає особливо спостереженій, анонімній діяльності в Інтернеті, передбачає високий рівень конфіденційності інформації. Я згоден з висновком Дж. А. Колдвелла з цього питання:
>
> .. . розсудлива і поінформована особа, занепокоєна захистом приватного життя буде очікувати те, що діяльність особи на власному комп'ютері у власному будинку буде приватною. На мою думку, не має значення, що особисті характерні риси розкритої

> інформації стосувалися сестри пана Спенсер тому, що пан Спенсер особисто і безпосередньо піддавався впливу наслідків поведінки поліції в цій справі. Таким чином, поведінка поліції *prima facie* залучала право пана Спенсера на приватне життя, і у зв'язку з цим його інтерес в конфіденційності розкритої інформації є прямим та особистим ... "

70. В рішенні також надана відповідь на занепокоєння прокуратури в тому, що визнання права на онлайн анонімність знищить адаптований до злочинів інтернет пейзаж. Визнаючи, що це занепокоєння не може бути непоміченим, суддя Кромвелл пояснив, що визнання інтересу не може бути прирівняне до права на анонімність, а також те, що в цій справі, наприклад, здавалося очевидним, що поліція могла легко отримати порядок подання для отримання інформації про абонента.

71. Стосовно питання, чи було очікування конфіденційності обґрунтованим в умовах відповідних договірних і законодавчих положень, в рішенні було виявлено, що збір ISP, використання і розкриття особистої інформації про своїх абонентів підпорядковувалися Закону про захист особистої інформації та електронні документи (" PIPEDA "), який захищав особисту інформацію, якою володіють організації, які здійснюють комерційну діяльність, від розкриття без відома або згоди особи, якої стосується інформація. Рішення викладає наступне:

> «[62] Розділ 7 (3) (*гр.* 1) (б) надає дозвіл розкриття без згоди урядові установі, якщо ця установа вказала свої *законні повноваження* отримати інформацію. Але питання полягає в тому, чи існували такі законні повноваження, які, у свою чергу, частково залежить від того, чи існують обґрунтовані очікування конфіденційності інформації про абонента. Таким чином *PIPEDA* не може бути використаний як фактор, який зважує проти існування обґрунтованого очікування конфіденційності ... З урахуванням того, що метою *PIPEDA* є встановлення правил, які регулюють, серед іншого, розголошення "особистої інформації у такий спосіб, який визнає право на конфіденційність приватних осіб стосовно їх особистої інформації" (розділ 3), було обґрунтованим, що Інтернет-користувач може очікувати, що простий запит поліції не викликатиме зобов'язання розкривати особисту інформацію або скасовуватиме загальну заборону *PIPEDA* розкривати особисту інформацію без згоди.*»*

72. В рішенні далі було встановлено, що поліція в своєму запиті не мала законних повноважень, і, отже, інформація була отримана неконституційно. Суд відмовився провести паралель з іншими повсякденними запитами поліції, такими як допит жертви злочину. Посилаючись на справу *R. v. Duarte*, [1990] 1 S.C.R. 30 він виявив наступне :

> "[67] ... У справі *Дуарте* Суд розрізняв особу, яка повторювала розмови з підозрюваним у поліції та поліцію, яка здійснювала аудіозапис цієї ж розмови. Суд постановив, що небезпека «не є ризиком того, що буд-яка повторює наші слова, але значно підступніша небезпека, притаманна наданню дозволу державі на свій необмежений розсуд записувати та передавати наші слова " ... Так само у цій справі запит поліції до інтернет-провайдера розкрити інформацію про абонента дійсно був проханням пов'язати пана Спенсера з певною онлайн-діяльністю, яка була предметом

моніторингу поліції, і, таким чином, залучав значно більший інтерес в конфіденційності, ніж просте запитання, яке поставила поліція під час розслідування ".

ПРАВО

I. СТВЕРДЖУВАНЕ ПОРУШЕННЯ СТАТТІ 8 КОНВЕНЦІЇ

73. Заявник скаржився на те, що його право на приватне життя було порушене тому, що (i) Інтернет-провайдер (далі « ISP ») зберіг його передбачувані особисті дані незаконно і (ii) поліція отримала дані про абонента, пов'язані з його динамічною IP-адресою і, отже, його персональні дані довільно, без судового наказу в порушення статті 8 Конвенції, яка має наступний зміст:

" 1. Кожен має право на повагу до свого приватного і сімейного життя, до свого житла і 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.

".

A. Прийнятність

1 Стосовно передбачуваного незаконного утримання персональних даних Інтернет-провайдером (ISP)

74. Уряд стверджував, що заявник не подав скаргу до національних судів про незаконне збереження його персональних даних ISP. Як наслідок суди не розглядали це питання в оскаржених рішеннях. Крім того, вони стверджували, що, оскільки ISP є приватною юридичною особою, заявник міг би подати позов для відшкодування збитків у цивільному провадженні. Так чи інакше, ця частина заяви, на їх думку, повинна бути визнаною неприйнятною за невичерпання національних засобів судового захисту.

75. Крім того, уряд наполягав, що заявник не міг стверджувати, що він був жертвою передбачуваного порушення статті 8 стосовно утримання персональних даних, оскільки ці дані не стосувалися його, а абонента інтернет-послуг, яким був його батько.

76. Заявник стверджував, що провайдер зберігав його персональні дані протягом майже шести місяців не маючи чіткої правової основи для таких дій і, таким чином, в порушення статті 8 Конвенції. У своїх зауваженнях, поданих 15 жовтня 2015 року, заявник стверджував, що він подав свою скаргу до Суду не тому, що Інтернет-провайдер не зміг зберегти його персональні дані в таємниці або тому, що він зберігав їх поза встановлений законодавством термін, а тому, що держава отримала і використала дані, про які йде мова,

в кримінальному провадженні проти нього. Він стверджував, що він наполягав під час кримінального провадження на тому, що суди покладалися на незаконно отримані докази.

77. Суд зазначає, що уряд заперечував статус жертви заявника щодо цієї скарги. Проте він не вважає необхідним розглядати це заперечення тому, що ця частина заяви в будь-якому випадку є неприйнятною на наступних підставах.

78. Суд зауважує, що метою статті 35**§1** є надання Договірним державам можливості запобігання або виправлення порушень, які були пред'явлені проти них, перш ніж ці твердження будуть передані в установи Конвенції. Це правило є важливим аспектом принципу, згідно з яким механізм захисту, встановлений Конвенцією, є додатковим до національних систем, які забезпечують захист прав людини. Отже, скарга, яка повинна була згодом бути поданою до Суду, повинна була спочатку бути поданою - принаймні по суті - до відповідного національного органу влади та відповідно до офіційних вимог та строків, встановлених національним законодавством (дивіться, серед інших авторитетних джерел, *Сейдовіч проти Італії* [ВП], № 56581/00, §§ 43-44, ЄСПЛ 2006 - II) .

79. В цій справі заявник скаржився в своїй заяві до Суду на збереження ISP того, що він вважав його персональними даними. Проте, йому не вдалося вичерпати національні засоби судового захисту у зв'язку з цим, оскільки він не подав цю скаргу, принаймні по суті, під час провадження в національному суді.

80. Отже, ця частина заяви повинна бути визнана неприйнятною відповідно до статті 35§1 та 4 Конвенції.

2 Стосовно розкриття інформації про абонента

81. Уряд стверджував, що заявник не міг вимагати статусу жертви тому, що інформація про абонента, яку ISP розкрила поліції, стосувалася його батька.

82. Заявник оскаржив це твердження. Він стверджував, що його приватне життя було порушене, а не абонента, а питання, яке було головним в цій справі, полягало не в праві власності, а в праві на приватне життя.

83. Суд зазначає, й у цьому питання тісно пов'язане з сутністю заяви і тому приєднується до заперечення уряду по суті справи.

84. Суд вважає, що ця скарга не є явно необґрунтованою у значенні статті 35 §3 (a) Конвенції. Він також зазначає, що вона не є неприйнятною на будь-яких інших підставах. Тому вона повинна бути визнана прийнятною.

B. Факти

1. Доводи сторін

(a) Заявник

85. Заявник посилався на визначення персональних даних в Конвенції від 1981 року (дивіться пункт 46 вище) стверджуючи, що отримання даних без наказу суду (дивіться пункт 7 вище) викликало його ідентифікацію.

86. Він також стверджував, що, незважаючи на те, він розкрив зміст свого повідомлення громадськості, особи яких неможливо встановити, він не відмовився від свого права на конфіденційність приватного життя стосовно трафіку (обліку) даних, тобто даних, які стосуються тривалості і часу використання Інтернету, та даних, які стосуються до того, хто використовував Інтернет і до якого сайту він або вона отримували доступ під час цього використання. На його думку, такі дані користуються окремим захистом відповідно до концепції приватного життя, яке містить конфіденційність спілкування та конфіденційність інформації.

87. У зв'язку з цим він зазначив, що необхідно визнати суттєву різницю між статичними та динамічними IP-адресами. В той час як можливо виділити аналогію між статичною IP-адресою, яка назавжди була приписана пристрою, і номером телефону, динамічна IP-адреса призначалася кожного разу, коли комп'ютер отримував доступ до Інтернету. Посилаючись на рішення Федерального конституційного суду Німеччини від 24 січня 2012 року (дивіться пункт 63 вище), заявник стверджував, що, обираючи динамічну IP-адресу, як і у абонента в цій справі, особа обирає приховування його або її особистості, оскільки необхідні додаткові дані для ідентифікації комп'ютера, який використовується для доступу до Інтернет і тим самим абонента. На його думку динамічна IP-адреса підпадає під сферу даних про трафік (вимірювання), до якої застосовується розділ 149b (1).

88. Заявник також зазначив, що дані про зміст повідомлення були отримані без участі органів влади Словенії. Органам влади Словенії був необхідний наказ суду для отримання таких даних, але вони уникнули цей необхідний крок подавши запит про отримання інформації про абонента на основі розділу 149B (3) в CPA. Стосовно останнього заявник стверджував що в той час, коли поліція Словенії отримала дані, які з'єднують його IP-адресу з його особою, закон, який регулював доступ до таких даних, не був чітким (*lex certa*), і тому законність, яку вимагав другий пункт статті 8, не була дотримана. Зокрема, на момент втручання (серпень 2006 року) положення національного законодавства щодо цього питання були суперечливими. Другий пункт статті 37 Конституції вимагав наказ суду для втручання в право на конфіденційність спілкування. ЄСА передбачав, що дані про трафік повинні зберігатись у таємниці, а повідомлення можливо було перехоплювати лише на підставі наказу компетентного органу влади. В національній правовій системі це могли бути лише рішення суду або, теоретично, наказ про переслідування в судовому порядку. У всякому разі, згідно з розділом 107 можливо було лише «перехоплювати» дані, а не передавати певні збережені дані. Крім того, провайдери мали зобов'язання видаляти збережені дані відповідно до розділу 104,щойно вони вже не будуть необхідними виставлення рахунків. З іншого боку, розділ 149b (1) та (3) CPA передбачав різні умови для доступу до даних, і було незрозуміло, яка була відмінність у їх застосуванні. Внаслідок цієї невизначеності в національному законодавстві неможливо стверджувати, що правовий захист від свавільного втручання державних органів влади в право на конфіденційність був достатнім.

89. На думку заявника ECA був *lex specialis* щодо CPA і не передбачав можливості передачі персональних даних поліції. В такій ситуації лакун в с законодавстві Конституція повинна застосовуватися безпосередньо, а Конституція чітко вимагала наказ суду про передачу таких даних.

(b) Уряд

90. Уряд пояснив, що IP-адреса була персональними даними та динамічна IP – адреса також була персональними даними, але вони не складали дані про трафік. Єдиною відмінністю між цими двома адресами було те, що статична IP-адреса залишалася абонентом до того часу, доки він не змінить Інтернет-провайдера, в той час як нова динамічна IP-адреса призначалася кожного разу, коли абонент отримував доступ до інтернету. Стосовно обох, ISP зберігав дані про час використання певної IP-адреси.

91. Уряд стверджував, що розслідування було зосереджене на заявникові лише після того, як відбулося вилучення та огляд комп'ютерів та після допиту осіб, які мешкали за тією адресою. Таким чином, зв'язок між абонентом та заявником став очевидним лише після обшуку в будинку, який здійснювався на підставі чинного судового наказу.

92. Визнаючи, що IP-адреса була елементом особистої інформації тому, що вона дозволяла визначити особу, уряд зазначав, що кожний користувач міг обирати, чи використовувати веб-сайт, який дозволяв розкриття персональних даних і/або зміст спілкування з невизначеним і необмеженим колом осіб. Уряд стверджував, що заявник не оскаржував той факт, що він сховав IP-адресу, яку він використовував для доступу до файлообмінної програми. Оскільки розголошення IP-адреси передбачало розкриття інформації про абонента, заявник не виявив наміру зберігати свою особистість в таємниці або приховувати її, отже його право на приватне життя не було залучене в цій справі.

93. Уряд стверджував, що заявник не міг очікувати, що інформація про абонента, пов'язаного з динамічною IP – адресою, могла бути прихована від поліції. На думку уряду оскаржені заходи були законними та пропорційними меті захисту недоторканості дітей, які як особливо вразливі особи користуються особливим захистом відповідно до Конвенції.

94. Уряд провів паралель з ситуацією, коли підозрюваного спіймали з системою внутрішнього телевізійного спостереження під час водіння. У такій ситуації фотокартка підозрюваного і його реєстраційні знаки були достатніми для того, щоб ідентифікувати його. Так само в цій справі необхідно припустити, що в той момент, коли поліція отримала динамічну IP – адресу і терміни її використання, користувач був ідентифікований за допомогою таких даних. Таким чином уряд стверджував, що національні суди правильно застосували розділ 149B (3) замість розділу 149b (1), оскільки останній стосувався даних про трафік, а не даних стосовно власника або користувача пристрою зв'язку.

2 Оцінка Суду

(a) Попередні зауваження і обсяг оцінювання Суду

95. Суд спочатку зазначає особливий контекст цієї справи, який стосується розкриття інформації про абонентів, пов'язану з динамічною IP-адресою. Він звертає увагу на широке законодавство та прецедентне право щодо захисту персональних даних та конфіденційності електронного зв'язку в межах Європейського Союзу та буде покладатися на них та на інші відповідні матеріали порівняльного права під час оцінювання деяких технічних питань, які застосовуються до цієї справи. Суд також буде, якщо доречно, враховувати правові доктрини, встановлені в цих матеріалах.

96. Як попереднє питання Суд також зазначає, що IP-адреса - це унікальний номер, присвоєний кожному пристрою в мережі, який дозволяє пристроям спілкуватися один з одним. На відміну від статичної IP-адреси, яка постійно виділена певному мережевому інтерфейсу певного пристрою, динамічна IP-адреса призначається ISP тимчасово, як правило, кожного разу, коли пристрій підключається до Інтернету (дивіться пункти 61, 87 і 90 вище). IP-адреса надає певні подробиці, такі як Інтернет-провайдер, до якого підключений користувач, і більш широке фізичне місце розташування, найімовірніше, місце розташування ISP. Таким чином більшість динамічних IP-адрес можливо простежити до Інтернет-провайдера, а не до певного комп'ютера. Для того, щоб отримати ім'я та адресу абонента використовуючи динамічну IP – адресу ISP, як правило, повинен шукати цю інформацію і з цією метою вивчити відповідні дані про підключення своїх абонентів (дивіться пункти 61 і 65 вище) .

97. В цій справі інформація про динамічну IP-адресу та час, коли вона була присвоєна, були зібрані поліцією Швейцарії, яка здійснила моніторинг користувачів певної мережі Інтернет, яка залучає матеріал з дитячою порнографією. Поліція Швейцарії передала інформацію поліції Словенії, яку вона отримали від ISP – ім’я та адреса абонента, пов'язаного з динамічною IP – адресою, про яку йде мова, - адреса батька заявника (дивіться пункти 6 і 7 вище) .

98. Уряд стверджує, що стаття 8 Конвенції не застосовується в цій справі, оскільки заявник не оскаржений захід не вплинув безпосередньо на заявника і тому, що навіть якщо б він постраждав, він вже добровільно відмовився від свого права на конфіденційність публічно обмінюючись файлами, про які йде мова (дивіться пункти 92 і 93 вище). Для того, щоб відповісти на ці запитання Суд повинен розглянути питання стосовно того, чи заявник, або будь-яка особа, яка використовує Інтернет, мала обґрунтоване очікування того, що його публічна діяльність онлайн буде залишаються анонімною (дивіться пункти з 115 до 118 вище) .

99. У зв'язку з цим Суд що існування порушення має обмежений стримуючий ефект, якщо не існує засобів для ідентифікації справжнього порушника та притягнення його до відповідальності. Тут Суд зауважує, що він не виключає можливості того, що позитивні обов’язки держави за статтею 8 стосовно гарантування фізичної чи душевної недоторканності особи можуть поширюватися на питання, пов’язані з ефективністю кримінального розслідування, навіть коли не йдеться про кримінальну відповідальність представників держави. З точки зору Суду, держави мають позитивний обов’язок, що випливає зі статті 8 Конвенції, установити кримінальну відповідальність за

правопорушення проти особи, у тому числі замах на такі правопорушення, а також посилити стримуючий ефект такої криміналізації, застосовуючи положення кримінального закону на практиці шляхом ефективного розслідування та кримінального переслідування. Там, де виникає загроза фізичному чи душевному спокою дитини, такі заходи набувають навіть ще більшої важливості. Суд нагадує у цьому зв'язку, що сексуальне насильство є безсумнівно огидним типом правопорушення з украй негативними наслідками для його жертв. Діти та інші вразливі особи мають право на захист держави, у вигляді дієвого стримування, від таких тяжких форм втручання в надзвичайно важливі аспекти їхнього приватного життя (дивіться *K.U. проти Фінляндії*, № 2872/02, § 46, ЄСПЛ 2008-V). Проте, на питання, поставлені урядом стосовно застосування статті 8, необхідно відповісти незалежно від законного або незаконного характеру розглянутої діяльності, а також без будь - якої шкоди для вимоги Конвенції того, щоб захист вразливих осіб повинен бути наданий державами-членами, як зазначено, серед іншого, в справі *К.Ю. проти Фінляндії* (наведена вище) .

(b) застосовність статті 8

(і) Повторення відповідних принципів

100. Суд повторює, що приватне життя - це широкий термін, який не піддається вичерпному визначенню. Стаття 8 захищає, *зокрема,* право на ідентичність і розвиток особистості, а також право встановлювати і розвивати стосунки з іншими людьми і зовнішнім світом. Отже, існує зона взаємодії особи з іншими особами, навіть в публічному контексті, яка може підпадати під «приватне життя» (дивіться *Узун проти Німеччини,* №. 35623/05, § 43, ECHR 2010 -VI (витяги)).

101. Існує цілий ряд елементів, які є доречними для розгляду питання стосовно того, чи вплинули на приватне життя особи заходи, які відбулися за межами його будинку або приватних приміщень. Для того, щоб з'ясувати, чи застосовуються поняття "приватне життя" та "кореспонденція", Суд неодноразово перевіряв, чи мали особи обґрунтовані сподівання того, що їх приватне життя буде поважатись та захищатись (дивіться *Барбулеску проти Румунії* [ВП], № 61496/08, § 73, ECHR 2017, і *Копланд проти Сполученого Королівства,* №. 62617/00, § § 41- 42, ECHR 2007 I). У цьому контексті Суд стверджував, що обґрунтоване очікування конфіденційності є важливим, хоча й не обов'язково вирішальним фактором (дивіться *Барбулеску,* наведена вище, § 73).

102. У контексті персональних даних Суд зазначив, що термін "приватне життя" не повинен тлумачитися суворо. Суд виявив, що широке тлумачення відповідає тлумаченню Конвенції від 1981 року, метою якого є «забезпечення на території кожної Сторони кожній особі ... поваги його прав і основних свобод, і зокрема його права на конфіденційність стосовно автоматизованої обробки персональних даних, які стосуються нього "(стаття 1). Такі персональні дані будуть визначені як «будь-яка інформація, яка стосується ідентифікованої особи або особи, яку можливо ідентифікувати (стаття 2) (дивіться. *Аманн проти Швейцарії* [ВП], № 27798/95, § 65, ЄСПЛ 2000 - II, дивіться. також пункт 46 вище).

103. З добре встановленого прецедентного права витікає, що якщо був збір даних про певну особу, обробка або використання персональних даних або публікація матеріалу, про який йде мова, у такий спосіб або такого рівня, який зазвичай неможливо передбачити, виникають міркування приватного життя (дивіться *Satakunnan Markkinapörssi Oy і Satamedia Oy проти Фінляндії* [ВП], №. 931/13, § 136, ЕСПЛ 2017 (витяги)). Таким чином, стаття 8 Конвенції передбачає право на форму інформаційного самовизначення, яка дозволяє особам покладатися на їх право на конфіденційність щодо даних, які, хоч і нейтральні, збираються, обробляються та розповсюджуються колективно та у такій формі або у такий спосіб. що можуть зачіпати їх права відповідно до статті 8 (в тому ж місці, § 137).

104. Суд раніше вважав, що інформація, така як встановлення даних за номерами телефонів, які викликаються (дивіться *Мелоун проти Сполученого Королівства,* 2 серпня 1984 року, § 84, Серія А, т. 82), особиста інформація, яка стосується телефону, електронної пошти і використання Інтернету (дивіться *Копленд,* наведена вище, §§ 41 та 43), інформація, яка зберігається прокуратурою стосовно фактів щодо ділових стосунків заявника (дивіться *Аманн*, наведена вище, § 66) та публічна інформація, яка зберігається органами влади, про далеке минуле заявника (дивіться *Ротару проти Румунії* [ВП], № 28341/95, §§ 43 і 44, ЄСПЛ 2000 - V) підпадає під сферу застосування статті 8.

105. Крім того, Суд раніше визнав в справі *Delfi A.S. проти Естонії* ([ВП] № 64569/09, § 147, ЄСПЛ 2015) що анонімність вже давно використовується для уникнення репресій або небажаної уваги. Тому вона може служити важливим чинником, що сприяє вільному поширенню ідей та інформації, у тому числі, зокрема, в Інтернеті. Водночас Суд не випускає з уваги й те, з якою легкістю, масштабністю і швидкістю відбувається поширення інформації в Інтернеті, а також живучість у мережі Інтернет будь-якої інформації, яка одного разу була там розміщена, у зв’язку з чим наслідки протиправних висловлювань в Інтернеті можуть бути значно більш негативними ніж у випадку, коли йдеться про такі висловлювання в традиційних медіа (там само).

106. У вищезазначеній справі Суд також розробив різні рівні анонімності, залучені в онлайн-діяльності, і відзначив наступне (в тому ж місці, пункт 148) :

> " Суд зауважує, що рівень анонімності в Інтернеті може бути різним. Користувачі Інтернету можуть бути анонімними для більшої частини публіки, але водночас можуть бути ідентифіковані постачальником послуг завдяки їхнім обліковим записам або контактним даним, які можуть бути або неперевіреними, або підлягати певній перевірці – йдеться про різні процедури, починаючи з обмеженої перевірки (наприклад, за допомогою активації облікового запису через адресу електронної пошти або через аккаунт у соціальній мережі) до підтвердження автентичності особи, чи то за допомогою національних електронних ідентифікаційних карток, чи то даних аутентифікації користувача в системі інтернет-банкінгу. Постачальник послуг може також надати своїм користувачам широкі можливості користування правом анонімності, взагалі не зобов’язуючи їх ідентифікувати себе, і в такому випадку ідентифікація таких осіб можлива лише обмеженою мірою за допомогою інформації,

що зберігається постачальниками послуг доступу до мережі Інтернет. Розкриття такої інформації можливе, як правило, лише за наявності відповідного розпорядження слідчого або судового органу і за певних обмежувальних умов. Тим не менш, у деяких випадках її розкриття може потребуватися з метою ідентифікації правопорушників і притягнення їх до відповідальності".

(ii) Застосування вищенаведених принципів у цій справі

(α) Характер інтересів, що зачіпаються

107. Уряд не заперечував, що інформація про абонента в принципі стосувалася персональних даних (дивіться пункти 90 і 92 вище). Такий висновок також витікає з визначень, які містяться в Конвенції від 1981 року, законодавстві Європейського Союзу, а також національному законодавстві, спрямованому на їх реалізацію (дивіться пункти 40, 46, 53 та 57 вище).

108. Крім того, Суд зазначає, що інформація про абонента, пов'язана з певною динамічною IP-адресою, присвоєною в певний час, не була загальнодоступною і тому її неможливо порівняти з інформацією, знайденою в традиційному телефонному довіднику або загальнодоступній базі даних про реєстраційні номери транспортних засобів, на які посилається уряд (дивіться пункт 94) вище) Дійсно, здавалося б, що для того, щоб ідентифікувати абонента, якому була призначена певна динамічна IP-адреса в певний час, ISP повинен отримати доступ до збережених даних щодо певних подій в сфері телекомунікацій (дивіться, наприклад, пункти 29, 61, 65 і 95 вище). Використання таких збережених даних може викликати міркування приватного життя (дивіться пункт 103 вище).

109. Крім того, Суд не може ігнорувати той особливий контекст, в якому намагалися отримати інформацію про абонента у цій справі. Єдина мета отримання інформації про абонента полягала в тому, щоб ідентифікувати певну особу, яка стоїть за самостійно зібраним матеріалом, який відображає дані, якими він ділився. У зв'язку з цим Суд зазначає, що існує зона взаємодії особи з іншими особами, яка може підпадати під сферу дії "приватного життя" (дивіться пункт 100 вище). Інформація про таку діяльність зачіпає аспект конфіденційності щодо моменту, коли вона пов'язана або її можливо приписати ідентифікованій особі або фізичній особі, яку можливо ідентифікувати (для посилання на ідентифікацію, хоча і в досить іншому контексті, дивіться *Пек проти Сполученого Королівства,* № 44647/98, § 62, ЄСПЛ 2003 - I, і *J.S .проти Сполученого Королівств* (ріш.), № 445/10, §§ 70 та 72, 3 березня 2015 року). Тому те, що може здаватися додатковою інформацією, яку намагається отримати поліція, а саме ім'я та адресу абонента, повинне в таких ситуаціях, як в цій справі, розглядатися як пов'язане з відповідним попереднім змістом, який виявляє дані (дивіться окремі думки судді Конституційного Суду, наведені в пунктах 31 і 34, порівняйте також з позицією Верховного суду Канади, наведену в пунктах 69 і 72 вище, і Федерального конституційного суду Німеччини, наведену в пунктах 64 і 65 вище). Інший висновок заперечував би необхідний захист інформації, яка може виявити багато подробиць про

онлайн-діяльність особи, в тому числі чутливі подробиці його або її інтересів, переконань і стилю інтимного життя .

110. З урахуванням вищезазначених міркувань Суд дійшов висновку, що ця справа стосується питань конфіденційності, які можуть бути залучені в захист статті 8 Конвенції.

(b) чи був заявник ідентифікований за допомогою оскарженого заходу

111. Суд повинен розглянути наступне твердження уряду стосовно того, що інформація про абонента, отримана поліцією, розкривала лише ім'я та адресу батька заявника, а не заявника (дивіться пункт 91 вище). У зв'язку з цим, Суд зазначає, що було прийнято вважати, що визначення персональних даних посилається на інформацію, яка стосується не лише ідентифікованих осіб, але і осіб, яких можливо ідентифікувати (дивіться пункти 40, 47, 53, 54, 55 та 58 вище) .

112. В цьому контексті, заявник був, без сумніву, користувачем служби Інтернету, про яку йде мова, (дивіться пункт 56 вище), і його діяльність онлайн контролювалася поліцією. Суд далі зазначає, що заявник використав Інтернет у такий спосіб, що, здавалося б, що то був його власний комп'ютер в його власному будинку. Це не мало великого значення, що ім’я заявника не було зазначене в інформації про абонента, отриманій поліцією. Дійсно, це не є незвичним для однієї сім'ї, мати єдину підписку на Інтернет-послуги, якою користуються декілька членів сім'ї. Той факт, що вони не підписані особисто на Інтернет-послугу, не впливає на їх очікування конфіденційності, які побічно залучаються, коли розкривається інформація про абонента, яка стосується їх приватного користування Інтернетом.

113. Зрозуміло, що мета оскарженого заходу, а саме отримання поліцією без рішення суду даних про абонента, пов'язаного з динамічною IP-адресою, наданих поліцією Швейцарії (дивіться пункт 7 вище), полягала в з’єднанні комп'ютера, який використовується в певному місці та, можливо, певною особою. Інформація про абонента, яка містила також адресу, дозволяла поліції визначити будинок, в якому відбувалося це інтернет з'єднання. Це надало їм можливість ідентифікувати заявника як підозрюваного користувача мережі Razorback .

114. З урахуванням вищезазначеного, а також того, що національні суди не відхилили справу на підставі того, що заявник не був абонентом Інтернет-послуг, про яку йде мова, Суд дійшов висновку, що цей факт неможливо вважати бар’єром для застосування Статті 8 у цій справі. Відповідно, Суд відхиляє заперечення уряду стосовно передбачуваної відсутності статусу жертви (дивіться пункт 83 вище).

(γ) чи мав заявник обґрунтоване очікування конфіденційності

115. Для того, щоб з'ясувати, чи поняття "приватне життя" було застосовним для цієї справи Суд повинен розглянути питання стосовно того, чи з огляду на загальнодоступний характер відповідної мережі заявник мав обґрунтоване очікування того, що його приватне життя буде поважатися та захищатись (дивіться пункт 101 вище). У зв'язку з цим Конституційний суд Словенії і уряд-відповідач (дивіться пункти 14 і 18 рішення

Конституційного суду, наведені в пункті 29 вище; дивіться також пункт 92 вище) вважали важливим те, що заявник брав участь у в мережі Razorback, доступ до якої не був обмежений. Вони вважали, що він свідомо розкрив мережеву активність і пов'язану динамічну IP – адресу громадськості. Отже, на їх думку, його очікування конфіденційності не були законними, і, крім того, можливо було вважати, що він відмовився від нього (в тому ж місці).

116. Суд, як Конституційний суд, визнає, що заявник, під час обміну файлами з порнографічними матеріалами за допомогою мережі Razorback, очікував зі своєї суб'єктивної точки зору, що, що діяльність буде залишатися конфіденційною і його особистість не буде розкрита (дивіться пункт 14 рішення Конституційного суду, наведене у пункті 29 вище). Проте, на відміну від Конституційного Суду Суд вважає, що той факт, що він не приховує свою динамічну IP-адресу, припускаючи, що це є можливим, не може бути вирішальним під час оцінювання того, чи було його очікування конфіденційності обґрунтованим з суб'єктивної точки зору. У зв'язку з цим Суд зазначає, що питання, очевидно, полягає не в тому, чи міг заявник обґрунтовано очікувати збереження його динамічної IP – адреси в таємниці але в тому, чи міг він обґрунтовано очікувати конфіденційності стосовно його особистості .

117. Суд раніше визнав аспект анонімності онлайн конфіденційності (дивіться *Delfi AS,* наведена в пункті 105 вище, дивіться також пункт 12 рішення Конституційного суду, наведені в пункті 29 вище) стосовно характеру діяльності в Інтернеті, в якому користувач бере участь без обов'язкової ідентифікації. Ця концепція анонімності конфіденційності є важливим фактором, який необхідно враховувати під час цього оцінювання. Зокрема, не стверджувалося, що заявник будь-коли розкрив свою особу стосовно онлайн-діяльності, про яку йде мова (дивіться в зв'язку з цим особливу думку судді Жадек Пенза, наведена в пункті 33 вище), або його, наприклад, міг ідентифікувати певний провайдер веб-сайту за допомогою облікового запису або контактних даних. Отже його онлайн діяльність залучала більш високий рівень анонімності (дивіться *Delfi AS,* наведена в пункті 105 вище, § 148), як це було підтверджено тим фактом, що присвоєну динамічну IP-адресу, навіть якщо її могли бачити інші користувачі мережі, неможливо було простежити до певного комп'ютера без перевірки даних ISP після наступного запиту поліції .

118. Наприкінці Суд зазначає, що застосовна нормативно- правова база також може бути доречним, хоч і не обов'язково визначальним фактором під час визначення обґрунтованого очікування конфіденційності (дивіться., наприклад, *J.S. проти Сполученого Королівства* (ріш.), наведене вище, § 70, та *Пеєв проти Болгарії,* № 64209/01, § 39, 26 липня 2007 року). В цій справі жодна зі сторін не надала інформацію про умови угоди, на підставі якого надавалися послуги Інтернет батьку заявника. Стосовно законодавчої бази, Суд вважає достатнім зазначити, що стаття 37 Конституції гарантувала конфіденційність листування та спілкування, а також вимагала, щоб будь-яке втручання у це право було засноване на рішенні суду (дивіться пункт 35 вище). Тому, з точки зору чинного законодавства у відповідний час, очікування заявником конфіденційності стосовно його діяльності в Інтернеті неможливо вважати невиправданим або необґрунтованим.

(δ) Висновок

119. На всіх вищезазначених підставах Суд дійшов висновку, що інтерес заявника в захисті його ідентичності щодо його діяльності в Інтернеті підпадає під поняття " приватного життя ", тому стаття 8 була застосовною до цієї скарги.

(c) Дотримання вимог статті 8

(і) Чи було втручання?

120. З урахуванням вищезазначеного висновку стосовно того, що право заявника на повагу до його приватного життя, як це гарантується статтею 8 § 1, було залучене в цій справі, Суд також вважає встановленим, що запит поліції до ISP і їх використання інформації про абонента, яка викликала ідентифікацію заявника, складали втручання у це право (дивіться, *mutatis mutandis, Ротару,* наведена вище, § 46 та *Узун,* наведена вище, § 52). З огляду на вищезазначене Суд не вважає необхідним визначати, чи захід, про який йде мова, також складав втручання в право заявника на повагу до його листування.

121. Таким чином, Суд повинен перевірити, чи втручання в право на приватне життя було відповідним вимогам статті 8§1, іншими словами, чи було воно "відповідним до закону", переслідувало одну або декілька законних цілей, викладених цьому пункті і було "необхідним в демократичному суспільстві" для досягнення мети або цілей, про які йде мова.

(ii) Чи було втручання згідно із законом?

122. Суд зазначає, що вираз "згідно із законом" у значенні статті 8 §2 вимагає, по-перше, щоб оскаржений захід мав певну основу в національному законодавстві. По-друге, національне законодавство повинне бути доступним для відповідної особи. По-третє, особа, яка постраждала, повинна мати можливість передбачити наслідки національного законодавства для нього, і, по-четверте, національне законодавство повинне бути сумісним з верховенством права (дивіться. серед багатьох інших авторитетних джерел, *Ротару,* наведена вище, § 52; *Свобода та інші проти Сполученого Королівства,* № 58243/00, § 59, 1 липня 2008 року, і *Саллінен та інші проти Фінляндії,* № 50882/99, § 76, 27 вересня 2005 року).

123. Суд також повторює, що національні органи влади, зокрема суди, повинні тлумачити та застосувати національне законодавство. Проте суд зобов'язаний перевірити, чи спосіб, у який тлумачиться і застосовується національне законодавство, створює наслідки, які узгоджуються з принципами Конвенції, які тлумачаться у світлі прецедентного права Суду (дивіться *Кочіарелла проти Італії* [ВП], № 64886/01, §§ 81 та 82, ЄСПЛ 2006 - V).

124. У цій справі припускаючи, що отримання поліцією інформації про абонента, пов'язаної з динамічною IP-адресою, про яку йде мова, мало певну основу в національному законодавстві, оскільки розділ 149b (3) CPA передбачав, що поліція може отримати інформацію про власника або користувача певних електронних засобів зв'язку

від ISP (дивіться пункт 36 вище) Суд повинен з'ясувати, чи є цей закон доступним, передбачуваним та сумісним з верховенством права.

125. Суд зазначає, що в цій справі не виникає жодних питань щодо доступності закону. Стосовно інших вимог, Суд повторює, що правило є "передбачуваним", якщо воно сформульоване з достатньою точністю для того, щоб кожна особа (якщо це необхідно з відповідною консультацією) регулювати свою поведінку (дивіться *Ротару,* наведена вище, § 55 та ці принципи, підсумовані в цій справі). Крім того, сумісність з верховенством права вимагає, щоб національне законодавство забезпечувало належний захист від свавільного втручання в права, захищені статті 8 (дивіться, з *відповідними змінами, Аманн*, наведена вище, §§ 76-77; *Биков проти Росії* [ВП], № 4378/02, § 76, 10 березня 2009 року; дивіться. також *Вебер та Саравіа проти Німеччини* (ріш.), № 54934/00, § 94, ЄСПЛ 2006 р. - XI ; та *Свобода та інші,* наведена вище, § 62). Таким чином Суд повинен бути задоволений тим, що існують відповідні та ефективні гарантії від зловживань. Це оцінювання залежить від усіх обставин справи, таких як характер, обсяг та тривалість можливих заходів, підстави, необхідні для їх наказу, органи влади, які мають право надавати дозвіл, здійснювати та наглядати за ними, а також тип засобу судового захисту, наданий національним законодавством (дивіться *Асоціація з європейської інтеграції та прав людини та Екімджиєв проти Болгарії,* №. 62540/00, § 77, 28 червня 2007 року із посиланням на *Класс та інші проти Німеччини,* 6 вересня 1978 року, § 50, Серія A 28, і *Узун,* наведена вище, § 63).

126. З урахуванням особливого контексту цієї справи Суд підкреслює, що Конвенція про кіберзлочинність зобов'язує держави робити такі заходи, як збір даних про трафік в режимі реального часу і видача порядків представлення, доступними для органів влади в боротьбі, *зокрема,* зі злочинами, пов'язаними з дитячою порнографією (дивіться пункти 47 до 51 вище). Проте такі заходи відповідно до статті 15 цієї Конвенції «підпорядковуються умовам і гарантіям, передбаченим національним законодавством [держав-членів]» і повинні «якщо це є доречним з огляду на природу відповідного повноваження або процедури, *серед іншого,* містити судовий або інший незалежний нагляд, підстави, які виправдовують застосування, і обмеження сфери застосування і терміну таких повноважень або процедур» (дивіться пункт 52 вище).

127. В цій справі Суд зазначає, що розділ 149 b (3) CPA (дивіться пункт 36 вище), на який посилаються національні органи влади, стосувався запиту на отримання інформації про власника або користувача певних засобів електронного спілкування. Він не містить певних правил щодо зв’язку між динамічною IP-адресою та інформацією про абонента. Суд також зазначає, що стаття 37 Конституції вимагає судового наказу для будь-якого втручання в конфіденційність спілкування (дивіться пункт 35 вище). Крім того, ЄСА (дивіться пункт 37 вище), який спеціально регулює таємність та конфіденційність електронних засобів зв'язку, у відповідний час не передбачав можливості доступу та передачі інформації про абонентів та відповідних даних про трафік для цілей кримінального провадження. Він передбачав, що електронні повідомлення, в тому числі відповідні дані про трафік, є конфіденційними і повинні бути захищені ISP (дивіться пункт 37 вище). Він також передбачав, що ISP не повинен передавати дані про трафік іншим

особам, якщо це не було необхідним для надання послуги, за винятком випадків, коли компетентний орган влади видав наказ про законне перехоплення повідомлень (дивіться розділ 103 ЄСА, наведений у пункті 37 вище). Таким чином, законодавство було, принаймні, не когерентним щодо рівня захисту, наданому інтересу заявника в конфіденційності.

128. Зазначивши, що Суд буде узурпувати функцію національних судів, якщо вони будуть намагатися зробити авторитетне твердження щодо того, який закон повинен був переважати у цій справі. Натомість він повинен звернутися до обґрунтування, запропонованого національними судами. Він зазначає у зв'язку з цим, що Конституційний Суд визнав, що «особа користувача, який спілкується [була] одним з важливих аспектів конфіденційності спілкування», і її розкриття вимагало наказу суду відповідно до статті 37 §2 Конституції (дивіться пункт 18 рішення Конституційного суду, викладеного в пункті 29 вище). А саме, відповідно до тлумачення Конституційного суду, яке було відповідним до його попереднього прецедентного права, в якому було виявлено, що дані про трафік, як це визначено відповідно до національного законодавства, підпадають під захист статті 37 Конституції (дивіться там само), розкриття інформації про абонента, пов'язаної з певною динамічною IP – адресою, в принципі, вимагало наказу суду і не могло бути отримане за допомогою звичайних письмових запитів поліції.

129. Суд зазначає, що, по суті, єдиною підставою для відхилення Конституційним судом скарги заявника було те, що для надання дозволу розкриття інформації про абонента без наказу суду - існувало припущення, що заявник «відмовився від законного очікування конфіденційності» (дивіться пункт 18 рішення Конституційного суду, наведене в пункті 29 вище). Проте, Суд, з урахуванням висновків в контексті застосування статті 8, не виявляє, що позиція Конституційного суду з цього питання узгоджувалася зі сферою дії права на конфіденційність відповідно до Конвенції (дивіться пункти з 115 до 118 вище). З урахуванням висновку Конституційного Суду стосовно того, що «особа користувача, який спілкується» підпадає під захист статті 37 Конституції (дивіться пункт 128 вище), висновок Суду стосовно того, що заявник мав достатні підстави очікувати, що його особистість стосовно до його діяльності в Інтернеті буде залишатися конфіденційною (дивіться пункти з 115 до 118 вище), наказ суду був необхідним в цій справі. Крім того, в національному законодавстві не існувало перешкод у поліції для отримання цього наказу з урахуванням того, що вони через декілька місяців після отримання інформації про абонентів, протягом яких, очевидно, в цій справі не було проведено слідчих заходів, подали клопотання та отримали наказ суду щодо того, що, здається, було, принаймні частково, тією ж інформацією, якою вони вже володіли (дивіться пункт 8 вище). Посилання національних органів влади на розділ 149b (3) CPA було явно невідповідним і, що є більш важливим, він не надавав практично жодного захисту від свавільного втручання .

130. У зв'язку з цим Суд зазначає, що у відповідний час не існувало жодних правил, які визначали умови для збереження даних, отриманих відповідно до розділом 149b (3) CPA, а також жодних гарантій від зловживань посадових осіб під час процедури доступу та передачі таких даних. Стосовно останнього, поліція, маючи у своєму розпорядженні

інформацію про певну онлайн-діяльність, могла б визначити автора подавши запит до ISP для того, щоб він знайшов цю інформацію. Крім того не було встановлено, що існував незалежний нагляд за використанням цих повноважень поліції у відповідний час незважаючи на те, що ці повноваження, як тлумачать національні суди, змусили ISP отримати збережені дані про з'єднання та дозволили поліції встановити зв'язок між великою кількістю інформації про онлайн-діяльність з певною особою без її згоди (дивіться пункти 108 та 109 вище).

131. Суд далі зазначає, що незабаром після того, як були вжиті оскаржені заходи проти заявника, парламент прийняв поправки до ECA (дивіться пункт 38 вище, а також відповідні положення в наступному новому законі, наведеному в пункті 39). Ці поправки передбачали, серед іншого, правила збереження даних про походження зв'язку, а саме, *зокрема,* ім'я та адресу абонента, якому було призначена певна IP-адреса, та процедура доступу до них та їх передачі. Проте це не мало жодного впливу на ситуацію заявника.

132. З урахуванням вищезазначеного Суд вважає, що закон, на якому був заснований оскаржений захід, тобто отримання поліцією абонентської інформації, пов'язаної з динамічною IP- адресою, про яку йде мова (дивіться пункт 7 вище), та спосіб, у який він був застосований національними судами, не були чіткими і не пропонували достатні гарантії від свавільного втручання права статті 8.

133. За цих обставин Суд вважає, що втручання в право заявника на повагу до його приватного життя не було "згідно із законом" згідно зі статтею 8§2 Конвенції. Отже, Суд не повинен розглядати, чи має оскаржений захід законну мету і був пропорційним.

134. Розглянувши всі вищезазначені міркування Суд дійшов висновку, що мало місце порушення статті 8 Конвенції.

II. ЗАСТОСУВАННЯ СТАТТІ 41 КОНВЕНЦІЇ

47. Стаття 41 Конвенції передбачає:

> «Якщо Суд визнає факт порушення Конвенції або Протоколів до неї і якщо внутрішнє право відповідної Високої Договірної Сторони передбачає лише часткове відшкодування, Суд, у разі необхідності, надає потерпілій стороні справедливу сатисфакцію.»

A. Шкода

136. Заявник вимагав 32 000 євро (EUR) щодо відшкодування моральної шкоди, які містили 7000 євро за страждання, яких він зазнав під час розгляду судової справи проти нього, 15000 євро тому, що він був необґрунтовано ув'язнений і 10 000 євро за таврування в суспільстві, від якого він постраждав внаслідок його засудження.

137. Уряд стверджував, що вимога відшкодування моральної шкоди заявника була необґрунтованою і надмірною. Вони також стверджували, що не існувало жодного зв'язку між передбаченим порушенням статті 8 в цій справі і стврджуваною моральною шкодою,

завданою заявнику у зв’язку з його засудженням в кримінальному порядку і з тюремним ув'язненням. Зокрема, навіть якщо інформація, про яку йде мова, була б вилучена з матеріалів справи, заявник не уникнув би кримінального провадження проти нього. Крім того, уряд стверджував, що оскільки заявник визнав, що він міг подати запит про відновлення провадження у випадку виявлення порушення, декларативний висновок Суду є достатнім.

138. Суд вважає, що сам висновок про порушення є достатньою справедливою сатисфакцією моральної шкоди, яка могла бути завдана заявникові.

B. Судові та інші витрати

139. Заявник також вимагав 4335, 50 євро відшкодування судових та інших витрат, понесених в національних судах, та 2600 євро для відшкодування витрат, понесених в Суді плюс податок на додану вартість (ПДВ). Він стверджував, що ці суми були розраховані на основі офіційного тарифу для адвокатів.

140. Уряд стверджував, що витрати, про які стверджував заявник щодо його представництва під час провадження в національному суді, містили ПДВ. Вони також додали видатки на юридичний висновок, а саме 2000 євро, який явно не був підготовлений для цілей провадження в національному суді. Щодо вимоги відшкодування витрат на провадження у Суді уряд стверджував, що вони були надмірними. Крім того, за винятком рахунку за вищезазначений юридичний висновок, заявник не надав жодних доказів того, що він поніс витрати у зв’язку з його законним представництвом.

141. Відповідно до прецедентного права Суду заявник має право на відшкодування судових та інших витрат лише якщо було продемонстровано, що вони були дійсно і обов'язково понесені та є обґрунтованими щодо обсягу. У цій справі з урахуванням документів, які знаходяться у його розпорядженні, та зазначених вище критеріїв Суд вважає обґрунтованим присудити суму в 922 євро для відшкодування судових видатків і витрат в провадженні в національних судах та 2600 євро для відшкодування витрат під час провадження в Суді. Таким чином, він повинен отримати відшкодування судових та інших витрат на суму 3522 євро.

C. Пеня

142. Суд вважає, що пеня в разі несвоєчасної виплати має визначатися на підставі граничної позичкової ставки Європейського центрального банку плюс три відсоткові пункти.

НА ЦИХ ПІДСТАВАХ СУД

1 *Вирішує* шістьма голосами проти одного погодитися з запереченням уряду щодо відсутності статусу жертви у зв’язку з розкриттям інформації про абонента відповідно до статті 8 Конвенції і *відхиляє* її;

2. *Оголошує* більшістю голосів скаргу щодо розголошення інформації про абонента згідно зі статтею 8 Конвенції прийнятною, а решту заяви - неприйнятною;

3. *Постановляє,* шістьма голосами проти одного, що мало місце порушення статті 8 Конвенції;

4. *Постановляє* одноголосно, що висновок про порушення є достатньою справедливою сатисфакцією моральної шкоди, завданої заявникові;

5 *Постановляє,* шістьма голосами проти одного,

(a) що держава-відповідач повинна сплатити заявнику протягом трьох місяців з дня, коли рішення стане остаточним відповідно до статті 44 § 2 Конвенції 3522 євро (три тисячі п'ятсот двадцять два євро) плюс будь-який податок, який може бути стягнуто заявникові, щодо судових та інших витрат;

(b) що після закінчення вищезазначеного періоду в три місяці до розрахунку на вищенаведену суму нараховується пеня за ставкою, яка дорівнює граничній ставці кредитування Європейського центрального банку протягом періоду невиконання зобов'язань плюс три відсотки;

6. *Відхиляє* одноголосно решту вимог заявника щодо справедливої сатисфакції.

Учинено англійською мовою і повідомлено письмово 24 квітня 2018 року відповідно до пунктів 2 і 3 правила 77 Регламенту Суду.

Андреа Тамієтті — Заступник секретаря секції

Ганна Юдківська — Голова

Відповідно до пункту 2 статті 45 Конвенції та пункту 2 правила 74 Регламенту Суду до цього рішення додано такі окремі думки:

(а) окрема думка судді Г. Юдківської, яка збігається з позицією більшості та до якої приєднався суддя М. Бошняк ;

(б) окрема думка судді Ф. Вехабовіча, яка не збігається з позицією більшості.

GY.
ANT