ВЕЛИКА ПАЛАТА

**БАРБУЛЕСКУ проти РУМУНІЇ**

*(Заява № 61496/08)*

РІШЕННЯ

СТРАСБУРГ

5 вересня 2017

*Це рішення є остаточним. До нього можуть бути внесені редакційні зміни.*

У справі Барбулеску проти Румунії,

Європейський Суд з прав людини, засідаючи Великою Палатою у складі:

Guido Raimondi, *головуючий*, Angelika Nußberger, Mirjana Lazarova Trajkovska, *судді*, Luis López Guerra,ad hoc *суддя*, Ledi Bianku, Işıl Karakaş, Nebojša Vučinić, André Potocki, Paul Lemmens, Dmitry Dedov, Jon Fridrik Kjølbro, Mārtiņš Mits, Armen Harutyunyan, Stéphanie Mourou-Vikström, Georges Ravarani, Marko Bošnjak, Tim Eicke, *судді*,  
а також Søren Prebensen, *заступник секретаря Великої Палати*,

Провівши 30 листопада 2016 року та 8 червня 2017 слухання за закритими дверима,

Проголошує наступне рішення, яке було прийнято в останній згаданий день:

ПРОЦЕДУРА

1. Дану справу розпочато за заявою (№ 61496/08) проти Румунії, яку подав до Суду відповідно до статті 34 Конвенції про захист прав людини та основоположних свобод (надалі – «Конвенція») громадянин Румунії, пан Богдан Михай Барбулеску (надалі – «заявник») 15 грудня 2008 року.

2. Заявника представляли пан E. Домокос-Ханку та пан О. Ювердеану, адвокати, які практикують у Бухаресті. Уряд Румунії (надалі – «Уряд») представляла його Уповноважена, пані С. Брумар, з Міністерства іноземних справ.

3. Заявник скаржився, зокрема, на те, що рішення його роботодавця розірвати контракт ґрунтувалося на порушенні його права на повагу до його приватного життя та кореспонденції, закріпленого у статті 8 Конвенції, і що національні суди не виконали своє зобов’язання щодо захисту цього права.

4. Заяву було передано до Четвертої секції Суду (правило 52 § 1 Регламенту Суду). 12 січня 2016 року Палата цієї секції, у складі Андраса Саджо, головуючого, Вінсента А. Де Гаетано, Боштьяна М. Жупанчича, Нони Цоцорії, Пауло Пінто де Альбукерке, Егідіюса Куріса та Юлії Мотоц, суддів, а також Фатоша Арасі, заступника секретаря секції, одноголосно проголосила скаргу стосовно 8 Конвенції прийнятною, а решту заяви неприйнятною. Вона постановила, шістьма голосами проти одного, що не мало місця порушення статті 8 Конвенції. Окрему думку судді Пінто де Альбукерке було додано до рішення Палати.

5. 12 квітня 2016 заявник просив відправити справу до Великої палати відповідно до статті 43 Конвенції та правила 73. 6 червня 2016 комісія Великої Палати прийняла його запит.

6. Склад Великої палати був визначений відповідно до статті 26 §§ 4 та 5 Конвенції та правила 24. Юлія Мотоц, суддя, обрана від Румунії, відмовилася від засідання у справі (правило 28). Згодом Луїс Лопес Герра був призначений головуючим у якості судді *ad hoc* (стаття 26 § 4 Конвенції та правило 29 § 1).

7. Заявник та Уряд подали подальші письмові зауваження (Правило 59 § 1).

8. На додаток до цього, зауваження третьої сторони були отримані від уряду Франції та Європейської конфедерації профспілок; головуючий дозволив обом сторонам взяти участь у письмовій процедурі (стаття 36 § 2 Конвенції та правило 44 § 3).

9. Слухання відбулося у відкритому порядку у Будинку прав людини, Страсбург, 30 листопада 2016 року (правило 59 § 3).

До Суду з’явилися:

(a) *з боку Уряду*  
Пані C. Брумар, *Уповноважена*,  
Пан Г.В. Гаврила, член національної юридичної служби,   
відряджений до Управління Уповноваженого Уряду, *адвокат*,  
Пані Л.А. Русу, повноважний міністр, постійний   
представник Румунії в Раді Європи, *радник*;

(b) *з боку заявника*  
Пан E. Домокос-Ханку,   
Пан O. Ювердеану, *адвокати*.

Суд вислухав звернення пана Домокоса-Ханку, пана Ювердеану, пані Брумар та пана Гаврили, і також їх відповіді на запитання суддів.

ФАКТИ

I. ОБСТАВИНИ СПРАВИ

10. Заявник народився у 1979 році та проживає в Бухаресті.

11. З 1 серпня 2004 року до 6 серпня 2007 року він працював у Бухарестському відділенні С., румунської приватної компанії (надалі – «роботодавець»), на посаді інженера з продажу. За запитом свого роботодавця, з метою відповіді на запити покупців, він створив аккаунт для миттєвих відповідей з використанням Yahoo Messenger, сервісу онлайн-чату, який забезпечує передачу тексту в режимі реального часу через інтернет. Він вже мав інший особистий акаунт Yahoo Messenger.

12. Внутрішні розпорядження роботодавця забороняли працівникам користуватися ресурсами компанії, з наступним формулюванням:

Стаття 50

“Будь-яке порушення порядку та дисципліни на території компанії суворо забороняється, зокрема:

...

– ... використання з особистою метою комп’ютерів, фотокопірів, телефонів або приладів для телексу та факсу.”

13. Положення не містили жодних посилань на можливість роботодавця відстежувати розмови підлеглих.

14. З наданих Урядом документів видається, що заявникові було повідомлено про внутрішні розпорядження роботодавця, і він підписав їх копію 20 грудня 2006 року, після ознайомлення зі змістом.

15. 3 липня 2007 року Бухарестське відділення отримало та поширило серед усіх працівників інформаційне повідомлення, яке було складено та відправлено Клузьким головним офісом 26 червня 2007 року. Роботодавець просив працівників ознайомитися з повідомленням та підписати його копію. Відповідні частини повідомлення містили наступне:

“1. ... Час, проведений у компанії, повинен бути якісним часом для всіх! Приходьте на роботу для праці та вирішення професійних питань, а не ваших особистих проблем! Не витрачайте час для користування інтернетом, телефоном або факсом для питань, які не відносяться до праці або ваших обов’язків. Це диктують [базова освіта], здоровий глузд та закон! Роботодавець зобов’язаний контролювати та моніторити працю робітників і вживати карних заходів до тих, хто винен!

Ваші порушення будуть ретельно відстежуватися та каратися!

2. У зв’язку з повторюваними [дисциплінарними] порушеннями стосовно начальника, [а також] використання інтернету, телефону та фотокопіру у власних цілях, недбалістю та нездатністю виконувати свої обов’язки, пані Б.А. була звільнена на дисциплінарній підставі! Візьміть урок з її поганого прикладу! Не робіть тих же помилок!

3. Уважно прочитайте колективний трудовий договір, внутрішні положення компанії, вашу посадову інструкцію та трудовий договір, який ви підписали! Це є підґрунтям нашої співпраці! Між роботодавцем та працівником! ...”

16. Також з наданих Урядом документів, у тому числі реєстру відвідуваності роботодавця, видається, що заявник ознайомився з повідомленням та підписав його у період з 3 до 13 липня 2007 року.

17. Крім того, видається, що з 5 до 13 липня 2007 року роботодавець записував переговори заявника з використанням Yahoo Messenger у режимі реального часу.

18. 13 липня 2007 року о 16.30 роботодавець викликав заявника для отримання пояснення. У відповідному повідомленні заявник був проінформований про те, що його розмови у Yahoo Messenger підлягали моніторингу і що існували докази того, що він використовував інтернет в особистих цілях в порушення внутрішніх розпоряджень. Були створені діаграми, які вказували, що інтернет-активність заявника була вищою, ніж у його колег. На той час він не був проінформований про те, чи включав моніторинг його розмов їх зміст. Повідомлення було сформульовано наступним чином:

“Будь ласка, поясніть, чому ви використовуєте ресурси компанії (інтернет-зв’язок, месенджер) для особистих цілей упродовж робочого часу, як демонструють прикріплені діаграми.”

19. Того ж дня заявник проінформував роботодавця у письмовій формі про те, що використовував Yahoo Messenger лише для робочих цілей.

20. О 17.20 pроботодавець знову викликав заявника для отримання пояснення, надіславши наступне повідомлення:

“Будь ласка, поясніть, чому уся кореспонденція, якою ви обмінювалися з 5 до 12 липня 2007 року, використовуючи адресу Бухарестського сайту С., мала приватну мету, як демонструють прикріплені сорок п’ять сторінок.”

21. Сорок п’ять сторінок, згадані у повідомленні, складалися з розшифровки повідомлень, якими заявник обмінювався з братом та нареченою упродовж періоду моніторингу своїх повідомлень; повідомлення стосувалися особистих питань, і деякі мали інтимний характер. До розшифровки також входили п’ять повідомлень, якими заявник обмінювався зі своєю нареченою з використанням особистого акаунту Yahoo Messenger; ці повідомлення не містили ніякої інтимної інформації.

22. Також 13 липня заявник повідомив роботодавцю у письмовій формі, що на його думку, роботодавець учинив кримінальне правопорушення, а саме, порушив таємницю кореспонденції.

23. 1 серпня 2007 року роботодавець розірвав робочий контракт заявника.

24. Заявник опротестував своє звільнення у заяві до Бухарестського окружного суду (надалі – «окружний суд»). Він попросив суд, по-перше, відставити у сторону звільнення; по-друге, наказати роботодавцеві сплатити йому суми, які він заборгував стосовно заробітної плати та будь-яких інших виплат, та повернути його до посади; і по-третє, наказати роботодавцеві сплатити йому 100,000 румунських лей (приблизно 30,000 євро) в якості відшкодування шкоди, понесеної в результаті його звільнення, та відшкодувати судові витрати.

25. Щодо суті справи, спираючись на справу *Copland v. the United Kingdom* (№ 62617/00, §§ 43-44, ECHR 2007‑I), заявник стверджував, що розмови працівників за телефоном та електронною поштою на робочому місці охоплювалися поняттями «приватне життя» та «кореспонденція», і тому були захищені статтею 8 Конвенції. Заявник також стверджував, що рішення щодо його звільнення було незаконним, і що контролюючи його розмови та маючи доступ до їх змісту, роботодавець порушив кримінальне право.

26. Беручи до уваги шкоду, яку він отримав, за власними словами, заявник прийняв до уваги характер свого звільнення та стверджував, що зазнав переслідування з боку роботодавця у зв’язку з моніторингом його розмов та розкриттям їх змісту «колегам, які так або інакше брали участь у процедурі звільнення».

27. Заявник надав докази, у тому числі повну копію розшифровки його розмов за допомогою Yahoo Messenger та копію інформаційного повідомлення (див. пункт вище).

28. У рішенні від 7 грудня 2007 року окружний суд відхилив звернення заявника та підтвердив, що його звільнення було законним. Відповідні частини рішення містять наступне:

“Порядок проведення дисциплінарного розслідування чітко регулюється положеннями статті 267 Трудового кодексу.

У даній справі було продемонстровано, за допомогою письмових документів, прикріплених до матеріалів справи, що роботодавець провів дисциплінарне розслідування стосовно заявника, коли два рази викликав його у письмовій формі для надання пояснення та зазначення теми, дати, часу та місця інтерв’ю, а також того, що заявник мав можливість надати аргументи у свій захист стосовно стверджуваних дій, як очевидно з двох пояснювальних повідомлень, прикріплених до матеріалів (див. копії на сторінках 89 та 91).

Суд вважає, що моніторинг інтернет-розмов, у яких заявник брав участь з використанням програмного забезпечення Yahoo Messenger на комп’ютері компанії упродовж робочого часу – незалежно від того, чи були дії роботодавця незаконними з точки зору кримінального законодавства – не може підірвати належність дисциплінарних проваджень у даній справі.

Той факт, що положення стосовно вимоги допитати підозрюваного (*învinuitul*) у справі про стверджуване порушення та дослідити аргументи, надані на захист цієї особи, до того, як рішення про санкцію буде прийнято в імперативних термінах, підкреслює намір законодавства зробити повагу до прав захисту передумовою для належності рішення про накладення санкції.

У даній справі, оскільки працівник наполягав протягом дисциплінарного розслідування, що користувався Yahoo Messenger не для особистих цілей, а для надання порад покупцям щодо продуктів, які продавав роботодавець, суд вважає, що перевірка змісту розмов [заявника] була єдиним шляхом, за допомогою якого роботодавець міг перевірити обґрунтованість своїх аргументів.

Право роботодавця на моніторинг (*monitoriza*) працівників на робочому місці, [особливо] в тому, що стосується користування робочими комп’ютерами, формує частину більш широкого права, яке регулюється положеннями статті 40 (d) Трудового кодексу, права контролювати те, як працівники виконують свої робочі обов’язки.

Оскільки було продемонстровано, що увага працівників була звернута на той факт, що незадовго до дисциплінарної санкції заявника інший працівник був звільнений через використання інтернету, телефону та фотокопіру для особистих цілей, і що працівників попередили, що їх діяльність підлягатиме моніторингу (див. повідомлення № 2316 від 3 липня 2007 року, яке заявник підписав [після] ознайомлення – див. копію на листі 64), роботодавця не можна обвинувачувати у демонстрації відсутності транспарентності та у ненаданні працівникам чіткого попередження про те, що він моніторив їх користування комп’ютерами.

Доступ до інтернету на робочому місці є, перш за все, інструментом, який роботодавець робить доступним для працівників для професійного використання, і роботодавець, безперечно, має повноваження моніторити користування інтернетом в особистих цілях, в силу свого права контролювати діяльність працівників.

Такі перевірки з боку роботодавця є необхідними у зв’язку, наприклад, з ризиком того, що через використання інтернету працівники можуть пошкодити IT-системи компанії, здійснювати незаконну діяльність у киберпросторі, за яку компанія понесе відповідальність, або розкрити комерційну таємницю компанії.

Суд вважає, що скоєні заявником дії становлять дисциплінарне правопорушення у розумінні статті 263 § 2 Трудового кодексу, оскільки становлять порушення положення статті 50 внутрішніх положень С. ..., які забороняють використання комп’ютерів в особистих цілях.

Вищенаведені дії у внутрішніх розпорядженнях вважаються серйозними порушеннями, покаранням за які, відповідно до статті 73 тих же внутрішніх положень, [є] розривання робочого контракту з дисциплінарних підстав.

Беручи до уваги фактичні та юридичні аргументи, наведені вище, суд вважає, що оскаржуване рішення є обґрунтованим та законним, і відхиляє заяву, як необґрунтовану.”

29. Заявник оскаржив це рішення в Апеляційному суді Бухареста (надалі – «апеляційний суд»). Він повторив аргументи, які надав у суді першої інстанції та стверджував на додаток, що суд не досяг справедливого балансу інтересів, несправедливо поставивши у пріоритет інтерес роботодавця у користуванні свободою розсуду під час контролю часу та ресурсів працівників. Він також стверджував, що ані внутрішні розпорядження, ані інформаційне повідомлення не містило будь-яких ознак того, що роботодавець міг моніторити розмови працівників.

30. Апеляційний суд відхилив апеляцію заявника у рішенні від 17 червня 2008 року, відповідні частини якого містять наступне:

“Суд першої інстанції зробив правильний висновок про те, що інтернет є інструментом, який роботодавець робить доступним для працівників для професійного використання, і що роботодавець має право встановлювати правила для користування цим інструментом, наводячи заборони та положення, яких працівники повинні дотримуватися при користуванні інтернетом на робочому місці; очевидно, що в користуванні в особистих цілях можна відмовити, і що працівники у даній справі були належним чином проінформовані про це у повідомленні, виданому 26 червня 2007 року, відповідно до положень внутрішніх розпоряджень, у яких вони були проінструктовані щодо дотримання графіку, присутності на робочому місці [упродовж робочого часу та] ефективного використання робочого часу.

Щодо висновку – роботодавець, який зробив вклад, має право, при користуванні правами, закріпленими у статті 40 § 1 Трудового кодексу, моніторити користування інтернетом на робочому місці, а працівник, який порушує правила роботодавця щодо користування інтернетом в особистих цілях, вчиняє дисциплінарне порушення, яке може призвести до санкції, у тому числі серйозної.

Безсумнівно, існує конфлікт між правом роботодавця на моніторинг і правом працівників на захист їх приватного життя. Цей конфлікт був вирішений на рівні Європейського Союзу шляхом прийняття Директиви № 95/46/EC, яка виклала низку принципів, що регулюють моніторинг користування інтернетом та електронною поштою на робочому місці, у тому числі, зокрема, наступне.

- Принцип необхідності: моніторинг повинен бути необхідним для досягнення певної мети.

- Принцип зазначення мети: дані повинні збиратися з конкретною, чіткою та законною метою.

- Принцип транспарентності: роботодавець повинен надати працівникам повну інформацію про моніторингові операції.

- Принцип законності: операції з опрацювання даних можуть відбуватися лише з законною метою.

- Принцип пропорційності: персональні дані, які контролюються, повинні бути відповідними та належними стосовно конкретної мети.

- Принцип безпеки: роботодавець повинен вжити усі необхідні заходи безпеки для забезпечення того, щоб зібрані дані не були доступними третім сторонам.

З оглядом на той факт, що роботодавець мав право і обов’язок забезпечити безперебійне функціонування компанії і для цього [мав право] контролювати те, як працівники виконують професійні обов’язки, і той факт, [що він] користується дисциплінарними повноваженнями, які може використовувати законним шляхом і які [дозволяли у даній справі] моніторити та розшифровувати розмови за допомогою Yahoo Messenger, особисту мету яких працівник заперечував, після того, як працівник та його колеги були попереджені про те, що ресурси компанії не можна використовувати для таких цілей, не можна стверджувати, що такої законної мети можна було досягнути за допомогою будь-яких інших засобів, ніж порушення таємниці кореспонденції, або що не був досягнутий справедливий баланс між необхідністю захистити приватність [працівника] та правом роботодавця контролювати функціонування його бізнесу.

...

Відповідно, беручи до уваги наведені вище міркування, суд вважає, що рішення суду першої інстанції є законним та обґрунтованим, і що апеляція є необґрунтованою; тому вона повинна бути відхилена, відповідно до статті 312 § 1 Цивільно-процесуального кодексу.”

31. У той час, 18 вересня 2007 року заявник подав скаргу у кримінальному порядку проти статутних представників С., стверджуючи про порушення таємниці кореспонденції. 9 травня 2012 року Управління розслідування організованої злочинності та тероризму (УРОЗТ) прокуратури при Верховному касаційному суді постановило, що не було підстав відповідати, на підставі того, що компанія була власником комп’ютерної системи та інтернет-зв’язку і тому могла моніторити інтернет-активність своїх працівників і використовувати інформацію, яка зберігалася на серверах, а також беручи до уваги заборону на користування IT-системами в особистих цілях, в результаті чого моніторинг був передбачуваний. Заявник не скористався можливістю опротестувати рішення органів прокуратури в національних судах, яку передбачали застосовні процесуальні правила.

II. ВІДПОВІДНЕ НАЦІОНАЛЬНЕ ЗАКОНОДАВСТВО

A. Конституція

32. Відповідні частини Конституції Румунії передбачають:

Стаття 26

“1. Громадські органи влади поважають та захищають інтимне, сімейне та приватне життя.”

Стаття 28

“Таємниця листування, телеграфних повідомлень, інших поштових відправлень, телефонних розмов та будь-яких інших законних засобів зв’язку недоторканна.”

B. Кримінальний кодекс

33. Відповідні частини Кримінального кодексу, який був у силі на той час, передбачають:

Стаття 195 – Порушення таємниці кореспонденції

“1. Будь-яка особа, яка незаконно відкриє кореспонденцію іншої особи або перехопить розмови інших осіб чи спілкування з використанням телефону, телеграфу або будь-яких інших засобів передачі даних на велику відстань, понесе відповідальність у вигляді позбавлення волі на строк від шести місяців до трьох років.”

C. Цивільний кодекс

34. Відповідні положення Цивільного кодексу, який був у силі на час відповідних подій, були сформульовані наступним чином:

Стаття 998

“Будь-яка дія, вчинена особою, яка шкодить іншій особі, робить особу, яка заподіяла шкоду, відповідальною за її виправлення.”

Стаття 999

“Кожен несе відповідальність за шкоду, яку заподіяв не тільки власними діями, але і своєю бездіяльністю або недбалістю.”

D. Трудовий кодекс

35. У формулюванні, актуальному на той час, Трудовий кодекс передбачав:

Стаття 40

“1. Роботодавець, у принципі, має наступні права:

...

(d) право контролювати, як [працівники] виконують професійні обов’язки;

...

2. Роботодавець, у принципі, має наступні обов’язки:

...

(i) гарантувати конфіденційність персональних даних працівників.”

E. Закон № 677/2001 про захист осіб у зв’язку з опрацюванням персональних даних та про вільне переміщення таких даних

36. Відповідні частини Закону № 677/2001 про захист осіб у зв’язку з опрацюванням персональних даних та про вільне переміщення таких даних (надалі «Закон № 677/2001»), який відтворює певні положення Директиви 95/46/EC Європейського Парламенту та Ради Європейського Союзу від 24 жовтня 1995 року про захист осіб у зв’язку з опрацюванням персональних даних та про вільне переміщення таких даних (див. пункт нижче), передбачають:

Стаття 3 – Терміни

“У цьому законі наведені нижче терміни означають наступне:

(a) ’персональні дані’ – будь-яка інформація, яка відноситься до ідентифікованої або такої, що може бути ідентифікована, фізичної особи; особа, яка може бути ідентифікована – це особа, яку можна упізнати прямим або непрямим шляхом, зокрема, за ідентифікаційним номером або однією чи декільком характерним рисам фізичних, фізіологічних, економічних, культурних або соціальних особливостей такої особи;

...”

Стаття 5 – Умови законності при опрацюванні даних

“1. Персональні дані ... не можуть бути опрацьовані будь-яким шляхом, якщо суб’єкт даних не дав чітку та недвозначну згоду на це.

2. Згода суб’єкта даних не буде необхідною за наступних обставин:

(a) якщо опрацювання є необхідним для виконання контракту, стороною якого є суб’єкт даних, або для вжиття заходів за запитом суб’єкта даних до укладення контракту;

...

(e) якщо опрацювання даних є необхідним для цілей законних інтересів, переслідуваних контролером або третьою стороною, або сторонами, яким розкриваються дані, окрім випадків, коли над такими інтересами переважають інтереси або основоположні права та свободи суб’єкта даних;

...

3. Положення пункту 2 не завдають шкоди статутним положенням, які регулюють обов’язок громадських органів влади щодо поваги та захисту інтимного, сімейного та приватного життя.”

Стаття 18 – Право на звернення до суду

“1. Суб’єкти даних мають право звернутися до суду для захисту прав, які гарантує цей Закон і які були порушені, яке не завдає шкоди можливості подати скаргу до контролюючого органу.

2. Будь-яка особа, яка понесла шкоду в результаті незаконного опрацювання своїх персональних даних, може звернутися до компетентного суду за відшкодуванням [шкоди].

...”

III. МІЖНАРОДНЕ ПРАВО ТА ПРАКТИКА

A. Стандарти Організації Об’єднаних Націй

37. Настанови для регулювання комп’ютеризованих персональних даних, прийняті Генеральною Асамблеєю ООН 14 грудня 1990 року в Резолюції 45/95 (A/RES/45/95), наводять мінімальні гарантії, які повинно передбачати національне законодавство. Відповідні принципи передбачають:

“**1. Принцип законності та чесності**

Інформація про осіб не повинна збиратися або оброблятися нечесними або незаконними шляхами, вона не повинна використовуватися для цілей, які суперечать цілям та принципам Хартії Європейських Націй.

**2. Принцип точності**

Особи, які відповідають за складання файлів або їх зберігання, мають обов’язок проводити регулярні перевірки точності та актуальності записаних даних і забезпечувати, щоб вони були найповнішими для уникнення помилок або опущень, і щоб вони регулярно оновлювалися, або коли інформація, яка міститься у файлі, використовується протягом опрацювання інформації.

**3. Принцип уточнення мети**

Мета, якій повинен служити файл та його використання для цієї мети, повинна бути точною, законною, та, після встановлення, отримати певний ступінь публічності, або повинна бути доведеною до уваги відповідної особи, щоб зробити можливим подальше забезпечення наступного:

(a) Усі персональні дані, які збираються та записуються, повинні залишатися актуальними та відповідати заявленій меті;

(b) Ніякі з відповідних персональних даних не повинні використовуватися або розкриватися, без згоди відповідної особи, для цілей, несумісних з заявленою метою;

(c) Період зберігання даних не повинен перевищувати період, який дозволить досягти заявленої мети.

**4. Принципи доступу зацікавленої особи**

Кожна особа, яка має докази щодо своєї ідентифікації, має право знати, чи обробляється інформація щодо неї, та отримувати її у зрозумілій формі, без неналежних затримок або витрат, і вимагати здійснити відповідні виправлення або видалення у випадку незаконних, непотрібних або неточних записів, і коли дані передаються, особа має право бути проінформованою про адресатів. Повинно бути зроблено положення про захист правового захисту, якщо це необхідно, у контролюючому органі, указаному у принципі 8 нижче. Вартість будь-якого виправлення несе особа, відповідальна за матеріали справи. Бажано, щоб положення цього принципу застосовувалися до кожної особи, незалежно від національності або місця проживання.

...

**6. Повноваження щодо виключень**

Відхилення від принципів 1-4 можуть бути ухвалені тільки якщо вони є необхідними для захисту національної безпеки, громадського порядку, громадського здоров’я або моралі, а також, зокрема, прав та свобод інших осіб, особливо переслідуваних осіб (гуманітарна стаття), за умови, якщо таке відхилення чітко зазначено у законі або аналогічному положенні, оприлюдненому відповідно до внутрішньої правової системи, яке чітко означує обмеження та встановлює відповідні гарантії.

...”

38. Міжнародна організація праці (МОП) видала Кодекс практики щодо захисту персональних даних працівників (надалі – «Кодекс практики МОП») у 1997 році, в якому наводилися наступні принципи:

“**5. Загальні принципи**

5.1. Персональні дані повинні опрацьовуватися законно та чесно, і тільки для цілей, які мають пряме відношення для роботи працівника.

5.2. Персональні дані, у принципі, повинні використовуватися лише для цілей, для яких вони збиралися.

5.3. Якщо персональні дані повинні опрацьовуватися для цілей, які відрізняються від цілей, за яких дані збиралися, роботодавець повинен забезпечити, щоб вони не використовувалися способом, несумісним із початковою метою, і повинен вжити необхідних заходів для уникнення будь-яких непорозумінь, спричинених зміною мети.

5.4. Персональні дані, зібрані у зв’язку з технічними або організаційними заходами для забезпечення безпеки та належного функціонування автоматизованих інформаційних систем, не повинні використовуватися для контролю за поводженням працівників.

5.5. Рішення стосовно працівника не повинні ґрунтуватися лише на особистій обробці персональних даних цього працівника.

5.6. Персональні дані, зібрані за допомогою електронного моніторингу, не повинні бути єдиними чинниками при оцінці ефективності працівника.

5.7. Роботодавці повинні регулярно оцінювати свою практику опрацювання даних:

(a) для якомога сильнішого зменшення типу та обсягу персональних даних, які збираються, та

(b) для поліпшення шляхів захисту приватності працівників.

5.8. Працівників та їх представників необхідно інформувати про будь-який процес зібрання даних, правила, які регулюють цей процес, та їх права.

...

5.13. Працівники не можуть відмовитися від своїх прав на приватність.”

39. Стосовно більш конкретного питання моніторингу працівників, Кодекс практики МОП містить наступне:

“**6. Зібрання персональних даних**

6.1. Усі персональні дані, у принципі, повинні бути отримані від окремого працівника.

...

6.14. (1) Якщо працівники підлягають моніторингу, їх необхідно інформувати заздалегідь про підстави для моніторингу, розпорядок, застосовані методи та техніки, а також про дані, які збираються, і роботодавець повинен мінімізувати втручання у приватність працівників.

(2) Таємний моніторинг дозволяється лише у наступних випадках:

(a) якщо він відповідає національному законодавству; або

(b) якщо існує обґрунтована підозра кримінальної діяльності або іншого тяжкого порушення.

(3) Тривалий моніторинг повинен дозволятися, лише якщо його роблять необхідним питання здоров’я та безпеки або захисту майна.”

40. Кодекс Практики МОП також включає перелік індивідуальних прав працівників, зокрема тих, що стосується інформації про опрацювання персональних даних, доступу до таких даних та перегляду будь-яких вжитих заходів. Відповідні частини передбачають:

“**11. Індивідуальні права**

11.1. Працівники повинні мати право бути регулярно проінформованими про персональні дані, які збираються стосовно них, та про обробку таких даних.

11.2. Працівники повинні мати доступ до усіх своїх персональних даних, незалежно від того, чи такі дані обробляються автоматизованими системами або зберігаються у певному файлі, створеному у ручному режимі, стосовно окремого працівника, або у будь-якому іншому файлі, до якого входять персональні дані працівника.

11.3. Право працівника знати про обробку своїх персональних даних повинно включати право вивчати та отримувати копії будь-яких записів у той мірі, в якій дані, що містяться у записах, містять персональні дані працівника.

...

11.8. У випадку розслідування в інтересах безпеки роботодавці повинні мати право заперечити працівнику доступ до персональних даних цього працівника до закриття розслідування і в тій мірі, в якій цілі розслідування можуть бути під загрозою. Однак, ніяке рішення стосовно робочих відносин не може бути прийнятим до того, як працівник отримає доступ до усіх своїх персональних даних.

11.9. Працівники повинні мати право вимагати видалення або виправлення неправильних або неповних персональних даних, а також персональних даних, оброблених не у відповідності до положень цього кодексу.

...

11.13. У будь-якому законодавстві, нормативному акті, колективному договорі, робочих правилах або політиці, розробленій відповідно до положень цього кодексу, повинен вказуватися шлях для відшкодування, який дозволить працівникам опротестувати застосування роботодавцем цього інструменту. Необхідно встановити порядок отримання будь-якої скарги, поданої працівниками, та відповіді на неї. Процес оскарження повинен бути легкодоступним для працівників та простим у використанні.”

41. На додаток, 18 грудня 2013 року Генеральна Асамблея ООН прийняла Резолюцію № 68/167 про право на недоторканність приватного життя у цифрову епоху (A/RES/68/167), в якій, зокрема, закликала держави:

“(*a*) Поважати та захищати право на недоторканність приватного життя, у тому числі у контексті цифрової комунікації;

(*b*) Вжити заходів для того, щоб покласти край порушенням цих прав та створити умови для запобігання таким порушенням, у тому числі шляхом забезпечення того, щоб відповідне національне законодавство відповідало їх міжнародним зобов’язанням по міжнародному праву прав людини;

(*c*) Провести огляд своїх процедур, практики та законодавства, які стосуються спостереження за повідомленнями, їх перехоплення та зібрання персональних даних, у тому числі масового спостереження, перехоплення та зібрання, в цілях захисту права на недоторканність приватного життя шляхом забезпечення повного та ефективного виконання усіх обов’язків відповідно до національного права прав людини;

(*d*) Встановити нові або підтримувати існуючі незалежні, ефективні внутрішні наглядові механізми, здатні забезпечити транспарентність у відповідних випадках та підзвітність у державному нагляді за повідомленнями, їх перехопленні та зібранні персональних даних[.]”

B. Стандарти Ради Європи

42. Конвенція Ради Європи про захист осіб у зв’язку з автоматизованою обробкою персональних даних (1981, ETS № 108), яка набула сили стосовно Румунії 1 червня 2002 року, включає, зокрема, наступні положення:

Стаття 2 – Визначення

“Для цілей цієї Конвенції:

(a) термін "персональні дані" означає будь-яку інформацію, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною (далі - суб'єкт даних);

...

(c) термін "автоматизована обробка" включає такі операції, що здійснюються повністю або частково за допомогою автоматизованих засобів: зберігання даних, виконання логічних та (або) арифметичних операцій із цими даними, їхню зміну, знищення, вибірку або поширення;

...”

Стаття 3 – Сфера застосування

“1. Сторони зобов'язуються застосовувати цю Конвенцію до файлів персональних даних для автоматизованої обробки та до автоматизованої обробки персональних даних у державному та приватному секторах.

...”

Стаття 5 – Якість даних

“Персональні дані, що піддаються автоматизованій обробці,   
повинні:

(a) отримуватися та оброблятися сумлінно та законно;

(b) зберігатися для визначених і законних цілей та не використовуватися в спосіб, не сумісний із цими цілями;

(c) бути адекватними, відповідними та ненадмірними стосовно цілей, для яких вони зберігаються;

(d) бути точними та в разі необхідності оновлюватися;

(e) зберігатись у формі, яка дозволяє ідентифікацію суб'єктів даних не довше, ніж це необхідно для мети, для якої такі дані зберігаються.”

Стаття 8 – Додаткові гарантії для суб’єкта даних

“Будь-якій особі надається можливість:

(a) з'ясувати існування файлу персональних даних для автоматизованої обробки, його головні цілі, а також особу та постійне місце проживання чи головне місце роботи контролера файлу;

(b) отримувати через обґрунтовані періоди та без надмірної затримки або витрат підтвердження або спростування факту зберігання персональних даних, що її стосуються, у файлі даних для автоматизованої обробки, а також отримувати такі дані в доступній для розуміння формі;

...

(d) використовувати засоби правового захисту в разі невиконання передбаченого в пунктах "b" і "c" цієї статті прохання про підтвердження або у відповідних випадках про надання, виправлення або знищення персональних даних.”

Стаття 9 – Винятки та обмеження

“...

2. Відхилення від положень статей 5, 6 та 8 цієї Конвенції дозволяється тоді, коли таке відхилення передбачене законодавством Сторони та є в демократичному суспільстві необхідним заходом, спрямованим на:

(a) захист державної та громадської безпеки, фінансових інтересів держави або на боротьбу з кримінальними правопорушеннями;

(b) захист суб'єкта даних або прав і свобод інших людей;

...”

Стаття 10 – Санкції та засоби правового захисту

“Кожна Сторона зобов'язується встановити відповідні санкції та засоби правового захисту стосовно порушень положень внутрішнього права, що запроваджують основоположні принципи захисту персональних даних, визначені в цій главі.”

43. Рекомендація CM/Rec(2015)5 Комітету міністрів державам-учасникам щодо обробки персональних даних у контексті працевлаштування, яка була прийнята 1 квітня 2015 року, містить наступне:

“**4. Застосування принципів обробки даних**

4.1. Роботодавці повинні мінімізувати обробку персональних даних до даних, необхідних для переслідуваної мети в окремих справах.

...

**6. Внутрішнє використання даних**

6.1. Персональні дані, які збираються для цілей працевлаштування, повинні оброблятися роботодавцями лише для таких цілей.

6.2. Роботодавці повинні приймати політику, правила та/або інші інструменти щодо обробки даних для внутрішнього використання персональних даних у відповідності до принципів даної рекомендації.

...

**10. Транспарентність обробки**

10.1. Інформація стосовно персональних даних, якими володіють роботодавці, повинна бути доступною або безпосередньо відповідному працівнику, або за допомогою його представників, або доведена до уваги працівника за допомогою інших доречних засобів.

10.2. Роботодавці повинні надавати працівникам наступну інформацію:

– категорії персональних даних, які обробляються, та опис цілей обробки;

– одержувачі або категорії одержувачів персональних даних;

– доступні працівникам засоби користування правами, наведеними у пункті 11 цієї рекомендації, без шкоди для більш переважних засобів, гарантованих національним законодавством або їх правовою системою;

– будь-яку іншу інформацію, необхідну для забезпечення чесного та законного опрацювання.

10.3. Необхідно надавати особливо чіткий та повний опис категорій персональних даних, які будуть збиратися за допомогою ІКТ, у тому числі відеоспостереження, та їх можливого використання. Цей принцип також застосовується до конкретних форм обробки, передбачених у частині II додатку до даної рекомендації.

10.4. Інформація повинна надаватися у доступному форматі та регулярно оновлятися. У будь-якому випадку така інформація повинна надаватися до того як працівник здійснить відповідну дію, і бути доступною в інформаційних системах, які зазвичай використовує працівник.

...

**14. Використання інтернету та електронного зв’язку на робочому місці**

14.1. Роботодавці повинні уникати невиправданих та необґрунтованих втручань у право працівників на недоторканність приватного життя. Цей принцип поширюється на усі технічні прилади та ІКТ, якими користується працівник. Відповідні особи повинні бути належним чином та регулярно проінформовані про застосування чіткої політики приватності, відповідно до принципу 10 даної рекомендації. Інформацію, яка надається, необхідно зберігати в актуальному стані, і вона повинна включати ціль обробки або зберігання даних про трафік та архівацію професійних електронних спілкувань.

14.2. Зокрема, у випадку обробки персональних даних, які стосуються сторінок в інтернеті або інтранеті, відвіданих працівником, слід надавати перевагу вживанню запобіжних заходів, таких, як використання фільтрів, які запобігають конкретним операціям, і оцінці можливого моніторингу персональних даних, надаючи перевагу не-індивідуальним випадковим перевіркам анонімних або якимось чином агрегованих даних.

14.3. Доступ роботодавців до професійного електронного спілкування їх працівників, які були проінформовані заздалегідь про існування такої можливості, може відбуватися лише, якщо це необхідно, на підставах безпеки або інших законних підставах. У випадку відсутніх працівників роботодавець повинен вжити необхідні заходи та передбачити доречні процедури, спрямовані на забезпечення доступу до професійних електронних видів спілкування, лише коли у такому доступі є професійна необхідність. Доступ повинен здійснюватися у найменш агресивній формі і лише після інформування відповідних працівників.

14.4. Зміст, відправлення та отримання приватних електронних повідомлень на робочому місці не повинні відстежуватися за жодних обставин.

14.5. Після того, як працівник покидає організацію, роботодавець повинен вжити необхідні організаційні та технічні заходи для автоматичної деактивації акаунту працівника для відправлення електронних повідомлень. Якщо роботодавцю потрібно відновити зміст акаунту працівника для ефективного функціонування організації, він повинен зробити це до того, як працівник залишить організацію, і, якщо це можливо, у присутності цього працівника.”

IV. ПРАВО ЄВРОПЕЙСЬКОГО СОЮЗУ

44. Відповідні положення Хартії основних прав Європейського Союзу (2007/C 303/01) сформульовані наступним чином:

Стаття 7 – Повага до приватного та сімейного життя

“Кожна особа має право на повагу до її приватного та сімейного життя, недоторканність житла та таємницю кореспонденції.”

Стаття 8 – Захист персональних даних

“1. Кожна особа має право на захист персональних даних, які стосуються неї.

2. Такі дані повинні використовуватися відповідно до встановлених правил у відповідних цілях та на основі дозволу відповідної особи, або на іншій законній основі, викладеній у законодавстві. Кожна особа має право на доступ до даних, які були зібрані щодо неї, і право внести виправлення у ці дані.

3. Дотримання цих правил повинно підлягати контролю з боку незалежного органу влади.”

45. Директива 95/46/EC Європейського парламенту та Ради Європейського Союзу від 24 жовтня 1995 року про захист фізичних осіб при обробці персональних даних та про вільне переміщення таких даних (Надалі – «Директива 95/46/EC») зазначає, що метою національного законодавства про обробку персональних даних є захист права на недоторканність приватного життя, як визнається у статті 8 Конвенції та у загальних принципах законодавства Співтовариства. Відповідні положення Директиви 95/46/EC містять наступне:

Стаття 2 – Визначення

“В цілях даної Директиви:

(a) "персональні дані" означають будь-яку інформацію, що стосується встановленої фізичної особи чи фізичної особи, яку можна встановити ("суб'єкт даних"); 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;

...”

Стаття 6

“1. Держави-члени передбачають, що персональні дані повинні:

(a) оброблятися чесно і законно;

(b) збиратися для встановлених, чітких і законних цілей і надалі не оброблятися у спосіб, несумісний з цими цілями. Подальша обробка даних в історичних, статистичних чи наукових цілях не розглядається як несумісна, якщо держави-члени забезпечують відповідні гарантії;

(c) бути достовірними, відповідними і не надлишковими відносно цілей, заради яких вони збираються і/або надалі обробляються;

(d) бути точними і, якщо необхідно, обновлятися; слід вжити всіх розумних заходів, щоб гарантувати, що дані, які є неточними чи неповними, з урахуванням цілей, заради яких вони були зібрані чи заради яких вони надалі обробляються, стиралися чи виправлялися;

(e) зберігатися у формі, що дозволяє встановлювати особу суб'єктів даних не довше, ніж це необхідно для цілей, заради яких дані були зібрані чи заради яких вони надалі обробляються. Держави-члени встановлюють відповідні гарантії для персональних даних, що зберігаються протягом більш тривалих періодів з метою історичного, статистичного чи наукового використання.

2. Забезпечення дотримання пункту 1 покладається на контролера.”

Стаття 7

“Держави-члени передбачають, що персональні дані можуть оброблятися тільки за умови, що:

(a) суб'єкт даних недвозначно дав свою згоду; чи

(b) обробка необхідна для виконання контракту, стороною якого є суб'єкт даних, чи для вживання заходів на прохання суб'єкта даних до підписання контракту; чи

(c) обробка необхідна для дотримання правового зобов'язання, яким зв'язаний контролер; чи

(d) обробка необхідна для захисту життєво важливих інтересів суб'єкта даних; чи

(e) обробка необхідна для виконання завдання, здійснюваного в суспільних інтересах, чи при виконанні офіційних повноважень, якими наділений контролер або третя сторона, якій надаються дані; чи

(f) обробка необхідна в цілях законних інтересів, переслідуваних контролером чи третьою стороною або сторонами, для яких надаються дані, крім випадків, коли над такими інтересами переважають інтереси основних прав і свобод суб'єкта даних, що вимагають захисту згідно з пунктом 1 статті 1.”

Стаття 8 – Обробка особливих категорій даних

“1. Держави-члени забороняють обробку персональних даних, що вказують на расове чи етнічне походження, політичні погляди, релігійні чи філософські переконання, профспілкове членство, і обробку даних, що стосуються здоров'я чи статевого життя людини.

2. Пункт 1 не застосовується, якщо:

(a) суб'єкт даних дав свою недвозначну згоду на обробку цих даних, крім випадків, коли законодавство держав-членів передбачає, що заборона, згадана в пункті 1, не може бути знята при наданні згоди з боку суб'єкта даних; чи

(b) обробка необхідна з метою виконання зобов'язань і особливих прав контролера в області законодавства про працевлаштування, у тій мірі, у якій це дозволено національним законодавством, що передбачає адекватні гарантії; чи

(c) обробка необхідна для захисту життєво важливих інтересів суб'єкта даних чи іншої особи, якщо суб'єкт даних не може дати свою згоду через свою недієздатність чи неправоздатність; чи

...

(e) обробка стосується даних, що явно оприлюднені суб'єктами даних, чи необхідна для порушення, виконання чи захисту судових позовів.

...

4. За умови надання відповідних гарантій, держави-члени можуть на важливій підставі суспільного інтересу встановлювати винятки на додачу до тих, що передбачені в пункті 2, за допомогою або національного закону, або рішення наглядового органу.”

46. Робоча група з питань захисту даних (надалі – «Робоча група») була створена відповідно до статті 29 Директиви, і відповідно до статті 30, уповноважена:

“(a) розглядати будь-яке питання, що стосується застосування національних заходів, прийнятих відповідно до даної Директиви, з метою сприяння загальному застосуванню таких заходів;

(b) представляти Комісії висновки щодо рівня захисту в Співтоваристві та в третіх країнах;

(c) повідомляти Комісію про будь-яку запропоновану поправку до даної Директиви, про будь-які додаткові чи особливі заходи із захисту прав і свобод фізичних осіб при обробці персональних даних і про будь-які інші запропоновані заходи Співтовариства, що стосуються цих прав і свобод;

(d) виносити висновок про кодекси, складені на рівні Співтовариства.”

Робоча група є незалежним дорадчим органом Європейського Союзу. У вересні 2001 року вона видала висновок про обробку персональних даних у контексті працевлаштування (висновок 8/2001), який узагальнює основні принципи захисту даних: закінченість, транспарентність, законність, пропорційність, точність, безпеку та обізнаність персоналу. У висновку, який Робоча група прийняла відповідно до її ролі сприяння єдиному застосуванню національних заходів, вжитих відповідно до Директиви 95/46/EC, вона зазначила, що моніторинг електронної пошти включав обробку персональних даних, і висловила погляд, що будь-який моніторинг працівників повинен бути

“пропорційною відповіддю роботодавця на ризики, з якими він стикається, беручи до уваги законні інтереси недоторканності приватного життя та інші інтереси працівників.”

47. У травні 2002 року Робоча група видала робочий документ про спостереження та моніторинг електронних видів спілкування на робочому місці (надалі – «робочий документ»), у якому вона прямо врахувала положення Директиви 95/46/EC, взяті у світлі положень статті 8 Конвенції. Робочий документ запевнює, що сам факт того, що моніторинг або спостереження вважаються зручними для інтересів роботодавця, не може виправдати втручання у приватність працівника, і що будь-який моніторинг повинен відповідати чотирьом критеріям: транспарентності, необхідності, чесності та пропорційності.

48. Стосовно технічного аспекту в робочому документі говориться:

“Оперативна інформація може бути легко видана за допомогою такого програмного забезпечення, як попереджуючі вікна, які з’являються та попереджають працівника, що система виявила та/або вжила заходи для запобігання не ухваленого використання мережі.”

49. Більш конкретно, стосовно питання доступу до електронних листів працівників, робочий документ містить наступне:

“ Моніторинг електронної пошти або використання інтернету працівника може вважатися необхідним лише за виняткових обставин. Наприклад, моніторинг електронної пошти працівника може стати необхідним для отримання підтвердження або доказу певних дій з його боку. До таких дій входить злочинна діяльність з боку працівника в тій мірі, в якій роботодавцю необхідно захищати власні інтереси, наприклад, коли він несе відповідальність за дії працівника. До такої діяльності також може входити виявлення вірусів та у загальних термінах – будь-яка діяльність, яку роботодавець здійснює для забезпечення захисту системи.

Слід згадати, що відкриття електронних листів працівників може також бути необхідним за підстав, які не відносяться до моніторингу, наприклад, для продовження кореспонденції у випадку, якщо працівника немає в офісі (у зв’язку з хворобою або відпусткою) і кореспонденцію неможливо продовжувати без цього (наприклад, за допомогою автоматичної відповіді або переадресації).”

50. Суд Європейського Союзу тлумачив положення Директиви 95/46/EC у світлі права на повагу до приватного життя, гарантованого статтею 8 Конвенції, у справі *Österreichischer Rundfunk and Others* (C-465/00, C‑138/01 та C‑139/01, рішення від 20 травня 2003 року, ECLI:EU:C:2003:294, пункти 71 і далі).

51. Регламент (EU) 2016/679 Європейського парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб у зв’язку з опрацюванням персональних даних і про вільне переміщення таких даних, і повторювана Директива 95/46/EC (Загальний регламент захисту даних), опубліковані у OJ 2016 L 119/1, набули сили 24 травня 2016 та скасують Директиву 95/46/EC, починаючи з 25 травня 2018 року (стаття 99). Відповідні положення Регламенту передбачають:

Стаття 30 – Записи опрацювання даних

“1 Кожний контролер і, за необхідності, представник контролера повинні вести запис опрацювання даних, що належать до його сфери відповідальності. Такий запис повинен містити всю інформацію про:

(a) особу та контактні дані контролера та, за необхідності, об’єднаного контролера, представника контролера та співробітника з питань захисту даних;

(b) цілі цього Регламенту;

(c) опис категорій суб’єктів даних і категорій персональних даних;

(d) категорії одержувачів, яким персональні дані були або будуть розкриті, в тому числі одержувачі в третіх країнах або міжнародні організації;

(e) за необхідності, передавання персональних даних третій країні або міжнародній організації, в тому числі, ідентифікацію такої третьої країни чи міжнародної організації та, в разі актів передавання, вказаних у другому підпараграфі статті 49(1), документацію відповідних гарантій;

(f) за можливості, — передбачені часові обмеження для стирання різних категорій даних;

(g) за можливості, — загальний опис технічних і організаційних заходів безпеки, вказаних у статті 32(1).

2. Кожний оператор і, за необхідності, представник оператора повинні вести запис усіх категорій опрацювання, які здійснюють від імені контролера, що містить інформацію про:

(a) особу та контактні дані оператора чи операторів та кожного контролера, від імені якого діє оператор, та, за необхідності, представника контролера або представника оператора та співробітника з питань захисту даних;

(b) категорії опрацювання, що здійснюють від імені кожного контролера;

(c) за необхідності, передавання персональних даних третій країні або міжнародній організації, в тому числі, ідентифікацію такої третьої країни чи міжнародної організації та, в разі актів передавання, вказаних у другому підпараграфі статті 49(1), документацію відповідних гарантій;

(d) за можливості, — загальний опис технічних і організаційних заходів безпеки, вказаних у статті 32(1).

3. Записи, вказані в параграфах 1 і 2, повинні бути оформлені в письмовій формі, в тому числі, — в електронній.

4. Контролер або оператор і, за необхідності, представник контролера або оператора, повинні надавати запис на запит наглядового органу.

5. Обов’язки, вказані в параграфах 1 і 2, не можна застосовувати до підприємства чи організації з кількістю працівників, меншою за 250 осіб, за винятком, якщо здійснюване опрацювання може призвести до виникнення ризику для прав і свобод суб’єктів даних, призначене для окремого випадку, або якщо опрацювання передбачає спеціальні категорії даних, як зазначено в статті 9(1), або персональні дані про судимості і кримінальні злочини, вказані в статті 10.”

Стаття 47 –Зобов’язальні корпоративні правила

“1. Компетентний наглядовий орган затверджує зобов’язальні корпоративні правила відповідно до механізму послідовності, встановленого в статті 63, за умови, що вони:

(a) мають обов’язкову юридичну силу, їх застосовує і забезпечує їх виконання кожний зацікавлений член групи підприємств або групи підприємств, що здійснюють спільну господарську діяльність, в тому числі, їхні працівники;

(b) прямо надають суб’єктам даних права, які можна реалізувати, у зв’язку з опрацюванням їхніх персональних даних; і

(c) відповідають вимогам, встановленим у параграфі 2.

2. Зобов’язальні корпоративні правила, вказані в параграфі 1, повинні чітко визначати принаймні:

(a) структуру та контактні дані групи підприємств або групи підприємств, що здійснюють спільну господарську діяльність, та кожного з їхніх членів;

(b) передавання даних чи низку актів передавання, у тому числі категорії персональних даних, тип опрацювання і його цілі, тип суб’єктів даних, що зазнали впливу, та визначення відповідної третьої країни чи країн;

(c) їхню обов’язкову юридичну природу, як внутрішню, так і зовнішню;

(d) застосування загальних принципів захисту даних, зокрема, цільове обмеження, мінімізацію даних, обмежені періоди зберігання, якість даних, захист даних за призначенням і за замовчуванням, законодавчу базу опрацювання, опрацювання спеціальних категорій персональних даних, заходи для гарантування безпеки даних і вимоги щодо наступних актів передавання до органів, що не пов’язані зобов’язальними корпоративними правилами;

(e) права суб’єктів даних у сфері опрацювання і засоби реалізації таких прав, у тому числі, права не підлягати рішенням, що ґрунтуються винятково на автоматизованому опрацюванні, в тому числі, профайлінгу відповідно до статті 22, права подавати скаргу до компетентного наглядового органу та компетентних судів держав-членів згідно зі статтею 79, та отримувати правовий захист і, за необхідності, відшкодування за порушення зобов’язальних корпоративних правил;

(f) визнання контролером або оператором, що має осідок на території держави-члена, відповідальності за будь-які порушення зобов’язальних корпоративних правил будь-яким залученим членом, що перебуває поза межами Союзу; контролер або оператор звільняються від такої відповідальності частково або повністю лише за умов доведення, що такий член не несе відповідальності за подію, внаслідок якої заподіяно шкоду;

(g) як інформацію про зобов’язальні корпоративні правила, зокрема про положення, вказані в пунктах (г), (е) і (£) цього параграфа, надають суб’єктам даних, в доповнення до статей 13 і 14;

(h) завдання будь-якого співробітника з питань захисту даних, призначеного відповідно до статті 37, або будь-якої іншої особи чи установи, відповідальної за моніторинг дотримання зобов’язальних корпоративних правил в межах групи підприємств або групи підприємств, що здійснюють спільну господарську діяльність, а також моніторинг підготування та розгляду скарг;

(i) процедури подання і розгляду скарг;

(j) механізми в межах групи підприємств або групи підприємств, що здійснюють спільну господарську діяльність, для забезпечення перевірки відповідності зобов’язальним корпоративним правилам. Такі механізми передбачають перевірки захисту даних і методи забезпечення вжиття виправних дій для захисту прав суб’єкта даних. Результати такої перевірки необхідно повідомляти особі чи установі, вказаній в пункті (h), і раді контролюючого підприємства групи підприємств чи групи підприємств, що здійснюють спільну господарську діяльність, та надавати на запит компетентного наглядового органу;

(k) механізми для звітування та запису змін до правил і звітування про такі зміни до наглядового органу;

(l) механізм співпраці з наглядовим органом для забезпечення дотримання будь-яким членом групи підприємств або групи підприємств, що здійснюють спільну господарську діяльність, зокрема шляхом надання наглядовому органу результатів перевірок заходів, вказаних у пункті (j);

(m) механізми для звітування до компетентного наглядового органу про будь-які законні вимоги, які поширюються на члена групи підприємств або групи підприємств, що здійснюють спільну господарську діяльність в третій країні, що ймовірно матимуть суттєві негативні наслідки для гарантій, передбачених зобов’язальними корпоративними правилами; та

(n) відповідне навчання з питань захисту даних для персоналу, що має постійний або регулярний доступ до персональних даних.

3. Комісія має право визначити формат і процедури для обміну інформацією між контролерами, операторами і наглядовими органами для виконання зобов’язальних корпоративних правил у значенні цієї статті. Такі імплементаційні акти ухвалюють відповідно до експертної процедури, встановленої в статті 93(2).”

Стаття 88– Опрацювання в контексті зайнятості

“1. Держави-члени можуть, за допомогою закону чи колективних угод, передбачати спеціальні норми для забезпечення захисту прав і свобод щодо опрацювання персональних даних працівників у контексті зайнятості, зокрема для цілей працевлаштування, виконання трудового договору, в тому числі, виконання обов’язків, установлених законом або колективними угодами, управління, планування та організацію праці, рівність та різноманітність на робочому місці, здоров’я та безпеку на робочому місці, для цілей реалізації і користування, індивідуально чи колективно, правами та перевагами, пов’язаними із зайнятістю, та для цілей припинення трудових відносин.

2. Такі норми повинні включати відповідні і спеціальні заходи для захисту людської гідності суб’єкта даних, законних інтересів і фундаментальних прав, з особливим урахуванням прозорості опрацювання, передавання персональних даних у межах групи підприємств або групи підприємств, що здійснюють спільну господарську діяльність, та систем моніторингу на робочому місці.

3. Кожна держава-член повідомляє Комісію про такі положення свого закону, який вона ухвалює відповідно до параграфа 1, до 25 травня 2018 року та, без затримки, про будь-які подальші зміни і доповнення, що на них впливають.”

V. ПОРІВНЯЛЬНЕ ПРАВО

52. Доступні Суду документи стосовно законодавства держав-членів Ради Європи, зокрема, дослідження тридцяти чотирьох з них, вказують, що всі відповідні держави визнають у загальних поняттях, на конституційному або статутному рівні, право на недоторканність приватного життя та таємницю кореспонденції. Однак, лише Австрія, Фінляндія, Люксембург, Португалія, Словаччина та Великобританія чітко врегулювали питання приватності на робочому місці, у трудових законах або спеціальному законодавстві.

53. Щодо повноважень, які стосуються моніторингу, тридцять чотири держави-члена Ради Європи потребують, щоб роботодавці давали працівникам попередження про моніторинг заздалегідь. Воно може приймати різні форми, наприклад, повідомлення органів захисту персональних даних або представників працівників. Чинне законодавство Австрії, Естонії, Фінляндії, Греції, Литви, Люксембургу, Норвегії, Польщі, Словаччини та колишньої Югославської Республіки Македонії вимагає, щоб роботодавці повідомляли працівникам безпосередньо до початку моніторингу.

54. В Австрії, Данії, Фінляндії, Франції, Німеччині, Греції, Італії, Португалії та Швеції роботодавці можуть моніторити електронні листи, позначені працівниками, як «приватні», без дозволу ознайомлюватися з їх змістом. У Люксембурзі роботодавці не можуть відкривати електронні листи, які позначені, як «приватні», або явно мають приватний характер. Чеська Республіка, Італія та Словенія, а також Республіка Молдова у певній мірі, також обмежують обсяг, у якому роботодавці можуть моніторити спілкування своїх працівників, в залежності від того, чи є спілкування професійним або особистим за характером. У Німеччині та Португалії, як тільки було встановлено, що повідомлення є приватним, роботодавець повинен перестати читати його.

ПРАВО

I. СТВЕРДЖУВАНЕ ПОРУШЕННЯ СТАТТІ 8 КОНВЕНЦІЇ

55. Заявник стверджував, що його звільнення роботодавцем ґрунтувалося на порушенні його права на повагу до недоторканності приватного життя та кореспонденції, і що коли національні суди не скасували цей захід, вони не виконали своє зобов’язання щодо захисту відповідного права. Він спирався на статтю 8 Конвенції, яка передбачає:

“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. Висновки Палати

56. У своєму рішенні від 12 січня 2016 року Палата постановила, по-перше, що стаття 8 Конвенції була застосовною в даній справі. Посилаючись на концепцію обґрунтованого очікування приватності, вона постановила, що дана справа відрізнялася від справи *Copland* (цит. вище, § 41) та *Halford v. the United Kingdom* (25 червня 1997, § 45, *Reports of Judgments and Decisions* 1997‑III) у тому, що внутрішні розпорядження роботодавця заявника у даній справі суворо забороняли працівникам користуватися комп’ютерами та ресурсами компанії для особистих цілей. Палата прийняла до уваги характер спілкування заявника і той факт, що його розшифровка була використана в якості доказу у провадженнях у національному суді, і зробила висновок про те, що на кону було право заявника на повагу до його «приватного життя» та «кореспонденції».

57. Далі, Палата розглянула справу з точки зору позитивних зобов’язань держави, оскільки рішення про звільнення заявника було прийнято приватно-юридичною особою. Тому вона визначила, чи досягли національні органи влади справедливого балансу між правом заявника на повагу до приватного життя і кореспонденції та інтересами його роботодавця.

58. Палата зазначила, що заявник мав можливість звернутися зі справою та аргументами до трудових судів. Суди дійшли висновку про те, що заявник скоїв дисциплінарне правопорушення шляхом використання інтернету для особистих цілей упродовж робочого часу, і при цьому вони взяли до уваги процес дисциплінарних проваджень, зокрема – той факт, що роботодавець мав доступ до змісту розмов заявника лише після того, що заявник оголосив, що користувався Yahoo Messenger для робочих цілей.

59. Палата також зазначила, що національні суди не ґрунтували свої рішення на змісті переговорів заявника, і що моніторинг роботодавця обмежувався використанням заявником Yahoo Messenger.

60. Відповідно, Палата постановила, що не було порушення статті 8 Конвенції.

B. Обсяг справи у Великій Палаті

61. Суд зазначає, що у провадженнях у Палаті заявник стверджував, що рішення його роботодавця про розривання контракту ґрунтувалося на порушенні його права на повагу до недоторканності приватного життя і кореспонденції, закріпленого у статті 8 Конвенції, і що, не скасувавши цей захід, національні суди не виконали своє зобов’язання щодо захисту відповідного права. Палата проголосила цю скаргу прийнятною 12 січня 2016 року.

62. Суд повторює, що справа, передана до Великої Палати, є заявою, оскільки вона була проголошена прийнятною в Палаті (див. *K. and T. v. Finland* [GC], № 25702/94, §§ 140-41, ECHR 2001‑VII; *D.H. and Others v. the Czech Republic* [GC], № 57325/00, § 109, ECHR 2007‑IV; та *Blokhin v. Russia* [GC], no. 47152/06, § 91, ECHR 2016).

63. У своїх зауваженнях у Великій Палаті заявник уперше скаржився на відхилення скарги у кримінальному порядку у 2012 році, яку він подав у зв’язку зі стверджуваним порушенням таємниці кореспонденції (див. пункт нижче).

64. Ця нова скарга не була згадана у рішенні від 12 січня 2016 року щодо прийнятності, яке визначає межі розгляду заяви. Тому вона виходить за межі обсягу справи, визначеного Великою Палатою, яка, відповідно, не має юрисдикції щодо розгляду цієї скарги, і тому обмежиться розглядом скарги, яку Палата проголосила прийнятною.

C. Застосовність статті 8 Конвенції

1. Доводи сторін

(a) Уряд

65. Уряд стверджував, що заявник не міг заявляти про будь-які очікування «приватності» в тому, що стосується розмов з використанням сервісу обміну миттєвими повідомленнями, акаунт у якому був створений для професійного користування. Посилаючись на прецедентну практику судів Франції та Кіпру, Уряд стверджував, що повідомлення, відправлені працівником з використанням технічних засобів, які йому забезпечив роботодавець, необхідно було вважати професійними за характером, якщо працівник не визначив їх явно як приватні. Уряд зауважив, що за допомогою Yahoo Messenger було неможливо з технічної точки зору позначити повідомлення, як приватні; однак, заявник мав належну можливість вказати, що його повідомлення були приватними, на початковій стадії дисциплінарних проваджень, але наполягав на тому, що вони були пов’язані з роботою. Заявник був проінформований не тільки про внутрішні розпорядження роботодавця, які забороняли будь-яке особисте використання ресурсів компанії, але і про той факт, що його роботодавець розпочав процес моніторингу його повідомлень.

66. Уряд спирався на три подальші аргументи, стверджуючи, що стаття 8 Конвенції не була застосовною в даній справі. По-перше, не було доказів, які б свідчили, що розшифровка розмов заявника розкривалася його співробітникам; сам заявник надав повну розшифровку повідомлень у провадженнях у національних судах та не просив створити будь-які обмеження доступу до відповідних документів. По-друге, національні органи влади використали розшифровку повідомлень в якості доказів, оскільки заявник попросив про це, і оскільки органи прокуратури вже виявили, що моніторинг його спілкування був законним. По-третє, інформаційне повідомлення містило достатньо ознак для того, щоб заявник знав, що його роботодавець міг моніторити його повідомлення, і тому позбавляло їх приватного елементу.

(b) Заявник

67. Заявник не зробив жодних доводів щодо застосовності статті 8 Конвенції, але неодноразово наполягав на тому, що його спілкування носило приватний характер.

68. Він також стверджував, що оскільки він створив відповідний акаунт Yahoo Messenger і був єдиною особою, яка знала пароль, він мав обґрунтовані очікування приватності щодо своїх розмов. Заявник також стверджував, що не отримав попереднє повідомлення від роботодавця про моніторинг розмов.

2. Оцінка Суду

69. Суд зазначає, що питання, яке виникає в даній справі, полягає в тому, чи підпадають оскаржувані заявником питання під сферу дії статті 8 Конвенції.

70. На цій стадії свого розгляду Суд вважає корисним підкреслити, що «приватне життя» є широким терміном, який не підлягає вичерпному визначенню (див. *Sidabras and Džiautas v. Lithuania*, №№ 55480/00 та 59330/00, § 43, ECHR 2004‑VIII). Стаття 8 Конвенції захищає право на особистий розвиток (див. *K.A. and A.D. v. Belgium*, №№ 42758/98 та 45558/99, § 83, 17 лютого 2005), будь то у термінах особистості (див. *Christine Goodwin v. the United Kingdom* [GC], № 28957/95, § 90, ECHR 2002-VI) або особистої автономії, що є важливим принципом, який лежить в основі тлумачення гарантій статті 8 (див. *Pretty v. the United Kingdom*, № 2346/02, § 61, ECHR 2002-III). Суд визнає, що кожна особа має право на приватне життя, без непотрібної уваги до себе (див. *Smirnova v. Russia*,№№ 46133/99 та 48183/99, § 95, ECHR 2003‑IX (витяги)). Він також вважає зайвим обмеження поняття «приватного життя» «внутрішнім колом», в якому особа може вести особисте життя за своїм вибором, таким чином повністю виключаючи навколишній світ поза межами цього кола (див. *Niemietz v. Germany*, 16 грудня 1992, § 29, серія А № 251‑B). Таким чином, стаття 8 гарантує право на «приватне життя» у широкому сенсі, до якого входить право вести «приватне соціальне життя», тобто, можливість фізичної особи розвивати свою соціальну ідентичність. Стосовно цього відповідне право закріплює можливість підходу до інших осіб з метою встановлення та розвитку стосунків між ними (див. *Bigaeva v. Greece*, № 26713/05, § 22, 28 травня 2009, та *Özpınar v. Turkey*, № 20999/04, § 45 *in fine*, 19 жовтня 2010).

71. Суд робить висновок про те, що до поняття «приватне життя» може входити професійна діяльність (див. *Fernández Martínez* *v. Spain* [GC], № 56030/07, § 110, ECHR 2014 (витяги), та *Oleksandr Volkov v. Ukraine*, № 21722/11, §§ 165-66, ECHR 2013), або діяльність, яка відбувається у публічному контексті (див. Von Hannover v. Germany (№ 2) [GC], №№ 40660/08 та 60641/08, § 95, ECHR 2012). Обмеження професійного життя фізичної особи можуть охоплюватися статтею 8, якщо вони мають наслідки для способу, в який особа будує соціальну ідентичність шляхом розвитку стосунків з іншими людьми. Стосовно цього слід зауважити, що саме в ході робочого життя більшість осіб мають значну, якщо не найбільшу, можливість розвинути відносини із зовнішнім світом (див. *Niemietz*, цит. вище, § 29).

72. Крім того, стосовно поняття «кореспонденція», слід зазначити, що у формулюванні статті 8 це слово не супроводжується жодним прикметником, на відміну від терміна «життя». Дійсно, Суд вже постановляв, що у контексті кореспонденції шляхом телефонних дзвінків такі уточнення не робляться. У низці справ, які стосуються кореспонденції з адвокатом, навіть не передбачалася можливість того, що стаття 8 може бути незастосовною на підставі того, що кореспонденція мала професійний характер (див. *Niemietz*, цит. вище, § 32, з подальшими посиланнями). Крім того, Суд постановляв, що телефонні розмови охоплюються поняттями «приватне життя» та «кореспонденція» у розумінні статті 8 (див. *Roman Zakharov v. Russia* [GC], № 47143/06, § 173, ECHR 2015). У принципі, це також стосується випадків, коли телефонні дзвінки робляться або отримуються на території бізнесу (див. *Halford*, цит. вище, § 44, і *Amann v. Switzerland* [GC], № 27798/95, § 44, ECHR 2000‑II). Це також стосується електронних листів, надісланих з робочого місця, які користуються аналогічним захистом відповідно до статті 8, як і інформація, отримана за допомогою моніторингу користування інтернетом (див. *Copland*, цит. вище, § 41 у кінці).

73. З прецедентної практики Суду очевидно, що спілкування на території бізнесу, як і спілкування із дому, можуть охоплюватися поняттями «приватне життя» та «кореспонденція» у розумінні статті 8 Конвенції (see *Halford*, цит. вище, § 44; та *Copland*, цит. вище, § 41). Для того, щоб переконатися, чи застосовні поняття «приватне життя» і «кореспонденція», Суд декілька разів розглядав, чи мали особи обґрунтовані очікування того, що їх приватність буде дотримана та захищена (там само, і в тому, що стосується «приватного життя», див. також *Köpke v. Germany* (dec.), № 420/07, 5 жовтня 2010). У цьому контексті Суд заявляв, що обґрунтоване очікування приватності є значним, хоча і не обов’язково вирішальним чинником (див. *Köpke*, цит. вище).

74. Застосовуючи ці принципи у даній справі, Суд, у першу чергу, зауважує, що відповідний тип сервісу миттєвих інтернет-повідомлень є усього лише однією з форм зв’язку, які дозволяють фізичним особам вести приватне соціальне життя. У той же час, відправка та отримання повідомлень охоплюються поняттям «кореспонденція», навіть якщо вони надсилаються з комп’ютера працівника. Однак, Суд зазначає, що роботодавець заявника указав йому та іншим працівникам утримуватися від будь-якої особистої діяльності на робочому місці. Ця вимога з боку роботодавця відображалася у вигляді заходів, до яких входила заборона на використання ресурсів компанії для особистих цілей (див. пункт вище).

75. Суд також зазначає, що з метою забезпечення виконання цієї вимоги роботодавець встановив систему моніторингу користування інтернетом для працівників (див. пункти та вище). Документи у матеріалах справи, зокрема, ті, що стосуються дисциплінарних проваджень проти заявника, вказують на те, що упродовж моніторингу записувалися та зберігалися як направлення, так і зміст повідомлень заявника (див. пункти та вище).

76. Крім того, Суд зауважує, що незважаючи на цю вимогу роботодавця, заявник обмінювався повідомленнями особистого характеру з нареченою та братом (див. пункт вище). Деякі з цих повідомлень мали інтимний характер (там же).

77. Суд вважає, що з матеріалів справи очевидно, що заявник дійсно був проінформований про заборону користування інтернетом в особистих цілях, наведену у внутрішніх розпорядженнях роботодавця (див. пункт вище). Однак, не очевидно, що він був проінформований до початку моніторингу своїх повідомлень про те, що такий моніторинг матиме місце. Так, Уряд стверджував, що заявник ознайомився з інформаційним повідомленням роботодавця у невстановлений день з 3 до 13 липня 2007 року (див. пункт вище). Однак, національні суди не уточнили, чи був заявник проінформований про моніторинг до дати його початку, беручи до уваги, що заявник записував переговори у режимі реального часу з 5 до 13 липня 2007 року (див. пункт вище).

78. У будь-якому випадку, не видається, що заявник був проінформований заздалегідь про обсяг та характер моніторингової діяльності його роботодавця, або про можливість того, що його роботодавець міг мати доступ до змісту його повідомлень.

79. Суд також приймає до уваги аргумент заявника про те, що він сам створив відповідний акаунт Yahoo Messenger та був єдиною особою, яка знала пароль (див. пункт вище). Крім того, Суд зауважує, що матеріали справи вказують на те, що роботодавець також мав доступ до особистого акаунту заявника у Yahoo Messenger (див. пункт вище). У будь-якому випадку, заявник створив відповідний акаунт Yahoo Messenger за вказівками роботодавця для відповіді на запити клієнтів (див. пункт вище), і роботодавець мав доступ до нього.

80. Залишається питання про те, чи залишили розпорядження роботодавця заявника з обґрунтованим очікуванням приватності, і якщо так – в якій мірі. У будь-якому випадку, вказівки роботодавця не можуть звести приватне соціальне життя на робочому місці до нуля. Повага до приватного життя та приватності кореспонденції продовжує існувати, навіть якщо можуть існувати необхідні обмеження.

81. У світлі усіх наведених вище міркувань Суд робить висновок про те, що спілкування заявника на робочому місці охоплювалося концепціями «приватне життя» та «кореспонденція». Відповідно, за обставин даної справи, стаття 8 Конвенції є застосовною.

D. Дотримання статті 8 Конвенції

1. Доводи сторін та зауваження третьої сторони

(a) Заявник

82. У своїх письмових зауваженнях у Великій Палаті заявник стверджував, що Палата не звернула достатню увагу на певні фактичні аспекти справи. По-перше, він підкреслив конкретні особливості Yahoo Messenger, який був призначений для особистого використання. Рішення його роботодавця щодо використання цього інструменту у робочому контексті не міняє той факт, що він у першу чергу призначався для особистих цілей. Тому заявник вважав себе єдиним власником акаунту Yahoo Messenger, який він завів за запитом роботодавця.

83. По-друге, заявник стверджував, що його роботодавець не ввів жодну політику користування інтернетом. Він не отримав жодного попередження про можливість того, що його повідомлення можуть моніторитися або бути прочитаними; він також не давав згоди у цьому відношенні. Якщо б така політика існувала і він був проінформований про неї, він би утримався від розкриття певних аспектів свого приватного життя в Yahoo Messenger.

84. По-третє, заявник стверджував, що слід проводити різницю між користуванням інтернетом в особистих цілях з метою отримання прибутку і «невеликою нешкідливою приватною розмовою», метою якої не було отримання прибутку і яка не заподіяла шкоди роботодавцю; у зв’язку з цим заявник зазначив, що протягом дисциплінарних проваджень проти нього роботодавець не обвинувачував його у завданні шкоди компанії. Заявник підкреслив розвиток інформаційних та комунікаційних технологій, а також соціальних звичок та звичаїв, пов’язаних з їх використанням. Він стверджував, що сучасні робочі умови роблять неможливим проведення чіткої розмежувальної лінії між приватним та професійним життям, і поставив під сумнів законність будь-якої політики керівництва, яка б забороняла користування інтернетом та будь-якими приладами в особистих цілях.

85. З юридичної точки зору заявник стверджував, що держава Румунія не виконала своє позитивне зобов’язання за статтею 8 Конвенції. Більш конкретно, національні суди не скасували його звільнення, хоча й визнали, що мало місце порушення його права на повагу до приватного спілкування.

86. По-перше, заявник стверджував, що Палата неправильно відрізнила дану справу від справи *Copland* (цит. вище, § 42). На його думку, рішучим чинником при аналізі справи було не те, чи дозволяв роботодавець користування інтернетом в особистих цілях, а той факт, що роботодавець не попередив працівника про те, що його розмови можуть підлягати моніторингу. У цьому зв’язку заявник стверджував, що його роботодавець спочатку помістив його під спостереження, і лише після цього дав йому можливість вказати, чи були його розмови приватними або пов’язаними з роботою. Суд повинен був розглянути, чи давала заборона на користування інтернетом в особистих цілях роботодавцю право моніторити працівників, і чи повинен був роботодавець надавати підстави для такого моніторингу.

87. По-друге, заявник стверджував, що аналіз Палати стосовно другого пункту статті 8 не відповідав прецедентній практиці Суду у тому, що він не прагнув переконатися в тому, чи відповідало закону втручання у право заявника на повагу до його приватного життя та кореспонденції, чи переслідувало воно законну мету і чи було необхідним у демократичному суспільстві.

88. Що стосується юрисдикції трудових судів, заявник стверджував, що вони мали компетенцію для проведення повного огляду законності та обґрунтування заходу, про який їм повідомляли. Суди повинні були запитати надання необхідних доказів та висунути будь-які відповідні фактичні або юридичні питання, навіть якщо вони не були згадані сторонами. Відповідно, трудові суди мали широку юрисдикцію для розгляду будь-яких питань, які стосувалися спорів щодо трудового законодавства, у тому числі спорів щодо поваги до приватного життя та кореспонденції працівників.

89. Однак, у справі заявника національні суди скористувалися жорстким підходом, спрямованим лише на ухвалення рішення роботодавця. Вони здійснили неправильний аналіз фактичних аспектів справи і не взяли до уваги конкретні особливості спілкування у кіберпросторі. Тому порушення права заявника на повагу до його приватного життя та кореспонденції було умисним та незаконним, його метою було зібрання даних, які б дозволили розірвати його контракт.

90. Нарешті, заявник скаржився уперше у провадженнях у Великій Палаті на результат скарги у кримінальному порядку, яку подав у 2007 році: у 2012 році відділення прокуратури, яке відповідало за розслідування організованої злочинності та тероризму (УРОЗТ) відхилило його скаргу, не встановивши належним чином факти справи.

91. На слуханні у Великій Палаті заявник стверджував, у відповідь на питання суддів, що через те, що його роботодавець зробив лише один принтер доступним для працівників, усі його колеги могли бачити зміст сорока п’яти сторінок розшифровки його переговорів за допомогою Yahoo Messenger.

92. Заявник закликав Велику Палату виявити порушення статті 8 Конвенції та скористатися можливістю підтвердити, що моніторинг кореспонденції працівників міг здійснюватися лише у відповідності з застосовним законодавством, у транспарентний манер та на підставах, передбачених законодавством, і що роботодавці не мали свободи розсуду для моніторингу кореспонденції працівників.

(b) Уряд

93. Уряд стверджував, що роботодавець записав розмови працівника з 5 до 13 липня 2007 року та дав йому можливість звітувати про користування інтернетом, яке було значнішим, ніж у його співробітників. Уряд зауважив, що оскільки заявник наполягав на тому, що зміст його повідомлень відносився лише до роботи, роботодавець розслідував його пояснення.

94. Уряд стверджував, що у своїй апеляції проти рішення суду першої інстанції заявник не опротестував висновок суду про те, що він був проінформований про здійснення роботодавцем моніторингу користування інтернетом. У цьому зв’язку Уряд надав копію інформаційного повідомлення, виданого роботодавцем та підписаного заявником. На підставі реєстру відвідування роботодавця Уряд зауважив, що заявник підписав повідомлення у період з 3 до 13 липня 2007 року.

95. Уряд також стверджував, що роботодавець записував розмови заявника у режимі реального часу. Не було доказів того, що роботодавець мав доступ до попередніх розмов заявника або його приватної електронної пошти.

96. Уряд указав на свою згоду з висновками Палати та стверджував, що Румунська держава виконала своє позитивне зобов’язання відповідно до статті 8 Конвенції.

97. По-перше, Уряд зауважив, що заявник вирішив звернутися зі своїми скаргами до національних судів у контексті спора про трудове законодавство. Суди розглянули всі його скарги та зважили усі зацікавлені інтереси, але центр їх аналізу полягав у тому, чи відповідали дисциплінарні провадження проти заявника національному законодавству. Заявник мав можливість висунути в національних судах свою конкретну скаргу на порушення його права на повагу до приватного життя, наприклад, шляхом дії відповідно до Закону № 677/2001 або деліктного позову, але він обрав не робити це. Він також подав скаргу у кримінальному порядку, яка призвела до рішення прокуратури про відмову в подальших діях, на підставі того, що моніторинг розмов заявника з боку роботодавця не був незаконним.

98. Посилаючись більш конкретно на позитивні зобов’язання держави, Уряд стверджував, що підходи держав-членів Ради Європи значно відрізнялися один від одного в тому, що стосується регулювання моніторингу роботодавцями працівників. Деякі держави включили це питання у більш широкий обсяг опрацювання персональних даних, у той час як інші прийняли конкретне законодавство у цій галузі. Навіть серед другої групи держав не існує єдиного рішення щодо обсягу та цілі моніторингу, який здійснює роботодавець, попереднього повідомлення працівників або використання інтернету в особистих цілях.

99. Спираючись на справу *Köpke* (цит. вище), Уряд наполягав, що національні суди досягли належного балансу між правом заявника на повагу до приватного життя і кореспонденції та правом його роботодавця організовувати та контролювати роботу в компанії. На думку Уряду, коли розмови контролюються приватною організацією, належного розгляду з боку національних судів достатньо для цілей статті 8, і не було необхідності у конкретному захисті засобами законодавчої системи.

100. Уряд також стверджував, що національні суди розглянули питання законності та необхідності рішення роботодавця та досягли висновку про те, що дисциплінарні провадження були проведені у відповідності до чинного законодавства. Уряд надав особливу важливість характеру проведення проваджень, особливо можливості заявника вказати, чи були відповідні розмови приватними. Якщо б заявник скористувався цією можливістю, національні суди зважили б зацікавлені інтереси іншим чином.

101. У зв’язку з цим Уряд зазначив, що у провадженнях у національних органах влади сам заявник надав повну розшифровку свого спілкування, без вжиття будь-яких запобіжних заходів; замість цього він міг розкрити лише імена відповідних акаунтів або надати витяги зі своїх розмов, наприклад, тих, які не містили інтимної інформації. Уряд також опротестував твердження заявника про те, що його розмови були розкриті колегам, що лише дисциплінарна комісія з трьох учасників мала доступ до них.

102. Уряд також стверджував, що рішення роботодавця було необхідним, оскільки він повинен був розслідувати аргументи, висунуті заявником у дисциплінарних провадженнях, для визначення того, чи дотримувався заявник внутрішніх розпоряджень.

103. Нарешті, Уряд стверджував, що необхідно провести розрізнення між характером повідомлень та їх змістом. Уряд зауважив, як і Палата, що національні суди взагалі не взяли зміст розмов заявника до уваги, а лише розглянули їх характер та визнали, що вони були особистими.

104. Тому Уряд дійшов висновку про те, що скарга заявника відповідно до статті 8 Конвенції була необґрунтованою.

(c) Треті сторони

(i) Уряд Франції

105. Уряд Франції посилався, зокрема, на свою концепцію обсягу позитивних зобов’язань національної влади щодо забезпечення поваги до приватного життя працівників та їх кореспонденції. Уряд Франції надав всеосяжний огляд застосовних положень французького цивільного права, трудового права та кримінального права у цій сфері. На його думку, стаття 8 Конвенції була застосовною лише до суто персональних даних, кореспонденції та електронної діяльності. У зв’язку з цим уряд Франції посилався на прецедентну практику Французького касаційного суду щодо того, що будь-які опрацьовані дані, надіслані та отримані за допомогою електронного обладнання роботодавця, вважалися професійними за характером, якщо працівник чітко та точно не позначив їх, як приватні.

106. Уряд Франції стверджував, що держави мали користуватися більш широкою свободою розсуду в цій галузі, оскільки мета полягала в досягненні балансу між конкуруючими особистими інтересами. Роботодавець міг моніторити професійні дані та кореспонденцію працівників у розумній мірі, за умови переслідування законної цілі, і міг використовувати результати моніторингу у дисциплінарних провадженнях. Уряд Франції підкреслив, що працівників необхідно було попереджати заздалегідь про такий моніторинг. Крім того, коли були задіяні дані, чітко означені працівником, як приватні, роботодавець міг попросити суди наказати провести слідчі заходи та вказати приставу отримати доступ до відповідних даних та записати їх зміст.

(ii) Європейська конфедерація профспілок

107. Європейська конфедерація профспілок стверджувала, що було необхідно захистити приватність у робочому середовищі, беручи до уваги, зокрема, той факт, що працівники структурно залежали від роботодавців у цьому контексті. Після узагальнення застосовних принципів міжнародного та європейського права вона стверджувала, що доступ до інтернету повинен вважатися правом людини, і що право на повагу до кореспонденції необхідно посилити. Згода, або, щонайменше, попереднє повідомлення, працівників є необхідним, і представників персоналу необхідно інформувати до того, як роботодавець зможе опрацювати особисті дані працівників.

2. Оцінка Суду

(a) Чи стосується справа негативного або позитивного зобов’язання

108. Суд повинен визначити, чи слід розглядати дану справу у термінах негативного або позитивного зобов’язання держави. Він повторює, що в силу статті 1 Конвенції Договірні Сторони «повинні забезпечити кожному в межах їх юрисдикції права та свободи, визначені у ... [цій] Конвенції». У той час як ключова ціль статті 8 полягає в захисті фізичних осіб від довільного втручання з боку державних органів влади, вона також може накладати на державу певні позитивні зобов’язання щодо забезпечення ефективної поваги до прав, захищених статтею 8 (див., серед інших, *X and Y v. the Netherlands*, 26 березня 1985 року, § 23, серія A № 91; *Von Hannover (№ 2)*, цит. вище, § 98;та *Hämäläinen v. Finland* [GC], № 37359/09, § 62, ECHR 2014).

109. У даній справі Суд зауважує, що оскаржуваний заявником захід, а саме, моніторинг спілкування з використанням Yahoo Messenger, який призвів до дисциплінарних проваджень проти заявника та його звільнення за порушення внутрішніх розпоряджень роботодавця, які забороняли використання ресурсів компанії в особистих цілях, був вжитий не державним органом, а приватною комерційною компанією. Тому моніторинг розмов заявника та перевірка роботодавцем їх змісту для виправдання його звільнення не може вважатися «втручанням» у його право з боку державного органу влади.

110. Однак, Суд зазначає, що вжитий роботодавцем захід був прийнятий національними судами. Дійсно, моніторинг розмов заявника не був результатом прямого втручання національних органів влади; однак, їх відповідальність була б задіяна, якщо б оскаржувані факти випливали з їх нездатності забезпечити заявникові користування правом, закріпленим у статті 8 Конвенції (див., з необхідними змінами, *Obst v. Germany*,№ 425/03, §§ 40 та 43, 23 вересня 2010, і *Schüth v. Germany*, № 1620/03, §§ 54 та 57, ECHR 2010).

111. У світлі конкретних обставин справи, описаних у пункті вище, Суд вважає, беручи до уваги свої висновки щодо застосовності статті 8 Конвенції (див. пункт вище) та той факт, що користування заявником його правом на повагу до недоторканності приватного життя та кореспонденції було ускладнено діями приватного роботодавця, що скаргу необхідно розглянути з точки зору позитивних зобов’язань держави.

112. Хоча межі між позитивними та негативними зобов’язаннями держави відповідно до Конвенції не підлягають точному визначенню, застосовні принципи однакові. В обох контекстах слід особливо взяти до уваги справедливий баланс між інтересами фізичної особи та спільноти в цілому, що в будь-якому випадку підлягає свободі розсуду держави (див. *Palomo Sánchez and Others v. Spain* [GC], №№ 28955/06 та 3 інших, § 62, ECHR 2011).

(b) Загальні принципи, застосовні до оцінки позитивного зобов’язання держави щодо забезпечення поваги до приватного життя та кореспонденції в контексті працевлаштування

113. Суд повторює, що вибір засобів, розрахованих для забезпечення дотримання статті 8 Конвенції у сфері відносин фізичних осіб між собою є, у принципі, питанням, яке потрапляє до свободи розсуду Договірних Держав. Існують багато шляхів забезпечення поваги до приватного життя, і характер зобов’язання держави залежатиме від конкретних аспектів приватного життя, про які йдеться мова (див. *Söderman v. Sweden* [GC], № 5786/08, § 79, ECHR 2013, з подальшими посиланнями).

114. Тому задача Суду у даній справі полягає у проясненні характеру та обсягу позитивних зобов’язань, які держава-відповідач повинна була виконати при захисті права заявника на повагу до його приватного життя та кореспонденції у контексті працевлаштування.

115. Суд зауважує, що він вже постановляв, що за певних обставин позитивні зобов’язання держави відповідно до статті 8 Конвенції не виконуються належним чином, якщо вона не забезпечує повагу до приватного життя у відносинах між фізичними особами шляхом створення законодавчої системи, яка приймає до уваги різні інтереси, які необхідно захищати у конкретному контексті (див. *X and Y v. the Netherlands*, цит. вище, §§ 23, 24 та 27, і *M.C. v. Bulgaria*,№39272/98, § 150, ECHR 2003‑XII, стосовно сексуальних нападів на неповнолітніх; див. також *K.U. v. Finland*, № 2872/02, §§ 43 та 49, ECHR 2008, стосовно реклами сексуального характеру, поміщеній на сайті для побачень від імені неповнолітнього; *Söderman*, цит. вище, § 85, стосовно ефективності засобів правового захисту стосовно стверджуваного порушення особистої недоторканності, скоєного близьким родичем; і *Codarcea v. Romania*, № 31675/04, §§ 102-04, 2 червня 2009 року, стосовно медичної недбалості).

116. Суд визнає, що захисні заходи можна знайти не тільки у трудовому законодавстві, але й у цивільному та кримінальному праві. У тому, що стосується трудового законодавства, він повинен переконатися, чи повинна була держава-відповідач у даній справі створити законодавчу систему для захисту права заявника на повагу до приватного життя та кореспонденцію у контексті професійних відносин з приватним роботодавцем.

117. У зв’язку з цим Суд вважає з самого початку, що трудове законодавство має конкретні особливості, які необхідно взяти до уваги. Відносини роботодавця та працівника є договірними, з конкретними правами та обов’язками з обох сторін, і характеризуються юридичною субординацією. Вони регулюються власними юридичними правилами, які значно відрізняються від правил, застосовних в цілому до відносин між особами(див. *Saumier v. France*, № 74734/14, § 60, 12 січня 2017).

118. З нормативної перспективи, трудове законодавство залишає місце для переговорів між сторонами трудового контракту. Тому зазвичай самі сторони регулюють значну частину змісту своїх відносин (див., з необхідними змінами, *Wretlund v. Sweden* (dec.), № 46210/99, 9 березня 2004 року, стосовно відповідності до статті 8 Конвенції зобов’язання заявника, працівника на атомній електростанції, проходити перевірку на наркотики; беручи до уваги профспілкове звернення з точки зору статті 11, див. *Gustafsson v. Sweden*, 25 квітня 1996 року, § 45, *Reports* 1996‑II, та, з необхідними змінами, *Demir and Baykara v. Turkey* [GC], № 34503/97, §§ 140‑46, ECHR 2008, для конкретного випадку громадських службовців). Також з матеріалів порівняльного права у розпорядженні Суду видається, що не існує європейського консенсусу з цього питання. Декілька держав-членів чітко врегулювали питання користування працівниками їх правом на повагу до приватного життя та кореспонденції на робочому місці (див. пункт вище).

119. У світлі наведених вище міркувань Суд вважає, що Договірні Держави повинні мати широку свободу розсуду при оцінці необхідності встановлення юридичної системи, яка регулює умови, за яких роботодавець може регулювати електронне або інше спілкування непрофесійного характеру, яке працівники здійснюють на робочому місці.

120. Однак, свобода розсуду, якою користуються держави стосовно цього, не може бути необмеженою. Національні органи влади повинні забезпечити, щоб введення роботодавцем заходів моніторингу кореспонденції та інших комунікацій, незалежно від обсягу та тривалості таких заходів, супроводжувалося належними та достатніми гарантіями проти зловживання (див., з необхідними змінами, *Klass and Others v. Germany*, 6 вересня 1978 року, § 50, серія A № 28, та *Roman Zakharov*, цит. вище, §§ 232-34).

121. Суд знає про швидкий розвиток цієї галузі. Однак, він вважає, що пропорційність та процесуальні гарантії проти свавілля є ключовими. У цьому контексті національні органи влади повинні розглядати як важливі наступні чинники:

(*i*) чи було повідомлено працівнику про можливість того, що роботодавець може вжити заходи для моніторингу кореспонденції та інших комунікацій, і про втілення таких заходів. Хоча на практиці працівники можуть бути проінформовані різними шляхами в залежності від конкретних фактичних обставин кожної справи, Суд вважає, що для того, щоб заходи вважалися тими, що відповідають вимогам статті 8 Конвенції, повідомлення повинно бути чітким щодо характеру моніторингу та повинно надаватися заздалегідь;

(*ii*) обсяг моніторингу з боку роботодавця та ступінь втручання у приватність працівника. У цьому відношенні слід розрізняти моніторинг потоку повідомлень та їх змісту. Слід також взяти до уваги те, чи усі повідомлення підлягали моніторингу, або лише їх частина, як і питання того, чи обмежувався моніторинг часом та кількістю осіб, які мали доступ до результату (див. *Köpke*, цит. вище). Це також стосується обмежень у просторі моніторингу;

(*iii*) чи надав роботодавець законні підстави для виправдання моніторингу повідомлень та доступу до їх фактичного контексту (див. пункти , та вище для перегляду міжнародного та європейського права з цього питання). Оскільки моніторинг змісту повідомлень є за своїм характером більш агресивним методом, він потребує більш значного виправдання;

(*iv*) чи було можливо встановити систему моніторингу на основі менш агресивних методів та засобів, ніж прямий доступ до змісту повідомлень працівника. У цьому зв’язку повинна мати місце оцінка того, чи могла мета, яку переслідував роботодавець, бути досягнута без прямого доступу до повного змісту повідомлень працівника, у світлі конкретних обставин кожної справи;

(*v*) наслідки моніторингу для працівника, який йому підлягає (див., з необхідними змінами, аналогічний критерій, який застосовується до оцінки пропорційності втручання у користування свободою вираження поглядів, захищену статтею 10 Конвенції, у справі Axel Springer AG v. Germany [GC], № 39954/08, § 95, 7 лютого 2012 року, з подальшими посиланнями), і те, як роботодавець використовує результати моніторингу, зокрема, чи були результати використані для досягнення заявленої мети заходу (див. *Köpke*, цит. вище);

(*vi*) чи надавалися працівнику належні гарантії, особливо коли моніторинг, здійснюваний роботодавцем, носив агресивний характер. Такі гарантії повинні забезпечити, зокрема, щоб роботодавець не міг отримати доступ до фактичного змісту відповідних повідомлень, якщо працівник не міг бути проінформований заздалегідь про таку можливість.

У цьому контексті слід повторити, що для того, щоб бути плодотворними, робочі відносини повинні ґрунтуватися на взаємній довірі (див. *Palomo Sánchez and Others*, цит. вище, § 76).

122. Нарешті, національні органи влади повинні забезпечити, щоб працівник, спілкування якого підлягало моніторингу, мав доступ до засобу правового захисту в органі судової влади, який має юрисдикцію щодо визначення, хоча б по суті, того, як наведені вище критерії були дотримані, та чи були оскаржувані заходи законними (див. *Obst*, цит. вище, § 45, та *Köpke*, цит. вище).

123. У даній справі Суд розгляне, як національні суди, до яких звертався заявник, розглянули його скаргу на порушення роботодавцем його права на повагу до приватного життя та кореспонденції у контексті працевлаштування.

(c) Застосування наведених вище загальних принципів у даній справі

124. Суд зауважує, що національні суди постановили, що інтересами на кону в даній справі були, з одного боку, право заявника на повагу до приватного життя, і, з іншого боку, право роботодавця здійснювати моніторинг, і в тому числі – відповідні дисциплінарні повноваження, для забезпечення безперебійного функціонування компанії (див. пункти та вище). Він вважає, що в силу позитивних зобов’язань держави відповідно до статті 8 Конвенції, національні органи влади повинні були урівноважити ці інтереси.

125. Суд зауважує, що точною темою поданої до нього скарги є стверджувана нездатність національних судів, у контексті спору щодо трудового права, захистити право заявника, відповідно до статті 8 Конвенції, на повагу до його приватного життя та кореспонденції у контексті працевлаштування. Упродовж проваджень заявник скаржився, зокрема, у національних судах та в Суді, на те, що роботодавець здійснював моніторинг його спілкування за допомогою відповідних акаунтів Yahoo Messenger та використав зміст спілкування у подальших дисциплінарних провадженнях проти заявника.

126. Щодо того, чи розкрив роботодавець зміст спілкування співробітникам заявника (див. пункт вище), Суд зауважує, що цей аргумент недостатньо підтверджується матеріалами справи, і що заявник не надав ніяких подальших доказів на слуханні у Великій Палаті (див. пункт вище).

127. Тому Суд вважає, що скарга стосується звільнення заявника на основі моніторингу, який здійснював його роботодавець. Більш конкретно, він повинен уточнити в даній справі, чи здійснювали національні органи влади урівноваження, відповідно до вимог статті 8 Конвенції, між правом заявника на повагу до приватного життя і кореспонденції та інтересами роботодавця. Тому його задача полягає у визначенні того, чи досягли компетентні національні органи влади, у світлі усіх обставин справи, справедливого балансу між конкуруючими інтересами при прийнятті моніторингових заходів, яким підлягав заявник (див., з необхідними змінами, *Palomo Sánchez and Others*, цит. вище, § 62). Він визнає, що роботодавець мав законний інтерес у забезпеченні безперебійного функціонування компанії, і що цього можна було досягти шляхом встановлення механізмів для перевірки того, чи виконують працівники свої професійні обов’язки належно та з необхідною ретельністю.

128. У світлі наведених вище міркувань Суд спочатку розгляне спосіб, в який національні суди встановили відповідні факти у даній справі. Як окружний суд, так і апеляційний суд постановили, що заявник отримав попереднє повідомлення від роботодавця (див. пункти та вище). Тому Суд повинен переконатися, чи дотримали національні суди вимоги Конвенції при розгляді справи.

129. На цій стадії Суд вважає корисним повторити, що коли справа стосується встановлення фактів, він пам’ятає про субсидіарний характер своєї задачі, і повинен бути обережним при виконанні ролі суду факту першої інстанції, якщо це не роблять неминучим обставини конкретної справи (див. *Mustafa Tunç and Fecire Tunç v. Turkey* [GC], № 24014/05, § 182, 14 квітня 2015 року). Якщо національні провадження вже відбулися, задача Суду не полягає в заміні оцінки фактів, зробленої національними судами, власною оцінкою, і саме національні суди повинні встановити факти на основі доказів, які є в їх розпорядженні (див., серед інших, *Edwards v. the United Kingdom*, 16 грудня 1992, § 34, серія А № 247‑B). Хоча Суд не зв’язаний висновками національних судів та має право робити власну оцінку у світлі усіх матеріалів у своєму розпорядженні, за нормальних обставин він потребує переконливі елементи для того, щоб відхилитися від фактичних висновків, досягнутих національними судами (див. *Giuliani and Gaggio v. Italy* [GC], № 23458/02, § 180, ECHR 2011 (витяги), і *Aydan v. Turkey*, № 16281/10, § 69, 12 березня 2013).

130. Надані до Суду докази вказують на те, що заявник був проінформований про внутрішні розпорядження роботодавця, які забороняли користування ресурсами компанії в особистих цілях (див. пункт  вище). Він визнав зміст відповідного документу та підписав його копію 20 грудня 2006 року (див. пункт вище). Крім того, роботодавець надіслав усім працівникам інформаційне повідомлення, датоване 26 червня 2007 року, в якому їм нагадувалося, що використання ресурсів компанії в особистих цілях заборонялося, і пояснялося, що працівник був звільнений за порушення цього правила (див. пункт вище). Заявник ознайомився з повідомленням та підписав його копію у невстановлений день з 3 до 13 липня 2007 року (див. пункт вище). Нарешті, Суд зазначає, що 13 липня 2007 року заявник був двічі викликаний роботодавцем для надання пояснень щодо користування інтернетом в особистих цілях (див. пункти та вище). Спочатку, після демонстрації діаграм, які демонстрували його діяльність в інтернеті та діяльність його колег, заявник стверджував, що користувався акаунтом Yahoo Messenger лише у робочих цілях (див. пункти та вище). У подальшому, через сорок п’ять хвилин, після отримання сорока п’яти листів розшифровки свого спілкування з братом та нареченою, заявник проінформував роботодавця про те, що, на його думку, роботодавець скоїв кримінальне правопорушення, а саме – порушив таємницю кореспонденції (див. пункт вище).

131. Суд зазначає, що національні суди правильно визначили інтереси, які необхідно врівноважити – шляхом прямого посилання на право заявника на повагу до приватного життя – і застосовні правові принципи (див. пункти  та вище). Зокрема, апеляційний суд зробив чітке посилання на принципи необхідності, уточнення цілі, транспарентності, законності, пропорційності та безпеки, встановлені у Директиві 95/46/EC, і зауважив, що моніторинг користування інтернетом та електронними засобами зв’язку на робочому місці регулювався цими принципами (див. пункт вище). Національні суди також розглянули, чи проводилися дисциплінарні провадження у змагальному порядку та чи отримав заявник можливість висунути свої аргументи.

132. Залишається визначити, як національні органи влади взяли до уваги наведені вище критерії (див. пункт ) у своєму обґрунтуванні при урівноваженні права заявника на повагу до приватного життя і кореспонденції проти права роботодавця на здійснення моніторингу, у тому числі відповідних дисциплінарних повноважень, для забезпечення безперебійного функціонування компанії.

133. Що стосується того, чи отримав заявник попереднє повідомлення від роботодавця, Суд зауважує, що вже дійшов висновку про те, що заявник не був проінформований заздалегідь про ступінь та характер моніторингу, який здійснював роботодавець, або про можливість того, що роботодавець міг мати доступ до фактичного змісту його повідомлень (див. пункт  вище). Стосовно можливості моніторингу Суд зазначає, що окружний суд зауважив, що «увага працівників була звернута на той факт, що незадовго до дисциплінарної санкції заявника інший працівник був звільнений» (див. пункт вище), і що апеляційний суд виявив, що заявник був попереджений про те, що йому не слід користуватися ресурсами компанії в особистих цілях (див. пункт вище). Відповідно, національні суди не визначили, чи було заявникові повідомлено заздалегідь про можливість того, що роботодавець міг розпочати моніторинг, а також про обсяг та характер такого заходу. Суд вважає, що для того, щоб розцінювати попередження від роботодавця, як попереднє повідомлення, воно повинно надаватися до початку моніторингу, особливо якщо моніторинг призведе до доступу до змісту повідомлень працівників. Міжнародні та європейські стандарти вказують у цьому напрямку та потребують, щоб суб’єкт даних був проінформований до проведення будь-якого моніторингу (див. пункти та  вище; див. також, з перспективи порівняльного права, пункт вище).

134. Що стосується обсягу моніторингу та рівня втручання у приватність заявника, Суд зауважує, що це питання не розглянули ані окружний суд, ані апеляційний суд (див. пункти та вище), незважаючи на те, що видається, що роботодавець записував усе спілкування заявника упродовж періоду моніторингу у режимі реального часу, мав доступ до розмов та друкував їх зміст (див. пункти та вище).

135. Також не видається, що національні суди здійснили достатню оцінку того, чи існували законні підстави для виправдання моніторингу розмов заявника. Суд змушений зауважити, що апеляційний суд не визначив, яка конкретна мета у даній справі могла виправдати такий суворий моніторинг. Щоправда, цього питання торкнувся окружний суд, який згадав потребу уникнути завдання шкоди IT-системам компанії, відповідальності, яку компанія понесе у випадку незаконної діяльності у кіберпросторі, та розкриття комерційних таємниць компанії (див. пункт вище). Однак, на думку Суду, ці приклади можна розглядати лише в якості теоретичних, оскільки ніщо не вказувало на те, що заявник дійсно піддав компанію будь-якому з цих ризиків. Крім того, апеляційний суд взагалі не розглянув це питання.

136. На додаток до цього, ані окружний суд, ані апеляційний суд не розглянули в достатній мірі те, чи можна було досягти переслідуваної роботодавцем мети за допомогою методів менш агресивних, ніж доступ до фактичного змісту спілкування заявника.

137. Крім того, жодний суд не розглянув тяжкість наслідків моніторингу та подальших дисциплінарних проваджень. Стосовно цього Суд зазначає, що заявник отримав найвищу дисциплінарну санкцію, а саме - звільнення.

138. Нарешті, Суд зауважує, що національні суди не визначили, чи дійсно роботодавець вже отримав доступ до змісту розмов на момент, коли він викликав заявника для надання пояснень його користування ресурсами компанії, зокрема, інтернетом (див. пункти та вище). Суд зазначає, що національні органи влади не встановили, на якій стадії дисциплінарних проваджень роботодавець отримав доступ до змісту розмов. На думку Суду, визнання того, що доступ до змісту розмов міг існувати на будь-якій стадії дисциплінарних проваджень, суперечить принципу транспарентності (див. у цьому відношенні Рекомендацію CM/Rec(2015)5, цит. у пункті вище; для перспективи порівняльного права див. пункт вище).

139. Беручи до уваги поточні міркування, Суд вважає, що висновок апеляційного суду про те, що був досягнутий справедливий баланс між існуючими інтересами (див. пункт вище) є сумнівним. Таке твердження виявляється формалістичним та теоретичним. Апеляційний суд не пояснив конкретні підстави, пов’язані з конкретними обставинами заявника та його роботодавця, які призвели до досягнення такого висновку.

140. При цьому видається, що національні суди не визначили, зокрема, чи отримав заявник попереднє повідомлення від роботодавця про можливість того, що його повідомлення, відправлені через Yahoo Messenger, можуть підлягати моніторингу; вони також не прийняли до уваги той факт, що він не був проінформований про характер та обсяг моніторингу, або про рівень втручання у приватне життя та кореспонденцію. Крім того, суди не визначили, по-перше, конкретні підстави, які б виправдовували введення моніторингу; по-друге, чи міг роботодавець скористуватися заходами, пов’язаними з меншим рівнем втручання у приватне життя та кореспонденцію заявника; і по-третє, чи можна було отримати доступ до розмов без його відома (див. пункти та вище).

141. Беручи до уваги усі наведені вище міркування, і незважаючи на свободу розсуду держави-відповідача, Суд вважає, що державні органи влади не забезпечили належний захист права заявника на повагу до приватного життя та кореспонденції, і що вони не досягли справедливого балансу між існуючими інтересами. Відповідно, мало місце порушення статті 8 Конвенції.

II. ЗАСТОСУВАННЯ СТАТТІ 41 КОНВЕНЦІЇ

142. 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. Відшкодування шкоди

1. Матеріальна шкода

143. У Палаті заявник вимагав сплатити йому 59,976.12 євро (EUR) в якості відшкодування матеріальної шкоди, яку він, нібито, поніс. Він представляв, що ця сума представляла його поточну заробітну плату, на яку він мав би право, якщо б не був звільнений. На слуханні у Великій Палаті представники заявника стверджували, що наполягали на вимозі справедливої сатисфакції.

144. У своїх зауваженнях у Палаті Уряд стверджував, що був проти присудження будь-якої суми в якості відшкодування матеріальної шкоди, яку заявник, нібито, поніс. На думку Уряду, ця сума ґрунтувалася лише на припущенні, і між звільненням заявника та сумою, яку він вимагав, не було зв’язку.

145. Суд зауважує, що він виявив порушення статті 8 Конвенції в тому, що національні суди не встановили відповідні факти та не провели належний баланс між правом заявника на повагу до приватного життя і кореспонденції та інтересами роботодавця. Він не вбачає ніякого причинно-наслідкового зв’язку між виявленими порушеннями та заявленою матеріальною шкодою, і тому відхиляє цю вимогу.

2. Моральна шкода

146. У Палаті заявник також вимагав сплатити йому 200,000 євро в якості відшкодування моральної шкоди, яку він, нібито, поніс у результаті звільнення. Заявник стверджував, що через дисциплінарний характер звільнення він не міг знайти іншу роботу, його житловий стандарт значно погіршився, він втратив соціальний статус і в результаті цього його наречена вирішила у 2010 році закінчити їх стосунки.

147. Уряд зазначив у відповідь, що визнання порушення могло, у принципі, бути достатньою справедливою сатисфакцією. У будь-якому випадку Уряд стверджував, що сума, яку назвав заявник, була надмірною у світлі прецедентної практики Суду у цьому відношенні.

148. Суд вважає, що визнання порушення становить достатню справедливу сатисфакцію будь-якої моральної шкоди, яка могла бути понесена заявником.

B. Компенсація судових витрат

149. У Палаті заявник також вимагав сплатити йому 3,310 румунських лей (RON) (приблизно 750 євро) в якості відшкодування судових витрат, понесених у національних судах, та 500 лей (приблизно 115 євро) в якості гонорару адвокату, який представляв його у національних провадженнях. Заявник також вимагав сплатити йому 500 євро в якості гонорарів адвокатів, які представляли його у Суді. Він надав наступні документи у підтримку своєї вимоги:

- копії договору про надання юридичної допомоги та квитанції про сплату суми у 500 лей, стосовно гонорару адвокату в національних провадженнях;

- документи, які доводили, що він сплатив роботодавцеві суми в розмірі 2,700 лей та 610.30 лей у якості відшкодування судових витрат;

- копію квитанції на сплату суми в розмірі 2,218.64 лей, яка відповідала гонорару одного з адвокатів, які представляли заявника у Суді.

Заявник не прагнув відшкодування витрат, понесених у зв’язку з провадженнями у Великій Палаті.

150. У своїх зауваженнях у Палаті Уряд попросив Суд присудити заявникові лише ті суми, які були необхідними та відповідали обґрунтованим вимогам. У цьому зв’язку Уряд стверджував, що заявник не довів, що сплатив 500 євро в якості гонорарів адвокату, який представляв його у Суді, і що квитанція за сплату суми в розмірі 500 лей у якості гонорару адвокату, який представляв заявника у національних судах, не супроводжувалася допоміжними документами з викладенням подробиць щодо відпрацьованих годин.

151. Відповідно до прецедентного права Суду, заявник має право на відшкодування судових витрат лише в тій мірі, в якій було доведено, що вони дійсно відбулися та були необхідними й розумними за обсягом (див. *Lupeni Greek Catholic Parish and Others v. Romania* [GC], № 76943/11, § 187, ECHR 2016 (витяги)). У даній справі, беручи до уваги документи у своєму розпорядженні та свою прецедентну практику, Суд вважає розумним присудити заявникові суму в розмірі 1,365 євро, яка охоплює всі заявлені статті.

C. Пеня

152. Суд вважає розумним, що пеня повинна бути встановлена у розмірі граничної відсоткової ставки Європейського центрального банку, до якої слід додати три відсоткових пункти.

ЗА ЦИХ ПІДСТАВ СУД

1. *Постановляє*, одинадцятьма голосами проти шести, що мало місце порушення статті 8 Конвенції;

2. *Постановляє*, шістнадцятьма голосами проти одного, що виявлення порушення становить достатню справедливу сатисфакцію щодо моральної шкоди, понесеної заявником;

3. *Постановляє*, чотирнадцятьма голосами проти трьох, що,

(a) держава-відповідач повинна сплатити заявникові, упродовж трьох місяців, EUR 1,365 (одну тисячу триста шістдесят п’ять євро) в якості відшкодування судових витрат, конвертовані у валюту держави-відповідача за курсом, застосовним на дату виплати, плюс будь-який податок, який може бути стягнутий з заявника;

(b) зі спливом зазначеного тримісячного строку і до остаточного розрахунку на цю суму нараховуватиметься пеня у розмірі граничної процентної ставки Європейського центрального банку, яка діятиме в період несплати, до якої має бути додано три відсоткові пункти;

4. *Відхиляє*, одноголосно, решту вимог заявника щодо справедливої сатисфакції.

Складено англійською та французькою мовами й винесено на відкритому слуханні у Будинку прав людини, Страсбург, 5 вересня 2017 року.

Сорен Пребенсен Гвідо Раймонді  
 Заступник секретаря Головуючий

Відповідно до статті 45 § 2 Конвенції та правила 74 § 2 Регламенту Суду, до цього рішення додаються наступні окремі думки:

(a) частково окрема думка судді Каракаша;

(b) спільна окрема думка суддів Раймонді, Дєдова, Кйолбро, Мітса, Муру-Вікстрьом та Айке.

G.R.  
S.C.P.

ЧАСТКОВО ОКРЕМА ДУМКА СУДДІ КАРАКАША

(Переклад)

Я повністю погоджуюся з висновком більшості про порушення статті 8 Конвенції.

Однак, я не розділяю висновок більшості про те, що визнання порушення становить достатню справедливу сатисфакцію щодо моральної шкоди, понесеної заявником.

Очевидно, що відповідно до статті 41 Суд вирішує присудити певну суму в якості відшкодування моральної шкоди, якщо вважає за «необхідне» присудити відшкодування. Оскільки Суд має значну свободу визначати, в яких справах слід присудити відшкодування заявникам, він іноді робить висновки про те, що визнання порушення становить достатню справедливу сатисфакцію, і що у присудженні грошової компенсації немає необхідності (див., серед багатьох інших, *Nikolova v. Bulgaria*, № 31195/96, § 76, ECHR 1999-II; *Vinter and Others v. the United Kingdom* [GC], №№ 66069/09 та 2 інших, ECHR 2013 (витяги); та *Murray v. the Netherlands* [GC], № 10511/10, ECHR 2016). Для досягнення такого висновку Суд приймає до уваги всі факти справи, у тому числі характер визнаних порушень та будь-які особливі обставини, які є важливими для контексту справи (див., наприклад, *Vinter and Others*, цит. вище, та спільну частково окрему думку суддів Шпільмана, Саджо, Каракаша й Пінто де Альбукерке у справі *Murray*, цит. вище). Коли це виправдано обставинами справи, як у справі *McCann and Others v. the United Kingdom* (27 вересня 1995, § 219, серія A № 324), в якій Суд відмовився присудити будь-яку суму в якості відшкодування моральної шкоди, з оглядом на той факт, що три особи, підозрюваних у тероризмі, які були вбиті, планували підірвати бомбу у Гібралтарі, або характер виявленого порушення, як у справі *Tarakhel v. Switzerland* ([GC], № 29217/12, ECHR 2014 (витяги)), Суд постановляє, що визнання порушення є достатньою справедливою сатисфакцією щодо будь-якої моральної шкоди. Інакше кажучи, лише у виняткових справах Суд вирішує не присуджувати жодні суми в якості відшкодування моральної шкоди.

Можуть також існувати випадки, в яких Суд вирішує присудити нижчу суму, ніж сума, присуджена в інших справах, стосовно відповідної статті, знову беручи до уваги конкретні обставини контексту. Наприклад, у справі *A. and Others v. the United Kingdom* ([GC], № 3455/05, ECHR 2009), у контексті тероризму, Суд дав детальне обґрунтування (§ 252; див. також *Del Río Prada v. Spain* [GC], № 42750/09, § 145, ECHR 2013) та пояснив, чому він присудив значно нижчу суму, ніж в інших попередніх справах, які стосувалися незаконного тримання під вартою.

У даній справі національні суди не забезпечили належний захист права заявника на повагу до приватного життя та кореспонденції: На заявника тяжко вплинули дисциплінарні провадження проти нього, оскільки він був звільнений з посади.

Це порушення статті 8, безсумнівно, заподіяло заявникові моральної шкоди, яку не може задовольнити саме визнання того, що така шкода була понесена. У зв’язку з цим я проголосував за присудження хоча б невеликої суми в якості справедливої компенсації понесеної заявником моральної шкоди.

СПІЛЬНА ОКРЕМА ДУМКА СУДДІВ РАЙМОНДІ, ДЕДОВА, КЙОЛБРО, МІТСА, МУРУ-ВІКСТРЬОМ ТА АЙКЕ

Вступ

1. Ми погоджуємося з більшістю (деякі з нас – з певними ваганнями) у тому, що навіть у контексті, в якому з фактів у розпорядженні Суду складно побачити, як заявник міг мати «розумне очікування приватності» (див. нижче), стаття 8 застосовна в обставинах даної справи (див. пункти 69-81 рішення). Оскільки стаття 8 була визнана застосовною, ми також погоджуємося з тим, що скаргу цього заявника необхідно розглядати з точки зору позитивних зобов’язань держави (див. пункт 111 рішення). За умови подальшого ми також погоджуємося з загальними принципами, застосовними до оцінки позитивного зобов’язання держави, викладеними у пунктах 113-122 рішення.

2. Однак, за наведених нижче підстав ми, зі всією повагою, не погоджуємося з більшістю стосовно правильного підходу до позитивного зобов’язання держави у контексті цієї справи, і з висновком більшості про те, що «національні органи влади», під якими більшість розуміє лише трудові суди, «не забезпечили належний захист права заявника на повагу до приватного життя та кореспонденції і що вони не досягли справедливого балансу між існуючими інтересами» (див. пункт 141 рішення).

Принцип

3. У світлі того факту, що існує спільна точка зору про те, що дану заяву слід розглядати з посиланням на позитивне зобов’язання держави відповідно до статті 8, доречну початкову точку надає прецедентна практика Суду, яка визначає зміст та обсяг концепції «позитивного зобов’язання» у розумінні статті 8. Відповідні принципи були нещодавно узагальнені Великою Палатою у контексті позитивних зобов’язань щодо захисту фізичної та психологічної цілісності заявника від інших осіб, у справі *Söderman v. Sweden* ([GC], № 5786/08, §§ 78-85, ECHR 2013). У тій справі Суд чітко пояснив, що:

(a) мета статті 8 полягає в захисті фізичної особи від довільного втручання з боку державних органів влади. Однак, це положення служить не для того, щоб усього лише змусити державу утриматися від такого втручання: на додаток до цього переважно негативного зобов’язання існують позитивні зобов’язання, притаманні ефективній повазі до приватного або сімейного життя. Ці зобов’язання можуть включати вжиття заходів, розроблених для забезпечення поваги до приватного життя навіть у сфері відносин осіб між собою (див., зокрема, *Airey v. Ireland*, 9 жовтня 1979, § 32, серія А № 32) (*Söderman*, цит. вище, § 78);

(b) вибір засобів, розрахованих для забезпечення дотримання статті 8 Конвенції у сфері відносин фізичних осіб між собою, є, у принципі, питанням, яке потрапляє до свободи розсуду Договірних Держав, не зважаючи на те, чи є зобов’язання держави позитивними або негативними. Існують різні шляхи забезпечення поваги до приватного життя, і характер зобов’язання держави залежатиме від конкретних аспектів приватного життя, яких стосується справа (див., наприклад, *Von Hannover v. Germany (№ 2)* [GC], №№ 40660/08 і 60641/08, § 104, ECHR 2012; *Odièvre v. France* [GC], № 42326/98, § 46, ECHR 2003‑III; *Evans v. the United Kingdom* [GC], № 6339/05, § 77, ECHR 2007‑I; та *Mosley v. the United Kingdom*, № 48009/08, § 109, 10 травня 2011 року) (*Söderman*, цит. вище, § 79); і

(c) стосовно менш серйозних дій між фізичними особами, які можуть порушити психологічну цілісність, зобов’язання держави відповідно до статті 8 щодо підтримки та застосування на практиці належної правової системи, яка забезпечує захист, не завжди потребує, щоб існувало ефективне положення кримінального права, яке б охоплювало конкретну дію. Правова система може також складатися з засобів правового захисту в рамках цивільного права, здатних забезпечити достатній захист (див., з необхідними змінами, *X and Y v. the Netherlands*, 26 березня 1985, §§ 24 та 27, серія А № 91, і *K.U. v. Finland*, № 2872/02, § 47, ECHR 2008). Суд зазначає, наприклад, що у деяких попередніх справах стосовно захисту зображення особи від нападів інших осіб, представлені у державах-членах засоби правового захисту носили характер цивільного права, можливо – у поєднанні з процесуальними засобами правового захисту, такими, як надання судового наказу (див., зокрема, *Von Hannover*, цит. вище; *Reklos and Davourlis v. Greece*, № 1234/05, 15 січня 2009 року; і *Schüssel v. Austria* (dec.), № 42409/98, 21 лютого 2002 року) (*Söderman*, цит. вище, § 85).

4. Факти цієї справи, як визнає більшість, принаймні неявно (див. пункт 80 рішення), звичайно, дуже далекі від серйозності справ, які розглядаються у рішенні *Söderman*. Врешті-решт, у тій справі Суд розглядав твердження про порушення фізичної або психологічної цілісності особи іншою особою.

5. Однак, навіть у такому контексті очевидно, по-перше, що вибір засобів, призначених для забезпечення поваги до приватного життя відповідно до статті 8, навіть у сфері стосунків осіб між собою, належить, переважно, договірним державам; і це вибір, стосовно якого вони користуються широкою свободою розсуду (див. пункт 119 рішення, який уточнює, коли, на відміну від даної справи, на кону конкретний важливий аспект існування або ідентичності фізичної особи, або коли відповідна діяльність включає найбільш інтимний аспект приватного життя). В основі цього висновку лежить той факт, що не існує європейського консенсусу з цього питання, і лише шість з тридцяти чотирьох досліджених держав-членів Ради Європи чітко врегулювали питання приватності на робочому місці (див. пункти 52 та 118 рішення). По-друге, «заходи», вжиті державою відповідно до статті 8, повинні, в принципі, мати форму належної «юридичної системи», яка забезпечує захист постраждалого. Стаття 8 не обов’язково потребує існування ефективного положення кримінального права, яке б охоплювало конкретну дію. Правова система може також складатися з засобів правового захисту у межах цивільного права, здатних забезпечити достатній захист.

6. Це, звичайно, застосовується з необхідними змінами й до даної справи, в якій, як визначає більшість, Суд у кращому випадку турбується про невід’ємний, мінімальний рівень захисту приватного життя і кореспонденції на робочому місці від втручання приватного роботодавця.

Центральний момент перевірки

7. Визначивши деякі з наведених вище принципів, більшість, у пункті 123, несправедливо, на нашу думку, обмежила свою перевірку питанням про те, «як національні суди, до яких звернувся заявник, розглянули його скаргу на порушення роботодавцем його права на повагу до приватного життя та кореспонденції у контексті працевлаштування».

8. Визнаючи, що «засоби захисту можна знайти не лише у трудовому праві, але і у цивільному та кримінальному праві» (див. пункт 116 рішення), більшість, насправді, стала у стороні та уникнула справжнього питання, на яке необхідно відповісти, а саме, чи підтримала та застосувала Висока Договірна Сторона належну «правову систему», яка б надала щонайменше засоби правового захисту в рамках цивільного права, здатні забезпечити достатній захист заявника?

9. Як стверджувала держава-відповідач, і як визнала більшість, відповідна «правова система» у Румунії складається не лише з трудових судів, до яких заявник звернувся зі своєю скаргою. До неї також входили, зокрема:

(a) кримінальне правопорушення, «порушення таємниці кореспонденції» у розумінні статті 195 Кримінального кодексу (див. пункт 33 рішення); до речі, саме той засіб правового захисту, яким скористався заявник, коли подав скаргу у кримінальному порядку, але, після рішення прокурора про те, що не було підстав для відповіді на цю скаргу, не вичерпав його через те, що не опротестував це рішення в національних судах: пункт 31 рішення;

(b) положення Закону № 677/2001 «про захист фізичних осіб у зв’язку з опрацюванням персональних даних та вільним переміщенням таких даних» (див. пункт 36 рішення), який в очікуванні вступу Румунії до ЄС повторює деякі положення Директиви 95/46/EC Європейського Парламенту та Ради Європейського Союзу від 24 жовтня 1995 року про захист фізичних осіб у зв’язку з опрацюванням персональних даних та вільне переміщення таких даних. Цей закон чітко передбачає, у статті 18, право (i) подати скаргу до контролюючого органу та, в якості альтернативи або згодом, (ii) звернутися до компетентних судів за захистом прав на захист даних, гарантованим цим законом, у тому числі права прагнути відшкодування у зв’язку з будь-якою понесеною шкодою; а також

(c) положення Цивільного кодексу (статті 998 та 999; пункт 34 рішення), які дозволяють подати деліктний позов з метою отримання відшкодування шкоди, заподіяної навмисно або через недбалість.

10. Окрім скарги у кримінальному порядку, за якою не слідували жодні дії, жодний з національних засобів правового захисту не був застосований заявником. Замість цього заявник звернувся лише до трудових судів для оскарження здебільшого не втручання роботодавця у його приватне життя/кореспонденцію, а звільнення. Як більшість зауважила у пункті 24:

“Він попросив суд, по-перше, відставити у сторону звільнення; по-друге, наказати роботодавцеві сплатити йому суми, які він заборгував стосовно заробітної плати та будь-яких інших виплат, та повернути його до посади; і по-третє, наказати роботодавцеві сплатити йому 100,000 румунських лей (приблизно 30,000 євро) в якості відшкодування шкоди, понесеної в результаті його звільнення, та відшкодувати судові витрати.”

11. Лише у контексті цих проваджень щодо звільнення, спираючись на рішення Суду у справі *Copland v. the United Kingdom* (№ 62617/00, §§ 43-44, ECHR 2007-I), заявник стверджував, що рішення про його звільнення було незаконним, і що шляхом моніторингу його повідомлень та доступу до їх змісту роботодавець порушив кримінальне законодавство.

12. Той факт, що заявник був сфокусований переважно (якщо не виключно) на законності звільнення, а не на втручанні роботодавця у його право на повагу до приватного життя/кореспонденції, також відображається в тому, як справу заявника було представлено у цьому Суді. Як зазначає рішення у пункті 55, скарга заявника полягала в тому, що «його звільнення роботодавцем ґрунтувалося на порушенні його права на повагу до приватного життя та кореспонденції, і що коли національні суди не скасували цей захід, вони не виконали своє зобов’язання щодо захисту відповідного права».

13. Внаслідок цього не можна не помітити (хоча б побіжно), що якщо б Уряд-відповідач висунув це в якості попереднього заперечення, могли б виникнути питання про те, чи дійсно заявник вичерпав національні засоби правового захисту, «які стосуються заявлених порушень і в той же час є доступними та достатніми», шляхом звернення до трудових судів так, як він зробив (див. *Aquilina v. Malta* [GC], № 25642/94, § 39, ECHR 1999-III). Врешті-решт, у розпорядженні Суду немає матеріалів, які б свідчили, що будь-який з трьох засобів правового захисту, визначених вище, і зокрема, скарга до спеціалізованого контрольного органу з питань захисту даних та/або позов з метою відшкодування шкоди відповідно до Закону № 677/2001 до компетентних судів могли «призвести до невдачі» (див. *Davydov and Others v. Russia*, №75947/11, § 233, 30 травня 2017 року).

14. Наші сумніви щодо ефективності трудових судів у цьому контексті (та доречності того, що Суд обмежив свій аналіз належністю аналізу трудових судів) також підкреслюються тим фактом, що відповідно до юриспруденції Суду за статтею 6 Конвенції, незалежно від того, чи були дії роботодавця незаконними, цей факт не міг сам по собі підірвати належність дисциплінарних проваджень у даній справі. Врешті-решт, як цей Суд підтвердив нещодавно у справі *Vukota-Bojić v. Switzerland* (№ 61838/10, §§ 94-95, 18 жовтня 2016):

“... питання того, чи робило використання в якості доказів інформації, отриманої в порушення статті 8, несправедливим суд у цілому, всупереч статті 6, необхідно визначити, беручи до уваги усі обставини справи, у тому числі повагу до прав заявника на захист і якість та важливість відповідних доказів (порівняйте, зокрема, *Khan*, цит. вище, §§ 35-40; *P.G. and J.H. v. the United Kingdom*, цит. вище, §§ 77-79; та *Bykov v. Russia* [GC], № 4378/02, §§ 94-98, 10 березня 2009 року, в якому не було виявлено порушення статті 6).

Зокрема, необхідно розглянути, чи отримав заявник можливість опротестувати аутентичність доказів та заперечувати проти їх використання. Крім того, слід взяти до уваги якість доказів, як і обставини, за яких вони були отримані, і чи викликають ці докази сумніви щодо їх надійності та точності. Нарешті, Суд повинен надати ваги тому, чи мали відповідні докази вирішальне значення для результату проваджень (порівняйте, зокрема, *Khan*, цит. вище, §§ 35 і 37).”

15. У будь-якому випадку, наведені вище альтернативні національні засоби правового захисту, декотрі з яких явно більш придатні для захисту приватного життя/кореспонденції фізичних осіб на робочому місці, були важливими для оцінки того, чи була здатна створена в Румунії «правова система» забезпечити «належний захист» заявника від незаконного втручання у його право на повагу до приватного життя/кореспонденції відповідно до статті 8 з боку іншої приватної фізичної особи (у цьому випадку – його роботодавця).

16. Не включивши ці альтернативи, в достатній або будь-якій мірі, у свій аналіз, більшість не взяла до уваги важливі чинники, які стосуються питання, представленого у цій справі, і не надали ваги визнаній широкій свободі розсуду, якою користуються Високі Договірні Сторони при визначенні того, які заходи вживати та які засоби правового захисту передбачати відповідно до свого позитивного зобов’язання за статтею 8 щодо створення належної «правової системи». Без будь-яких доказів, які б свідчили, що національні засоби правового захисту, взяті по окремості або разом, не були в достатній мірі доступними або ефективними для надання захисту, який потребує стаття 8, нам здається, що немає підстави, на якій Суд може виявити порушення статті 8 за обставин даної справи.

17. До того, як залишити це питання доречного центрального моменту перевірки, ми хотіли б висловити свою щиру надію на те, що рішення більшості не слід читати, як загальну вимогу згідно з Конвенцією того, щоб коли більш доречні засоби правового захисту є доступними у національній правовій системі (такі, як, наприклад, засоби, які необхідно встановити відповідно до актуального законодавства ЄС щодо захисту даних), національні трудові суди, при розгляді такої справи, як справа заявника, повинні були продублювати функції будь-якого такого, більш доречного, спеціалізованого засобу правового захисту.

Аналіз з боку національних трудових судів

18. Однак, навіть якщо б, всупереч наведеному вище, концентрація більшості лише на аналізі з боку національних трудових судів була доречним підходом, ми також не погоджуємося з тим, що, в дійсності, цей аналіз є настільки дефективним, що це призвело до виявлення порушення статті 8.

19. При розгляді рішень окружного суду та Апеляційного суду Бухаресту ми зазначаємо, що обидва національні суди взяли до уваги внутрішні розпорядження роботодавця, які забороняли користування ресурсами компанії в особистих цілях (див. пункти 12, 28 та рішення). Ми також зауважуємо, що заявник був проінформований про внутрішні розпорядження, оскільки він ознайомився з ними та підписав їх копію 20 грудня 2006 року (див. пункт 14 рішення). Національні суди тлумачили положення цього інструменту, як ті, що мають на увазі можливість того, що певні заходи могли бути вжиті для моніторингу спілкування, і це могло значно зменшити для заявника можливість будь-якого обґрунтованого очікування того, що приватність його кореспонденції буде дотримана (порівняйте з *Halford v. the United Kingdom*, 25 червня 1997 року, § 45, *Reports of Judgments and Decisions* 1997‑III, та *Copland*, цит. вище, § 42). Тому ми вважаємо, що питання необхідно знову розглянути у цьому контексті.

20. У цьому контексті з доступних Суду доказів очевидно, що національні суди дійсно розглянули це питання. Окружний суд та апеляційний суд придали певну вагу інформаційному повідомленню, яке підписав заявник, і їх рішення вказують на те, що підписана копія повідомлення була надана у провадженнях у цих судах (див. пункти 28 та 30 рішення). Окружний суд зауважив, зокрема, що роботодавець попередив працівників про те, що їх діяльність, у тому числі користування комп’ютерами, підлягала моніторингу, і що заявник сам прийняв інформаційне повідомлення (див. пункт 28 рішення). Апеляційний суд також підтвердив, що «у користуванні [ресурсами компанії] в особистих цілях може бути відмовлено ... відповідно до положень внутрішніх розпоряджень», про які заявник був належним чином проінформований (див. пункт 30 рішення). Відповідно, національні суди визнали, на основі документів у своєму розпорядженні, що заявник міг отримати достатнє попередження про те, що його діяльність, у тому числі користування комп’ютером, доступ до якого йому дав роботодавець, могла підлягати моніторингу. Ми не вбачаємо підстави для відхилення від своїх рішень, і вважаємо, що заявник міг мати обґрунтовані очікування того, що його дії підлягали моніторингу.

21. Нарешті, ми зазначаємо, що національні органи влади здійснили ретельне урівноваження інтересів, беручи до уваги право заявника на повагу до приватного життя та право роботодавця на моніторинг, у тому числі й відповідні дисциплінарні повноваження, для забезпечення безперебійного функціонування компанії (див. пункти 28 та 30 рішення, див. також, з необхідними змінами, *Obst v. Germany*,№ 425/03, § 49, 23 вересня 2010, і *Fernández Martínez v. Spain* [GC], № 56030/07, § 151, ECHR 2014 (витяги). Зокрема, апеляційний суд, цитуючи положення Директиви 95/46/EC, зазначив, що у даній справі існував конфлікт між «правом роботодавця на моніторинг та правом працівників на захист приватності» (див. пункт 30 рішення).

22. Ми також зазначаємо, що на основі матеріалів у своєму розпорядженні національні суди визнали, що законна мета, яку переслідував роботодавець під час моніторингу спілкування заявника, полягала у користуванні «правом та обов’язком забезпечувати безперебійне функціонування компанії (див. цитату апеляційного суду у пункті 30 рішення). У той час, як національні суди придали більше ваги праву роботодавця на забезпечення безперебійного функціонування компанії та праву контролювати те, як працівники виконують свої обов’язки у контексту робочих відносин, ніж праву заявника на повагу до приватного життя та кореспонденції, ми вважаємо за розумне для роботодавця бажати переконатися в тому, що його працівники виконують свої професійні обов’язки при користуванні робочим місцем та обладнанням, до якого вони отримали доступ. Апеляційний суд виявив, що моніторинг спілкування заявника був для роботодавця єдиним шляхом досягнення законної мети, що змусило суд досягти висновку про те, що був досягнутий справедливий баланс між потребою захистити приватне життя заявника та правом роботодавця на контроль за функціонуванням бізнесу (див. пункт 30 рішення).

23. На нашу думку, вибір національних органів влади надати перевагу інтересам роботодавця над інтересами працівника сам по собі не здатний викликати питання відповідно до Конвенції (див., з необхідними змінами, *Obst*, цит. вище, § 49). Ми хотіли б повторити, що коли від національних органів влади вимагається досягнення справедливого балансу між декількома конкуруючими приватними інтересами, вони користуються певною свободою розсуду (див. *Hämäläinen v. Finland* [GC], № 37359/09, § 67 у кінці, ECHR 2014, та подальші посилання). Тому в даній справі, на нашу думку, національні суди діяли в межах свободи розсуду Румунії.

24. Ми також зазначаємо, що моніторинг, якого зазнав заявник, був обмежений за часом, і що докази в Суді вказують на те, що роботодавець контролював лише електронні повідомлення заявника та його інтернет-діяльність. Дійсно, заявник не стверджував, що будь-який інший аспект приватного життя, яким він користувався у професійному контексті, контролювався роботодавцем. Крім того, виходячи з доступних Суду доказів, результати моніторингу використовувалися лише в цілях дисциплінарних проваджень проти заявника та лише особи, залучені до цих проваджень, мали доступ до змісту повідомлень заявника (для аналогічного підходу, див. *Köpke v. Germany* (dec.), № 420/07, 5 жовтня 2010 року). У цьому зв’язку помітно, що більшість погоджується з тим, що заявник не обґрунтував свої твердження про те, що зміст повідомлень розкривався іншим колегам (див. пункт 126 рішення).

25. Нарешті, ми зазначаємо, що при розгляді справи, національні органи влади взяли до уваги ставлення заявника в ході професійної діяльності в цілому, і, зокрема, протягом дисциплінарних проваджень проти нього. Так, окружний суд визнав, що заявник скоїв дисциплінарне правопорушення, коли порушив внутрішні розпорядження роботодавця, які забороняли користуватися комп’ютерами в особистих цілях (див. пункт 28 рішення). Національні органи влади надали значної ваги своєму аналізу ставлення заявника у дисциплінарному провадженні, протягом якого він заперечував використання ресурсів роботодавця в особистих цілях та наполягав на тому, що користувався ними лише в робочих цілях, що не відповідало дійсності (див. пункти 28 та 30 рішення). Вони мали право це зробити. Це підтвердилося, коли заявник стверджував у цьому Суді, що хоча він знав, що використання робочого комп’ютера в особистих цілях заборонялося, лише знання про моніторинг з боку роботодавця запобігло б використанню робочого комп’ютера в особистих цілях; він не заперечував, що був проінформований про моніторинг, але не міг згадати, коли отримав інформаційне повідомлення, яке попередило його про моніторинг.

26. Врешті-решт, як більшість також підкреслює (див. пункт 121 рішення), для того, щоб бути плодотворними, робочі відносини повинні ґрунтуватися на взаємній довірі (див. *Palomo Sánchez and Others* *v. Spain* [GC], №№ 28955/06 та 3 інших, § 76, ECHR 2011). Відповідно, на нашу думку, в межах своєї свободи розсуду національні (трудові) суди мали право, при врівноваженні інтересів, узяти до уваги ставлення заявника, який розірвав зв’язок довіри з роботодавцем.

27. Враховуючи всі вищенаведені міркування та на відміну від більшості, ми робимо висновок про те, що право заявника на повагу до приватного життя та кореспонденції було захищено, і тому не мало місце порушення статті 8 Конвенції.

*Переклад Харківської правозахисної групи*