Ефективний демократичний контроль за діяльністю національних служб безпеки

Тематична доповідь

COMMISSIONER FOR HUMAN RIGHTS
COMMISSAIRE AUX DROITS DE L'HOMME
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Ефективний демократичний контроль за діяльністю національних служб безпеки

Тематична доповідь,
опублікована Комісаром
Ради Європи з прав людини

Рада Європи

Фото обкладинки: © Shutterstock

Обкладинка: Documents and Publications Production Department (SPDP), Council of Europe

Видано за фінансового сприяння Женевського Центру демократичного контролю над збройними силами

Переклад: Центр досліджень армії, конверсії та роззброєння

Макет видання українською мовою: Марк Канарський, Київ

Висловлюємо вдячність:

Цю доповідь підготовлено незалежним консультантом Айданом Уїллзом (Aidan Wills).

Зміст

ОСНОВНІ ПОЛОЖЕННЯ

Викриття колишнього найманого співробітника розвідки США Едварда Сноудена знову привернули увагу до діяльності служб безпеки країн – членів Ради Європи. Занепокоєння з приводу використання широкомасштабного електронного спостереження знову порушує питання про необхідність ефективного контролю за діяльністю служб безпеки. Контроль за діяльністю спецслужб є вкрай необхідним для того, щоб ці установи не лише сприяли захисту населення, якому вони покликані служити, але й додержувалися принципу верховенства права і прав людини у своїй діяльності. Однак одкровення Сноудена, причетність деяких європейських служб безпеки до таємного утримання під вартою і незаконної видачі підозрюваних у тероризмі, а також повідомлення про протиправну діяльність служб безпеки в деяких країнах Ради Європи сіють серйозні сумніви щодо здатності національних систем контролю ефективно виконувати свою функцію.

У такому контексті тематична доповідь аналізує способи підвищення ефективності національних систем контролю для кращого додержання прав людини і досягнення прозорості в роботі спецслужб.

Доповідь сфокусовано на вивченні різних способів контролю за діяльністю державних органів, включаючи самостійні відомства, відділи/підрозділи при державних органах і збройних силах, що мають повноваження із збору, аналізу і передачі розвідувальних даних усередині країни. Ці дані збираються для інформування політиків, військового керівництва, поліції, прикордонних і митних служб про наявні загрози національній безпеці й іншим ключовим національним інтересам. Незважаючи на те, що деякі служби безпеки уповноважені заарештовувати та утримувати громадян під вартою, ця доповідь не стосується питання контролю за такою їх діяльністю.

Комісаром Ради Європи з прав людини сформульовано ряд рекомендацій на основі питань, яких стосується це дослідження. Ці рекомендації викладено наприкінці даного резюме.

1. ОГЛЯД ВПЛИВУ ДІЯЛЬНОСТІ НАЦІОНАЛЬНИХ СЛУЖБ БЕЗПЕКИ НА ЗАХИСТ ПРАВ ЛЮДИНИ В ЄВРОПІ

Сучасні приклади впливу діяльності служб безпеки на права людини розглядаються за чотирма напрямами.

По-перше, це діяльність спецслужб, що позначається на недоторканості особи, включаючи право на життя, право на свободу і особисту недоторканність,

а також право не піддаватися катуванням або нелюдському, жорстокому і такому, що принижує гідність, поводженню. Наводяться приклади причетності служб безпеки до видачі та таємного утримання під вартою осіб, підозрюваних у тероризмі; до обміну інформацією, що призводить до видачі таких осіб, катування, нанесення ударів безпілотниками, а також до арештів і безпідставного утримання людей під вартою.

По-друге, це вплив діяльності служб безпеки на приватне і сімейне життя. У багатьох країнах це є найпоширенішим видом втручання служб безпеки в права людини. Досить докладно розглядаються масове спостереження й використання комунікаційних і метаданих; також приділяється увага питанням захищеності використання комп'ютерних мереж та міжнародному обміну розвідувальними даними.

По-третє, це відображення діяльності служб безпеки на свободі висловлювання думок, зборів та об'єднання. Розглядаються як прямі, так і непрямі втручання в ці права, у тому числі превентивний ефект унаслідок можливого і фактичного спостереження. Обговорюється також і більша шкода демократичним процесам, якої завдає втручання служб безпеки в роботу політиків, суддів і неурядових організацій (НУО).

Нарешті, коротко досліджується вплив діяльності служб безпеки на справедливий судовий розгляд, включаючи спостереження за спілкуванням адвокатів зі своїми клієнтами, а також обмеження права на справедливий судовий розгляд заходами засекречування інформації в контексті охорони державної таємниці у справах, до яких залучені служби безпеки.

2. ОГЛЯД МІЖНАРОДНИХ І ЄВРОПЕЙСЬКИХ СТАНДАРТІВ ЗДІЙСНЕННЯ ДЕМОКРАТИЧНОГО КОНТРОЛЮ ЗА ДІЯЛЬНІСТЮ НАЦІОНАЛЬНИХ СЛУЖБ БЕЗПЕКИ

Міжнародні та європейські стандарти контролю за діяльністю служб безпеки розподіляються на юридично-обов'язкові інструменти і необов'язкові принципи та рекомендації. Перша категорія містить у собі положення ряду міжнародних і регіональних договорів, а також їх тлумачення відповідними судами або спеціальними договірними органами. Незважаючи на те, що безпосередньо до контролю можна застосувати дуже малу кількість міжнародних або регіональних юридичних інструментів, чималу кількість положень, що безпосередньо стосуються контролю за службами безпеки, можна знайти у правозастосовній практиці Європейського суду з прав людини (далі – Суд або Страсбурзький суд) по статтях 3, 5, 8 і 13 Європейської конвенції про захист прав людини і основоположних свобод (далі – Конвенція або ЄКПЛ). Вони містять вимоги щодо ефективності розслідування серйозних порушень прав людини, наявності ефективних засобів правового захисту від порушень з боку служб безпеки, у тому числі в контексті таємного спостереження, попереднього одержання дозволу на застосування інтрузивних (що втручаються у приватне життя) методів спостереження, а також оцінку методів спостереження постфактум.

До другої категорії входять рекомендації, резолюції, заяви та доповіді з наступних чотирьох джерел: (i) установи Організації Об'єднаних Націй (ООН), у тому числі Генеральна Асамблея та її спеціально вповноважені агентства; (ii) установи Ради Європи, у тому числі Венеціанська комісія, Парламентська асамблея (ПАРЄ) та її доповідачі, а також Комісар з прав людини; (iii) Європейський Союз; та (iv) транснаціональні ініціативи громадянського суспільства. Упродовж останніх 10 років кількість таких документів різко зросла, настільки, що утворилася ціла галузь принципів «м'якого права» у сфері контролю; по кожному з них надано ключові або нові рекомендації, виділено істотні розбіжності між ними.

Найбільш повними є Збірник ООН щодо найкращої практики з контролю за службами безпеки (UN 2010a), підготовлений колишнім Спеціальним доповідачем ООН з питань прав людини і боротьби з тероризмом, а також знакова доповідь Венеціанської комісії про демократичний контроль за діяльністю служб безпеки. Ряд інших доповідей і резолюцій стосуються питання контролю за діяльністю служб безпеки у ширшому контексті. Особливо значимими є рекомендації, надані уповноваженими органами ООН, Комісаром Ради Європи з прав людини, ПАРЄ та Європейським парламентом у світлі викриття Сноудена.

Окремо розглядаються Глобальні принципи національної безпеки і Право на інформацію (принципи Тсване), оскільки вони містять керівні орієнтири з таких ключових питань, як доступ до інформації контролюючими органами і публічний доступ до документів, що перебувають у віданні служб безпеки та контролюючих органів. Інші положення, що досліджуються в доповіді, містяться в «Оттавських принципах» й у так званих принципах необхідності та пропорційності.

3. НАЦІОНАЛЬНА ПРАКТИКА КРАЇН – ЧЛЕНІВ РАДИ ЄВРОПИ

Країни – члени Ради Європи по-різному підходять до організації контролю за діяльністю своїх служб безпеки. У цьому розділі розглядаються внутрішньодержавні підходи до контролю з боку парламентських комітетів, інститутів незалежного контролю, включаючи експертні контролюючі органи, а також установ, що мають ширші повноваження, включаючи омбудсменів, комісарів із захисту персональних даних/інформації; а також з боку судових і квазісудових органів. Крім цього, у доповіді коротко розглядається роль політичних керівників, органів внутрішнього контролю служб безпеки та неформального контролю з боку громадянського суспільства і засобів масової інформації. Не розглядаючи національні системи контролю в сукупності, наводяться приклади з окремих складових цих систем у різних країнах. Це робиться для того, щоб акцентувати увагу на різниці в підходах різних країн й виокремити кращий позитивний досвід.

Особливо наголошується, що серед членів Ради Європи немає країни, система контролю якої узгоджувалася б з усіма міжнародними або регіональними

принципами та позитивним досвідом, наведеним у доповіді, як і не існує найкращого підходу до організації системи контролю за службами безпеки. Проте, мета доповіді – виокремити певні підходи або методи, що мають значні переваги з погляду захисту прав людини.

Парламентські комітети

Докладно розглядаються повноваження і роль комітетів парламентського контролю, що традиційно вважаються основними органами, відповідальними за контроль за діяльністю служб безпеки. Істотною ознакою ефективності роботи комітетів парламентського контролю є їх доступ до секретної інформації; це питання розглядається в доповіді у світлі альтернативних заходів захисту інформації, а також у зв'язку з делікатним питанням довіри конфіденційної інформації самим парламентаріям. У цьому підрозділі також розглядається питання відносин між парламентськими комітетами й іншими контролюючими органами, яке часто упускається з виду.

Інститути незалежного контролю

Усе помітнішу роль у контролі над діяльністю служб безпеки відіграють експертні органи з питань безпеки і розвідки. У доповіді викладається думка, що вони мають основне значення для підвищення ефективності контролю та поліпшення захисту прав людини.

Контроль з боку експертних органів з питань безпеки і розвідки стає все поширенішим. Часто вони найкраще можуть здійснювати повсякденний контроль за законністю діяльності служб безпеки. Ураховуючи переваги цих органів, у доповіді підкреслюється необхідність підвищення їхньої легітимності відповідно до демократичних принципів.

У більшості країн – членів Ради Європи органи захисту персональних даних і омбудсмени відіграють обмежену роль у контролі над службами безпеки. Проте у доповіді наводяться приклади, коли ці органи можуть сприяти ефективності систем контролю.

Судові органи

Стосовно судових органів мова йде, насамперед, у зв'язку з наданням ними дозволів на застосування інтрузивних методів спостереження. Привертає до себе увагу той факт, що далеко не всі держави передбачають одержання дозволу суду на масове відеоспостереження, доступ до комунікаційних даних або використання комп'ютерних мереж. Ця галузь права відстає від розвитку систем спостереження, а отже застосування навіть традиційних інтрузивних методів спостереження не вимагає санкції суду в більшості юрисдикцій. Ситуація поступово змінюється, у доповіді наводяться приклади держав – членів Ради Європи, які в цей час вимагають судового підтвердження необхідності масового спостереження і доступу до зібраних комунікаційних даних. Також у доповіді вітається залучення фахівців або громадських захисників до участі

в процесах щодо одержання дозволів на спостереження для забезпечення кращого захисту інтересів імовірних об'єктів спостереження.

Квазісудові дозвільні органи

У декількох країнах – членах Ради Європи створено квазісудові органи з надання дозволів на застосування інтрузивних методів спостереження. Досить докладно описано нову бельгійську систему, оскільки Бельгія є однією з небагатьох країн, в якій законодавство встановлює необхідність одержання особливого дозволу на експлуатацію комп'ютерних мереж. Перевагою таких контролюючих органів у порівнянні з судовими інстанціями може бути їх підзвітність іншій контролюючій установі.

Внутрішній контроль

Незважаючи на те, що власний контроль у службах безпеки не був об'єктом аналізу в рамках цієї доповіді, проте вважається важливим наголосити на ключовій ролі самих співробітників служб безпеки у забезпеченні того, щоб діяльність цих служб відповідала стандартам прав людини. Зовнішній контроль ніколи не буде ефективним, якщо в службі безпеки відсутня внутрішня культура, а співробітники не поважають права людини.

4. НА ШЛЯХУ ДО ДІЄВОГО І ДЕМОКРАТИЧНОГО КОНТРОЛЮ ЗА НАЦІОНАЛЬНИМИ СЛУЖБАМИ БЕЗПЕКИ

Спираючись на міжнародні стандарти і національний досвід, у цьому розділі доповіді викладаються найзначніші цілі та найважливіші принципи, що сприяють ефективності контролю за діяльністю служб безпеки. Деякі з них також узято як заголовки в Основних положеннях доповіді.

Демократичний контроль

Важливість демократичного контролю пояснюється тим, що служби безпеки (і, зокрема, відділення, що безпосередньо виконують оперативні завдання) надають державні послуги народу і від імені народу, а тому обрані народом представники повинні бути залучені до процесу забезпечення ефективності й законності державних послуг, що надаються спецслужбами. Демократичний характер контролю полягає, насамперед, у діях парламенту, що приймає закони з питань контролю за діяльністю служб безпеки, виділенні позапарламентським контролюючим установам необхідних бюджетних ресурсів, контролі над роботою експертних контролюючих органів, підвищенні ефективності роботи контролюючих органів, а також у постійному контролі й позапланових перевірках діяльності служб безпеки.

Попередній дозвіл на використання інтрузивних методів

Необхідність одержання незалежного дозволу до початку спостереження повинна поширюватися на нецільовий масовий збір інформації; збір і доступ до комунікаційних даних (у тому числі тих, що перебувають у приватних операторів); і, теоретично, на використання комп'ютерних мереж. Сам процес надання або повторної видачі дозволу на застосування інтрузивних методів спостереження також повинен бути предметом перевірок. З огляду на ускладнення, що можуть виникнути при зверненні до судових інстанцій за дозволом на використання інтрузивних методів, вибір може бути зроблено на користь квазісудової моделі контролю.

Розгляд скарг

Повноваження більшості контролюючих органів обмежуються наданням рекомендацій службам безпеки та/або органам виконавчої влади. Однак, з урахуванням вимог Європейської конвенції про захист прав людини щодо необхідності доступу до ефективного засобу правового захисту для всіх осіб, які стверджують, що їх права були порушені службами безпеки, держави повинні забезпечувати громадянам доступ також і до установ, здатних приймати юридично обов'язкові рішення.

Доступ до інформації, пов'язаної з міжнародним співробітництвом у сфері розвідувальної діяльності

На особливу увагу заслуговує питання доступу до інформації, що стосується міжнародного співробітництва в розвідувальній сфері. У зв'язку з міжнародним співробітництвом між службами безпеки і наслідками такого співробітництва для прав людини, вкрай важливою є можливість контролю за інформацією, обмін якою здійснюється в рамках такого співробітництва, як одержуваною, так і тією, що направляється в іноземні юрисдикції. Для належного контролю за обміном інформацією важливо, щоб контролюючі органи не розглядалися як «треті особи» ні на законодавчому рівні, ні на практиці, а також щоб вони не потрапляли у залежність від підконтрольних спецслужб у рамках здійснення контролю за їх діяльністю.

Ресурси для конролюючих органів

Можливості більшості служб безпеки щодо збору, обміну й одержання інформації зростають в силу технологічного прогресу, збільшення обсягів їх фінансування, а також завдяки використанню складніших систем для реалізації цих цілей. Відповідно, ключовою умовою ефективного контролю стає необхідність звернення до незалежної технічної експертизи. Системи збору і зберігання розвідувальної інформації стають усе складнішими, а їх вплив на права людини неможливо легко оцінити без залучення послуг експерта.

Оцінка роботи систем контролю: хто наглядає за наглядачами?

Незважаючи на те, що на території Ради Європи наявний прогрес у запровадженні контролю за діяльністю служб безпеки, далеко не всі країни продовжують удосконалювати свої системи, шляхом перегляду їх ефективності.

Для ефективності запобігання та реагування на порушення прав людини в контексті діяльності служб безпеки, органи, що здійснюють контроль за їх діяльністю, мають бути наділені відповідними правовими повноваженнями, ресурсами і повинні мати відповідну професійну компетенцію. Ці вимоги змінюються разом зі зміною характеру діяльності служб безпеки. У такому контексті є дуже важливим, щоб ефективність систем контролю періодично піддавалася перевірці. Перевірки можуть бути періодичними або позаплановими, а їх регламентація має бути передбачена законодавством, що регулює роботу контролюючих органів.

РЕКОМЕНДАЦІЇ КОМІСАРА

З урахуванням висновків і результатів проведених досліджень у доповіді Комісар виступає з наступними рекомендаціями, спрямованими на зміцнення контролю за національними службами безпеки і підвищення рівня захисту прав людини цими службами у своїй роботі.

Щоб забезпечити відповідність діяльності, статутів і політики служб безпеки вимогам Конвенції, а також з метою здійснення ефективного демократичного контролю за їх діяльністю, Комісар закликає держави – члени Ради Європи вжити наступних заходів.

Про систему контролю в цілому

1. Утворити новий або уповноважити існуючий орган (один або кілька), повністю незалежний від виконавчої влади та служб безпеки, метою якого стане контроль за усіма аспектами законодавства, правового статусу, управління та власне діяльності служб безпеки. Під усіма контролюючими органами, що згадуються у документі, маються на увазі незалежні контролюючі органи, яким властиві характеристики, окреслені в цих Рекомендаціях.
2. Забезпечити відповідність систем контролю за діяльністю служб безпеки відповідним мінімальним вимогам, що висуваються правозастосовною практикою Європейського суду з прав людини, вимогам, що містяться у Збірнику ООН щодо найкращої практики з контролю за службами безпеки (UN 2010a), а також у Рекомендаціях Венеціанської комісії.

Про межі контролю за службами безпеки

3. Забезпечити, щоб контроль за усіма етапами збору (незалежно від застосовуваних методів або джерел одержання), обробки, зберігання, поширення і знищення персональних даних службами безпеки здійснювався лише однією установою, незалежною від цих служб і від виконавчої влади.
4. Забезпечити, щоб контроль за службами безпеки не обмежувався питанням законності втручання служб безпеки у приватне і сімейне життя,

а поширювався також на втручання у свободу вираження думок, зборів, об'єднання, думки, совісті та релігії.

5. Уповноважити контролюючі органи ретельно вивчати додержання службами безпеки прав людини під час співробітництва з іноземними органами, включаючи співробітництво в сфері обміну інформацією, під час проведення спільних операцій, а також у рамках надання устаткування та проведення навчання. Контроль за співробітництвом служб безпеки з іноземними органами повинен включати, але не обмежуватися нижченаведеною діяльністю:

   а. вивчення відомчих директив і внутрішніх регламентів щодо міжнародного розвідувального співробітництва;

   б. оцінку ризиків порушення прав людини та їх мінімізації під час співробітництва з іноземними службами безпеки, а також у конкретних ситуаціях під час проведення спільних оперативних заходів;

   в. контроль за персональними даними, що передаються за рубіж, включаючи будь-які застереження й умови передачі даних;

   г. контроль за запитами служб безпеки на адресу закордонних партнерів з метою: (і) одержання інформації про будь-яких осіб; та (іі) спостереження за якими-небудь особами;

   д. оцінку угод про співробітництво в розвідувальній сфері;

   е. контроль за проведенням спільних операцій і реалізацією програм спостереження, здійснюваних у рамках співробітництва із закордонними партнерами.

6. Вимагати, щоб служби безпеки отримували дозвіл з боку незалежного від виконавчої влади органу, як у теорії, так і на практиці, на здійснення кожного з нижчеперелічених видів діяльності самостійно або у співробітництві з приватними компаніями:

   а. ведення нецільового масового спостереження незалежно від використовуваних методів, технологій або видів комунікацій, що підлягають взяттю під спостереження;

   б. використання ключових слів або інших фільтрів для вилучення даних з інформації, зібраної за допомогою масового спостереження, особливо, коли використання таких фільтрів здатне ідентифікувати особу;

   в. збір інформації з комунікацій/метаданих прямо або через третіх осіб, у тому числі приватних компаній;

   г. збір персональних даних, що перебувають у розпорядженні інших державних органів;

   д. спостереження через комп'ютерні мережі.

7. Упевнитися, що спостереження через комп'ютерні мережі піддається такому ж контролю, як і під час застосування інших методів спостереження, що однаково впливають на права людини.

8. Вивчити питання залучення до процесу надання дозволів на ведення цільового і нецільового спостереження незалежних захисників суспільних інтересів для представлення інтересів потенційних об'єктів спостереження.

9. Вивчити питання про те, як незалежний контролюючий орган може постфактум переглянути процедуру надання уповноваженим органом дозволу на ведення спостереження.

10. Утворити новий або наділити повноваженнями існуючий контролюючий орган для прийому та розгляду скарг щодо всіх аспектів діяльності служб безпеки. У тих випадках, коли такі органи обмежені винесенням юридично необов'язкових висновків і рекомендацій, держави повинні забезпечити заявникам можливість звернення до інших установ, здатних надати засіб правового захисту, що буде ефективним як за законом, так і на практиці.

11. Надати контролюючому органу повноваження щодо анулювання дозволу на ведення спостережень, а також припиняти ті спостереження, проведення яких не потребує отримання дозволів, у разі, коли таке спостереження буде розцінене як незаконне, а також надати контролюючому органу право вимагати знищення будь-якої інформації, отриманої з використанням таких методів.

12. Забезпечити, щоб процедури, у рамках яких розглядаються порушення, виявлені безпосередньо заявниками, або порушення, що стали відомі в інший спосіб, відповідали процесуальним нормам європейського законодавства в галузі прав людини.

Про незалежність і демократичну легітимність контролюючих органів

13. Намагатися зміцнювати зв'язки між експертними контролюючим органами і парламентами, уживаючи наступних заходів:

    а. надати відповідному парламентському комітету можливість призначати членів контролюючих органів;

    б. наділити парламент правом доручати експертним органам проводити розслідування з певних питань і справ;

    в. установити вимогу щодо звітності експертних контролюючих органів та їх участі в слуханнях у відповідному парламентському комітеті.

Про ефективність контролюючих органів

14. Забезпечити, щоб органи контролю за службами безпеки мали повний доступ до інформації, необхідної для реалізації їх повноважень, незалежно від рівня секретності. Доступ контролюючих органів до інформації має бути забезпечений законом і гарантований можливістю використання слідчих повноважень, що забезпечують такий доступ. Будь-які спроби об-

межити доступ контролюючих органів до засекреченої інформації повинні припинятися та, за необхідності, каратися.

15. Зобов'язати служби безпеки бути відкритими і співробітничати з контролюючими органами. Зі своєї сторони, контролюючі органи відповідають за професійне здійснення своїх повноважень, у тому числі щодо збору та використання секретної інформації лише для виконання завдань, покладених на них законом.

16. Забезпечити, щоб доступ контролюючих органів до інформації не обмежувався і не обумовлювався рішеннями третіх осіб або самих підконтрольних органів безпеки. Це вимоги є ключовими для забезпечення незалежності демократичного контролю від накладення вето з боку іноземних установ, які передавали інформацію службам безпеки. Доступ контролюючих органів до інформації повинен поширюватися на всю відповідну інформацію, яку мають служби безпеки, у тому числі й на ту, що надається іноземними службами.

17. Вимагати від служб безпеки самостійно розкривати контролюючим органам інформацію, використання якої несе певні ризики для прав людини, а також інформацію про потенційні порушення прав людини внаслідок діяльності служб безпеки.

18. Забезпечити законодавчу можливість для залучення незалежних фахівців, які володіють спеціальними знаннями, до роботи комітетів парламентського контролю та експертних контролюючих органів. Зокрема, контролюючі органи повинні мати можливість залучати фахівців в області інформаційних і комунікаційних технологій, які могли б допомогти таким установам краще розбиратися й оцінювати системи спостереження і, як наслідок, точніше оцінювати їхнє втручання в права людини.

19. Забезпечити достатні кадрові та фінансові ресурси установам, що здійснюють контроль за діяльністю служб безпеки, для повноцінної реалізації їх повноважень. Повноцінна реалізація повноважень передбачає необхідність вдаватися до спеціалізованих знань у сфері технологій, що дозволять контролюючим органам розбиратися й оцінювати системи збору, обробки і зберігання інформації. Достатність таких ресурсів має регулярно переглядатися з урахуванням того, що збільшення бюджету служб безпеки може потребувати одночасного збільшення бюджету контролюючих органів.

20. Забезпечити, щоб усі контролюючі органи, що мають доступ до секретної інформації та персональних даних (незалежно від того, є вони секретними чи ні), вжили заходів, що гарантували б використання цієї інформації виключно в межах повноважень контролюючих органів.

21. Законодавчо визначити обов'язок органів, що здійснюють контроль за діяльністю служб безпеки, періодично звітувати шляхом обнародування публічних версій своїх доповідей про проведену роботу та розслідування. Цей обов'язок спричиняє необхідність виділення додаткових ресурсів, що дозволять контролюючим органам складати змістовні звіти без шкоди для їх основних контрольних функцій.

22. Забезпечити, щоб законодавство про свободу інформації поширювалося також на служби безпеки та органи, що здійснюють контроль за ними, і, більше того, щоб рішення про відмову в наданні інформації приймалися індивідуально у кожному окремому випадку, були належним чином обґрунтовані й перевірялися незалежним комісаром із захисту персональних даних/інформації.

Про оцінку діяльності контролюючих органів і систем

23. Періодично оцінювати і переглядати правові норми, інституціональні основи та процедури, а також практику контролю за діяльністю служб безпеки. Наступні елементи повинні бути складовою частиною оцінки їх діяльності (але не обмежуватися ними):

    а. повноваження контролюючих органів, закріплені в нормах права;

    б. внесок контролюючих органів у забезпечення того, щоб правова основа, політика і сама діяльність служб безпеки відповідали внутрішньодержавним і міжнародним нормам в галузі прав людини;

    в. ефективність методів роботи контролюючих органів;

    г. використання нових технологій під час здійснення контролю;

    д. достатність повноважень і засобів для доступу до секретної інформації;

    е. захист інформації контролюючими органами;

    ж. взаємодія і співробітництво між контролюючими органами;

    з. звітність та інформування громадськості.

24. Оцінювати відповідність цілям національної безпеки заходів з контролю за збором і зберіганням персональних даних приватними компаніями, у тому числі постачальниками послуг зв'язку, а також співробітництво між приватними компаніями і службами безпеки.

25. Переглядати правову основу контролю за експлуатацією комп'ютерних мереж службами безпеки щодо достатності існуючих механізмів для додержання внутрішньодержавного і європейського законодавства в галузі прав людини.

Розділ 1

ВСТУП

Безперервні викриття колишнього вільнонайманого співробітника американської розвідки Едварда Сноудена знову привернули увагу до діяльності служб безпеки в країнах-учасницях Ради Європи. Тривога з приводу наслідків широкого електронного стеження знову порушила питання про адекватність контролю над службами безпеки. Не потребує доказів, що контроль за службами безпеки має основоположне значення для того, щоб ці інститути допомагали захисту людей, яким вони служать (та їх прав), і додержувалися закону і прав людини під час виконання цього завдання. Однак викриття Сноудена, причетність деяких європейських служб безпеки до таємного затримання та видачі підозрюваних у тероризмі осіб упродовж минулого десятиліття і триваючі обвинувачення в інших порушеннях у різних країнах породили серйозні сумніви щодо здатності національних систем контролю виконувати цю роль.

Так, Комісар Ради Європи з прав людини нещодавно назвав демократичний контроль за службами безпеки в багатьох європейських країнах «до прикрості неадекватним» (Commissioner for Human Rights 2015: 26).

У контексті цієї доповіді термін «контроль» використовується в широкому значенні, включаючи перевірку діяльності, принципів і правил служб безпеки до, під час та після їх застосування (прийняття). Він включає функції, які називають по-різному, – моніторинг, перевірка, розгляд, оцінка. Там, де йдеться про функції, при яких відповідний орган безпосередньо бере участь в ухваленні рішення про те, чи буде служба безпеки займатися тією або іншою діяльністю, і як саме, термін «контроль» вжито у вузькому значенні. Контроль за службами безпеки в цілому здійснюють: парламент; виконавча влада; суд; спеціальні контролюючі органи; внутрішні органи служб безпеки. Ці сторони разом називають «системою контролю». У контексті цієї доповіді «зовнішній контроль» означає контроль з боку інститутів, що є зовнішніми стосовно служб безпеки та відповідних департаментів/ міністерств/ міністрів виконавчої гілки влади. На додаток до офіційних інститутів контролю, які в цілому спираються на закон або навіть на конституцію, громадянське суспільство та ЗМІ також відіграють важливу роль у контролі над службами безпеки та моніторингу роботи контролюючих органів.

Поняття «служба безпеки» застосовується до державних органів, включаючи як самостійні відомства, так і департаменти/підрозділи інших урядових департаментів або збройних сил, що мають завдання із збору, аналізу і передачі інформації в межах держави для забезпечення прийняття обґрунтованих рішень політиками, військовим командуванням, поліцейськими слідчими органами та прикордонними (митними) відомствами щодо загроз національній безпеці й іншим фундаментальним національним інтересам. У деяких країнах-учасницях Ради Європи їх функції можуть включати також елементи правоохоронної діяльності та захисту об'єктів і людей. Для цього деякі служби безпеки також мають повноваження примусу – арешту і затримання. Контроль за цією діяльністю повинен регулюватися тими ж принципами, що застосовуються до персоналу правоохоронних органів – у цій доповіді вони детально не розглядаються.

Додержання прав людини службами безпеки залежить не тільки від ефективного контролю, але й від правової бази їх роботи. У численних публікаціях було розглянуто застосування Європейської конвенції з прав людини (Конвенція, або ЄКПЛ) до діяльності служб безпеки та сформульовано принципи щодо сфери та ходу їх діяльності[1]. Ця доповідь не буде повертатися до цих питань; вона не розглядатиме, що службам безпеки дозволено робити або як потрібно регулювати їх роботу. Мета цієї доповіді – систематизувати міжнародні стандарти і національні підходи до контролю за службами безпеки для пошуку практик і процедур, здатних посилити захист прав людини в роботі служб безпеки. Це буде зроблено спочатку шляхом аналізу міжнародних правових стандартів і принципів «м'якого права», що стосуються контролю, а потім – шляхом розгляду національних підходів до різних аспектів контролю. Нарешті, у цій доповіді буде розглянуто ряд завдань щодо розвитку (удосконалення) системи контролю за службами безпеки. Перед тим як приступити до оцінки, у документі представлено загальний огляд наслідків для прав людини в деяких сферах діяльності служб безпеки на території Ради Європи.

1. Наприклад: ООН 2010a; Cameron 2000; Omtzigt 2015.

Розділ 2

ЗАГАЛЬНИЙ ОГЛЯД ВПЛИВУ ДІЯЛЬНОСТІ НАЦІОНАЛЬНИХ СЛУЖБ БЕЗПЕКИ НА ЗАХИСТ ПРАВ ЛЮДИНИ В ЄВРОПІ

Давно визнано, що робота служб безпеки обмежує ряд прав людини і може підривати демократичні процеси в цілому. Служби безпеки мають ряд характеристик, що створюють потенціал для порушень прав людини, якщо ці служби не підлягають ефективному контролю і не спираються на ефективні закони. Серед таких характеристик – використання повноважень, пов'язаних з можливістю втручання, які можуть бути використані безконтрольно, значною мірою в умовах таємності, і в деяких країнах розглядаються як наданий уряду інструмент, що може бути використаний у політичних цілях.

Мета цієї глави – показати деякі шляхи, якими служби безпеки впливали (і продовжують впливати) на права людини в країнах-учасницях Ради Європи; вона не ставить за мету дати вичерпний аналіз того, як саме діяльність служб безпеки зачіпає права людини. Цей загальний огляд наведено, щоб краще продемонструвати, чому служби повинні підлягати суворій системі контролю. У всій цій главі мова йде про діяльність служб безпеки. Однак іноді це потрібно поширювати й на представників виконавчої влади, які направляють, визначають політику та у деяких випадках ставлять завдання службам безпеки. У різних країнах Ради Європи політична виконавча влада має давню історію (зло)вживань служб безпеки для незаконної й антидемократичної діяльності.

У цій главі буде наведено ряд найяскравіших прикладів діяльності служб безпеки, що зачіпає права людини, за минулі 15 років. Однак варто пам'ятати, що порушення прав людини службами безпеки в Європі мають давню історію, багато з них відбувалися в епоху, коли служби безпеки в на-

багато меншій мірі піддавалися регламентації і контролю, а громадськість була інформована про діяльність служб безпеки значно менше, ніж сьогодні. Серед яскравих історичних прикладів – систематичні порушення прав людини такими службами безпеки, як Stasi (у Німецькій Демократичній Республіці), Securitate (у Румунії) і STB (у Чехословаччині). Порушення прав людини в жодному разі не зводилися до діяльності служб безпеки колишнього Східного блоку. Розслідування в інших країнах, таких як Люксембург і Норвегія, виявили широке незаконне стеження всередині країни, головним чином – за лівими групами і політиками.

Сучасні приклади впливу, який діяльність служб безпеки може справляти на права людини, можна розбити на чотири великі категорії. По-перше, це діяльність, що впливає на недоторканість особи, включаючи право на життя, право на особисту свободу та безпеку і право не піддаватися катуванням, нелюдському, жорстокому й принизливому поводженню. По-друге, діяльність служб безпеки впливає на право на приватне і сімейне життя. У більшості юрисдикцій це головний інструмент впливу служб безпеки на права людини. По-третє, діяльність служб безпеки впливає на права на свободу слова, об'єднання і зборів. Нарешті, буде коротко розглянуто вплив служб безпеки на право на справедливий суд і судові процеси за участю служб безпеки.

2.1. Недоторканість і свобода особистості

Після терористичних актів у США 11 вересня 2001 року («9/11») на території Ради Європи мали місце викриття діяльності служб безпеки у контексті боротьби з тероризмом. Загалом ці викриття стосувалися контртерористичної діяльності під егідою США за участі тією чи іншою мірою принаймні 25 європейських служб безпеки і урядів (Commissioner for Human Rights 2014b). Стосовно причетності європейських служб безпеки до контртерористичної діяльності під егідою США, на сьогодні підтверджено або вважається, що служби країн-учасниць Ради Європи:

- розміщували секретні американські в'язниці, де підозрювані у тероризмі утримувалися без зв'язку із зовнішнім світом та в неналежних умовах[2];
- сприяли викраденню і передачі людей на такі ж об'єкти в Європі та за межами Європи[3];

2. Суд виніс рішення проти Польщі у двох випадках: Al Nashiri v. Poland; Husayn (Abu Zubaydah) v. Poland. Ці рішення вже є остаточними, після того як Страсбурзький суд відмовив у дозволі передати їх до його Великої палати. Тривають процеси проти Румунії (Al Nashiri v. Romania) і Литви (Abu Zubaydah v. Lithuania). Див. також: European Parliament 2013 та Connolly 2014.
3. Див., наприклад: El Masri v. «the former Yugoslav Republic of Macedonia» й Nasr and Ghali v. Italy. Див. також: Open Society Justice Initiative 2013: 78 (Georgia), 109 (Sweden).

- організовували та/або брали участь у допиті осіб, затриманих неєвропейськими розвідувальними службами, разом чи замість цих служб[4].

Такі дії порушували, зокрема, статті 3, 5, 6, 8 і 13 Європейської конвенції з прав людини. Повномасштабне дослідження цих викриттів перебуває за рамками цієї доповіді. Досить сказати, що інститути Ради Європи (набагато більше, ніж національні інститути) займалися розслідуванням та усуненням цих порушень прав людини. Зокрема, можна згадати звіти про розслідування Діка Марті (Dick Marty) для Комітету з правових питань і прав людини Парламентської асамблеї Ради Європи (ПАРЄ) і знакові рішення Європейського суду з прав людини у процесах Ан-Нашірі проти Польщі, Хусейн (Абу Зубайдах) проти Польщі і Ель-Масрі проти «Колишньої Югославської Республіки Македонія».

Крім порушень прав людини в контексті контртерористичної діяльності під егідою США, надходили повідомлення про катування, негуманне і принизливе поводження, довільні затримання і незаконне застосування сили зі смертельним результатом російськими силами безпеки, особливо в Чечні та Дагестані[5].

Було також багато заяв про те, що європейські служби безпеки причетні до порушення права на незастосування катувань та/або не бути довільно затриманим через передачу ними інформації закордонним партнерам. Хоча наслідки такого інформування важко перевірити, схоже, що передавалася, зокрема: інформація або питання, що ставилися особам, яких затримували і катували неєвропейські служби безпеки[6]; інформація розвідслужбам США, що могла бути використана для ідентифікації та виявлення місцезнаходження людей для позасудових убивств[7]; та інформація, що призвела до видачі людей та/або їх довільного затримання неєвропейськими розвідувальними службами[8].

Крім діяльності, що стосується міжнародного співробітництва розвідувальних служб, надходили повідомлення про те, що в деяких країнах Ради Європи служби безпеки продовжують брати участь у довільних арештах та утриманні людей без зв'язку із зовнішнім світом[9]. Саме в цій області таємність і широка свобода дій, характерні для роботи служб безпеки, становлять особливу загрозу недоторканості особи.

4. Див., наприклад: Human Rights Watch 2009: 17-35; Cobain 2013: 240-242, 253, 257-258 та Open Society Justice Initiative 2013: 78 (Germany).
5. Див., наприклад: ООН 2010b: параграфи 208-214 та Nemtsova 2012.
6. Cobain 2013: Chapter 8.
7. Див., наприклад: Singh and Scholes 2014; Stark 2011; Osborne 2013.
8. Див., наприклад, процес, що триває у Великобританії, Абдула Хакіма Бельхаджа (Abdul Hakim Belhaj): www.reprieve.org.uk/case-study/abdul-hakim-belhaj/, accessed 28 March 2015.
9. Наприклад: Commissioner for Human Rights 2013a: § 8.

2.2. Право на приватне і сімейне життя

Служби безпеки можуть найбільше впливати на право на приватне і сімейне життя шляхом збору, зберігання і передачі персональних даних[10]. Праву на приватне життя загрожує не лише фактична реалізація цих заходів, а й можливість їх застосування чи навіть існування законодавства, що дозволяє їх застосовувати[11]. Право на приватне життя, звісно, може бути законно обмежене службами безпеки, якщо це відповідає вимогам національного законодавства та ЄКПЛ.

У минулому занепокоєння з приводу впливу на право на приватне життя викликало в основному використання службами безпеки цілеспрямованого стеження за допомогою таких методів, як прослуховування особистого телефону або розміщення пристроїв для прослуховування в будівлі – іншими словами, заходи, спрямовані на певну особу чи організацію, зазвичай на підставі обґрунтованої підозри щодо участі в серйозній злочинній діяльності або іншій загрозі національній безпеці. Збір інформації про людину, включаючи залучення інформаторів та упровадження до груп, є ще одним аспектом роботи служб безпеки, що здавна має справляє вплив на приватне життя. Хоча такі дії продовжують мати місце і, як і раніше, впливають на право на приватне життя, на зміну занепокоєності ними у багатьох країнах Ради Європи приходить повідомлення про цілеспрямоване, масове стеження за електронними засобами зв'язку.

Швидкий розвиток технологій дав службам безпеки в ряді країн-учасниць Ради Європи можливість ширше контролювати засоби зв'язку при менших трудозатратах. В Європі суспільна увага у зв'язку з масовим перехопленням службами безпеки вперше привернули повідомлення про систему «Echelon» на початку сторіччя (European Parliament 2001). Набагато серйознішими стали викриття колишнього вільнонайманого співробітника американської розвідки Едварда Сноудена, що вперше пролунали влітку 2013 р. Сноуден повідомив про масштабне стеження за електронними засобами зв'язку й Інтернетом з боку Агентства національної безпеки США та різних служб безпеки в Європі. Повідомлення про подібні програми також з'явилися, зокрема, у Франції[12].

На відміну від більш традиційних методів спостереження, програми, про які повідомлялося, не обов'язково спрямовані проти конкретних осіб або органі-

10. Підтверджено Європейським судом з прав людини стосовно таких видів діяльності: телефонний зв'язок (Malone v. the United Kingdom [64]); електронна пошта (Weber and Saravia v. Germany [77]); зберігання інформації в реєстрах служб безпеки (Segerstedt-Wiberg and Others v. Sweden [72]); неповідомлення людини про збір інформації про неї (Segerstedt-Wiberg and Others v. Sweden [99]); зберігання та використання персональних даних службою безпеки (Leander v. Sweden [48]); передача та використання іншими органами влади, що являє собою окремий акт втручання (Weber and Saravia v. Germany [79]); передача на знищення та неповідомлення (Weber and Saravia v. Germany [79]); встановлення пристроїв для прослуховування (Vetter v. France [20]).
11. Weber and Saravia v. Germany [78-79]; Liberty and Others v. the United Kingdom [57].
12. Follorou and Johannes 2013; Follorou 2014; Bigo et al. 2014.

зацій у зв'язку з підозрою в участі у тій чи іншій діяльності. Замість цього широко застосовується автоматичне перехоплення (за допомогою різних інструментів, а іноді – за допомогою провайдерів послуг зв'язку) величезних масивів інформації, що проходить оптоволоконними кабельними чи бездротовими лініями зв'язку, або зберігається у третіх сторін. Зібрана інформація містить зміст повідомлень, а також так звані дані зв'язку, або метадані, такі як електронні адреси, IP-адреси, телефонні номери та місця знаходження телефонів. Зібрана інформація згодом проглядається або фільтрується з використанням певних налаштувань або умов пошуку інформації стосовно осіб (організацій), які цікавлять служби безпеки[13].

Викриття Сноудена викликали серйозну тривогу щодо права на приватне і сімейне життя. Така діяльність розслідувалася Європейським парламентом (ЄП), Комітетом з правових питань і прав людини ПАРЄ (доповідач Пітер Омтцигт (Pieter Omtzigt)) і різними національними контролюючими органами. Претензії в цьому зв'язку висувалися як у національних судах[14], так й у Страсбурзькому суді[15].

Коментуючи повідомлення про масове стеження, спеціальний доповідач ООН Бен Еммерсон (Ben Emmerson) заявляв, що:

> «Саме існування програм масового стеження таїть можливість непропорційного втручання у право на приватне життя ... постійний і невибірковий збір державами всіх повідомлень або метаданих є несумісним з існуючими концепціями приватного життя. [Ці програми –] прямий і триваючий виклик укоріненим нормам міжнародного права» (ООН 2014: §§18, 59).

Верховний комісар ООН з прав людини також висловив занепокоєння з приводу виправдань такого втручання у право на приватне життя, заявивши:

> «Буде недостатньо, якщо заходи спрямовуватимуться на пошук декількох голок у стозі сіна; правильний критерій – вплив заходів на стіг сіна, що відповідає можливій шкоді; а саме: чи є заходи необхідними і пропорційними» (Управління Верховного комісара ООН з прав людини 2014: §25).

Нарешті, Комісар Ради Європи з прав людини назвав таке масове стеження «серйозною загрозою праву на приватне життя» (Commissioner for Human Rights 2013b).

Право на приватне життя зачіпає не тільки перехоплення вмісту повідомлень, але й збір, зберігання і використання так званих даних зв'язку, або метаданих[16]. Хоча дані зв'язку можуть збиратися й зберігатися безпосередньо службами безпеки, у більшості країн приватні провайдери послуг зв'язку за законом зобов'язані зберігати дані зв'язку клієнтів протягом певного періоду.

---

13. Загальний огляд див. у: Venice Commission 2015: §§ 48-51; Bigo et al. 2013; Omtzigt 2015.
14. Див., наприклад, Privacy International in the UK: www.privacyinternational.org/?q=legal-actions, accessed 28 March 2015.
15. Big Brother Watch and Others v. the United Kingdom.
16. Докладніше див.: Commissioner for Human Rights 2014a: 115-117.

У квітні 2014 р. Судова палата Європейського Союзу ухвалила, що директива про зберігання даних ЄС, що дозволяла зберігання даних зв'язку провайдерами послуг зв'язку для правоохоронної діяльності, є несумісною з правом на приватне життя[17]. Коментуючи зв'язок даних зв'язку з приватним життям, палата ухвалила:

> «Дані [зв'язку], узяті в цілому, можуть дати змогу зробити дуже точні висновки щодо приватного життя людей, чиї дані зберігаються, такі як звички повсякденного життя, постійне або тимчасове місце проживання, щоденні або інші переміщення, заняття, соціальні відносини цих людей та їх соціальне оточення»[18].

У багатьох країнах-учасницях Ради Європи масове невибіркове стеження служб безпеки або не регламентується певним загальнодоступним законом, або регламентується настільки туманно, що закон передбачає мало обмежень і вносить мало ясності в ці заходи.

Це проблематично з позицій прав людини, оскільки ускладнює розуміння приватними особами й організаціями правової основи та підстав для можливого перехоплення їх повідомлень або заперечування такого стеження як незаконного (Commissioner for Human Rights 2014a: 109-110).

Незаконне проникнення до комп'ютерних мереж (у просторіччі – хакерство) є ще однією сферою діяльності служб безпеки, що таїть серйозний ризик для прав людини. Хакерство охоплює такі різні методи, як впровадження вірусів або «троянів» в інформаційні системи для вилучення інформації; використання камер і мікрофонів комп'ютерів і переносних пристроїв для фіксації діяльності користувачів; проникнення в електронні пристрої для маніпуляцій зі змістом відправлених ними (їм) повідомлень[19]. Цей бік діяльності залишається відносно новим, детально не регламентованим в законодавстві про служби безпеки і не розглянутим у публічних звітах про роботу служб безпеки. Проте ясно, що така діяльність являє собою серйозну загрозу для права на приватне і сімейне життя. Хакерство є потенційно більш безцеремонним, ніж перехоплення змісту повідомлень та/або метаданих, не останньою чергою тому, що воно дає доступ до інформації, якою людина воліла б ніколи та ні з ким не ділитися. У зверненні до Трибуналу з питань слідчих повноважень (*Investigatory Powers Tribunal*) Великобританії організація Privacy International передає загрозу приватному життю у такий спосіб:

> «Сучасний еквівалент вторгнення до чийогось будинку, пошуку в його шафах, щоденниках і листах та встановлення пристроїв для постійного стеження в майбутньому і, при використанні мобільних пристроїв, одержання хроноло-

17. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others, див. зокрема [29] [57] [58] та [65].
18. Там само, [27].
19. Загальний огляд див. у: Omtzigt 2015: §§ 66-69; Gallagher and Greenwald 2014; BBC News 2015.

гічної інформації, включаючи всі місця, де він був торік ... якщо мобільний пристрій є зараженим, постійне стеження ніде не дасть людині спокою» (Privacy International 2014: §§ 4-6, 11-18).

Якщо взяти як приклад використання мікрофону і камери смартфону для фіксації поточних контактів та оточення людини, це, безумовно, є більш безцеремонним, ніж розміщення прослуховуючих пристроїв у будинку або машині та/або персональне стеження за такою людиною. Хакерство також може привести до виникнення в системі слабких місць, чим можуть скористатися треті сторони, наприклад, організовані злочинні групи.

Поряд із занепокоєнням з приводу того, що міждержавний обмін розвідувальною інформацією може призвести до катувань і довільного затримання людини, передача персональних даних службами безпеки за рубіж часто має наслідки для права на приватне життя. Під час передачі персональних даних це право зачіпається щоразу. Особлива стурбованість виникає, коли іноземні служби безпеки, яким передається інформація, не мають аналогічних стандартів захисту даних та/або суворих юридичних вимог, що обмежують використання персональних даних з тією чи іншою метою. Хоча багато служб безпеки супроводжують передану інформацію застереженнями (вимогами щодо порядку використання інформації), вони не можуть повністю нівелювати можливі порушення одержувачем права на приватне життя. Наступне питання – навмисне або випадкове використання міждержавного обміну розвідувальною інформацією, щоб обійти обмеження, що, як правило, діють відносно збору інформації. У той час як служби безпеки зазвичай повинні отримати санкцію, наприклад, на перехоплення переговорів людини у своїй країні, якщо ту ж інформацію було отримано закордонним партнером і потім передано, вона може не підпадати під такі обмеження.

Ці ризики зростають в умовах обміну розвідувальною інформацією, що передбачають автоматичну передачу електронних даних та/або наявність вбудованих систем збору і зберігання інформації в інтересах декількох держав[20].

2.3. Права на свободу слова, зборів та об'єднання

Діяльність служб безпеки впливає на права на свободу слова, зборів та об'єднання, тобто права, покликані захистити взаємини з іншими людьми.

Перешкоджання цим правам може мати далекосяжні наслідки для процесів, властивих функціонуванню демократії та верховенства права, включаючи вільну пресу, діяльність політичних партій, профспілок, релігійних організацій і правозахисників.

Перешкоджання цим правам може бути прямим або опосередкованим. Служби безпеки іноді прямо перешкоджають праву на свободу слова, наприклад, змушуючи ЗМІ змінювати свою редакторську політику (Human Rights

20. Загальний огляд див. у: Venice Commission 2015: § 78.

Watch 2014a: 25), вимагаючи не допустити публікації інформації[21], наполягаючи, щоб організації видалили передану в ефір інформацію[22], змушуючи організації видаляти інформацію, що може (у подальшому) бути опублікована (Borger 2013), і вилучаючи інформацію у журналістів[23]. Такі заходи іноді можуть являти собою законне обмеження прав людини; однак вони також уживаються в порушення ЄКПЛ.

Настільки ж важливим є використання повноважень (наприклад, служб безпеки Росії), що дозволяють службам безпеки виносити попередження особам, поведінка яких (включаючи публікації або виступи) вважається небажаною, але ще не досягла порогу карного злочину[24].

Непряме перешкоджання правам на свободу слова, об'єднання та зборів у першу чергу відбувається через стеження, включаючи як цілеспрямовані, так і невибіркові заходи, і (все більше) хакерство служб безпеки. Моніторинг (можливий або фактичний) службами безпеки листування, висловлень і розмов людини може обмежувати реалізацію цих прав, оскільки він впливає на бажання людини брати участь у такому спілкуванні і може формувати зміст такого спілкування. Реагуючи на повідомлення про масове стеження в Інтернеті, Верховний Комісар ООН з прав людини зауважив, що під загрозою опиняються всі ці права, оскільки це права, якими все частіше користуються за допомогою цифрових ЗМІ (Управління Верховного Комісара ООН з прав людини 2014). У цьому контексті існує міцний зв'язок між правом на приватне і сімейне життя та свободою слова, об'єднання та зборів. Приватне життя дозволяє людям реалізувати інші свої права без незаконного втручання (Генеральна Асамблея ООН 2013).

Обмежувальний ефект (потенційного) стеження виникає не тільки унаслідок перехоплення змісту повідомлень або переговорів, але й, як нещодавно визнала Судова палата Європейського Союзу, через закони, що дозволяють зберігання даних зв'язку/метаданих[25].

Європейський суд з прав людини визнав, що не тільки фактичне ведення стеження впливає на право на свободу слова (і, за аналогією, об'єднання та зборів), але й саме існування законодавства, що дозволяє такі заходи, являє собою втручання[26]. Крім збору інформації, Суд визнав, що обробка персональних даних стосується не тільки права на повагу до приватного і сімейного життя, але й права на свободу думки, совісті та релігії, слова, зборів та об'єднання, якщо

21. Sunday Times v. the United Kingdom (No. 2).
22. Наприклад: Le Monde 2013.
23. Див., наприклад, справа Девіда Міранди (David Miranda) у Великобританії: www.bbc.co.uk/news/uk-23782782, accessed 28 March 2015.
24. Див., наприклад, дискусію Венеціанської комісії про такі повноваження в Росії: Venice Commission 2012: §§ 48-61.
25. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others [28].
26. Weber and Saravia v. Germany [144].

такі дані обробляються у зв'язку з політичною позицією людини або її участю в тих чи інших групах[27].

У деяких країнах Ради Європи правляча партія або керівники уряду/держави продовжують використовувати служби безпеки як інструмент. Таке втручання набуває різних форм. У найбільш грубій формі воно включає залякування (і навіть фізичні напади) з боку служб безпеки по відношенню до людей (організацій), які вважаються критично налаштованими щодо уряду, а також пряме втручання в політичні процеси (Commissioner for Human Rights 2013a: §39). Частіше служби безпеки прослуховують опозиційних політиків, НУО та суддів (на вимогу політичної виконавчої влади або за своєю власною ініціативою), щоб одержати компрометуючу інформацію для обчорнення та/або залякування осіб, що вважаються опонентами. Такі звинувачення звучали, наприклад, в «Колишній Югославській Республіці Македонія» і Сербії (Balkan Insight 2015a). Діяльність подібного характеру підриває демократичні процеси та верховенство права. Нарешті, були випадки, коли служби безпеки вели несанкціоноване стеження за представниками виконавчої влади (Higgins 2013). Це є особливо проблематичним з огляду на, що демократичне правління вимагає, щоб служби безпеки перебували під цивільним контролем і не ставали державою в державі.

Особливу тривогу викликає вплив стеження служб безпеки за ЗМІ, чиї функції включають інформування про політику і практику безпеки урядів. Стеження може підривати конфіденційність журналістських джерел і, відповідно, здатність журналістів розкривати «гріхи» уряду[28]. Така робота є особливо важливою з огляду на, що в багатьох країнах офіційні органи контролю були неефективними під час фіксації та реагування на порушення прав людини службами безпеки.

2.4. Право на справедливий суд і право на ефективний правовий захист

Діяльність служб безпеки може завдавати шкоди праву на справедливий суд і праву на ефективний правовий захист у різний спосіб. По-перше, людям часто дуже важко подати цивільний позов проти служб безпеки, навіть якщо вони знають, що їхні права могли бути порушені. Справа в тому, що уряди і служби безпеки можуть посилатися на аргумент державної таємниці, щоб не допустити заслуховування претензій, або дотримуватися тактики «не підтверджувати й не заперечувати» (відносно своїх агентів і діяльності), щоб вихолостити судочинство.

По-друге, якщо і вдається подати позов, судову процедуру може бути істотно змінено для захисту секретної інформації. Це може ускладнити або зробити

27. Segerstedt-Wiberg and Others v. Sweden [107].
28. Weber and Saravia v. Germany [143] [145]; див. також: European Parliament 2014: §§ 86-87.

неможливим справедливий суд. Наприклад, учасників та їх законних представників можуть не допустити до участі у процесі або його частині, що ускладнює їх ознайомлення і, більше того, захист у справах проти них. Також можуть бути обмежені або відсутні права на роз'яснення вироку і дуже обмежуватися права апеляції.

По-третє, перехоплення листування між адвокатами та їх клієнтами, як це було нещодавно виявлено у Великобританії, може порушувати рівність сторін і право на справедливий суд, особливо якщо в процесі беруть участь служби безпеки (Travis and Bowcott 2015).

По-четверте, передача інформації іноземним безпековим і правоохоронним органам може нести ризик для права на справедливий суд. Що стосується інформації, що передається іноземним органам, існує ризик її використання (всупереч попередженням про надійність або заборону використання в судовому процесі) у карних та інших процесах.

Інформація, отримана від іноземних органів, що могла бути отримана з порушенням прав людини або є ненадійною з інших причин, у деяких країнах може використовуватися у судових процесах, що робить їх несправедливими.

Нарешті, деякі країни прийняли закони, що дають співробітникам служб безпеки фактичний імунітет від розслідування та/або цивільних позовів. У Туреччині, наприклад, співробітників служб безпеки не можна переслідувати у судовому порядку без дозволу прем'єр-міністра і міністра внутрішніх справ[29]. Такі положення можуть сприяти безкарності порушень прав людини.

29. Turkey 2014; Human Rights Watch 2014b.

Розділ 3

ЗАГАЛЬНИЙ ОГЛЯД МІЖНАРОДНИХ І ЄВРОПЕЙСЬКИХ СТАНДАРТІВ ДЕМОКРАТИЧНОГО КОНТРОЛЮ ЗА НАЦІОНАЛЬНИМИ СЛУЖБАМИ БЕЗПЕКИ

Міжнародні та європейські стандарти контролю за службами безпеки в цілому можна розділити на обов'язкові правові інструменти («тверде право») і необов'язкові принципи або рекомендації («м'яке право»). До першої категорії належить ряд міжнародних і регіональних договорів, а також їх тлумачення відповідними судовими або договірними органами. Остання категорія включає рекомендації, резолюції, декларації та звіти із чотирьох джерел: (i) інститути ООН; (ii) інститути Ради Європи; (iii) Європейський Союз; (iv) міжнародні ініціативи громадянського суспільства.

3.1. Міжнародні та регіональні правові інструменти

Не існує міжнародних договорів, що безпосередньо стосуються контролю за службами безпеки. Однак Міжнародний пакт про громадянські і політичні права (МПГПП)[30], Конвенція ООН проти катувань (UNCAT) і ЄКПЛ містять статті, що стосуються зобов'язань держав з контролю за службами безпеки.

Усі країни-учасниці Ради Європи зв'язані цими договорами.

30. International Covenant on Civil and Political Rights, 16 December 1966 (entry into force 23 March 1976).

Конкретні вимоги щодо контролю відповідно до статті 8 ЄКПЛ (Право на повагу до приватного і сімейного життя)

Стаття 8 ЄКПЛ тлумачиться як така, що передбачає ряд вимог до контролю за службами безпеки. Застосовуючи статтю 8, Страсбурзький суд визначив критерії (мінімальних) вимог щодо контролю для того, щоб заходи служб безпеки, що обмежують право на приватне і сімейне життя, відповідали ЄКПЛ. Суд також виклав фактори, які можуть оцінюватися на індивідуальній основі під час ухвалення рішення, чи забезпечує дана система контролю достатній захист. Цю судову практику вироблено головним чином на основі позовів, поданих у зв'язку із цілеспрямованими і невибірковими заходами стеження, зберіганням персональних даних службами безпеки та спробами окремих осіб перевірити, чи зберігають служби безпеки їхні персональні дані.

Проте принципи, що тут обговорюються, можна застосувати до контролю за іншими заходами, що зачіпають статтю 8 Конвенції. Варто зазначити, що вони можуть поширюватися на хакерство в ситуаціях, коли ці заходи стосуються права на приватне життя. Хоча вони не розглядаються в цьому документі, слід зауважити, що діяльність служб безпеки повинна відповідати й іншим вимогам, викладеним у статті 8(2) та практиці її застосування, які не стосуються безпосередньо контролю (Venice Commission 2007, 2015).

Суд зауважив критичну важливість зовнішнього контролю для захисту від зловживань і довільного застосування заходів, пов'язаних із втручанням. Він підкреслив, що зовнішній контроль за заходами стеження може здійснюватися до реалізації цих заходів, під час їх реалізації або після їх завершення[31]. Останні етапи часто поєднують в один етап, що є відмінним від санкціонування заходів, пов'язаних із втручанням[32].

Що стосується санкціонування заходів стеження, то Суд чітко надав перевагу санкціонуванню стеження судовим органом, але не назвав це вимогою щодо дотримання статті 8[33]. Органи, покликані санкціонувати пов'язані із втручанням заходи, мають бути незалежними від відповідних служб і від виконавчої влади[34]. Суд дав зрозуміти, що ці запобіжні заходи різною мірою стосуються санкціонування цілеспрямованого і невибіркового стеження[35]. Оцінюючи, чи забезпечує даний орган або система достатній захист на етапі санкціонування, Суд може брати до уваги їх повноваження та компетенцію[36], а також кількість санкцій, що видаються щорічно[37].

---

31. Klass and Others v. Germany [54].
32. Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria [84]. Див. також: Cameron 2013: 170-171.
33. Klass and Others v. Germany [54] [56]; Kennedy v. the United Kingdom [167].
34. Dumitru Popescu v. Romania [72][73]; Klass and Others v. Germany [56].
35. Liberty and Others v. the United Kingdom [64].
36. Klass and Others v. Germany [56].
37. Lordachi and Others v. Moldova [51].

Європейський суд з прав людини також ухвалив рішення щодо правил подальшого контролю, зауваживши, що стаття 8 може бути порушена, якщо у ході подальшого розгляду заходів стеження, зберігання і знищення персональних даних службами безпеки не брав участі дійсно незалежний орган[38]. Повинна існувати чітка правова база, що визначає, як здійснюється такий контроль[39]. Нарешті, Суд визначив ряд додаткових характеристик контролюючих органів, пов'язаних з оцінкою того, чи забезпечують заходи з контролю достатній захист. Серед них – чи має контролер доступ до всіх відповідних документів (включаючи секретні матеріали); чи видаються публічні звіти (з відповідними обмеженнями для секретних матеріалів); і чи має контролюючий орган повноваження з анулювання санкції/ордеру на стеження та вимагати знищення отриманих матеріалів[40].

Окремо від Суду, у рішенні 2014 р., обов'язковому для 28 країн-учасниць Ради Європи, що є також членами ЄС, Велика судова палата ЄС указала, що для доступу державних органів до даних зв'язку потрібно:

«Попередній розгляд судом або незалежним адміністративним органом, рішення якого спрямовано на обмеження доступу до даних та їх використання лише тим, що необхідно для виконання поставленого завдання, який проводиться після обґрунтованого запиту цих органів, поданого в рамках процедур запобігання, виявлення або карного провадження»[41].

Слід зазначити, що це рішення було прийнято в конкретних умовах оцінки законності директиви ЄС про зберігання даних, що вимагала зберігання даних в основному для правоохоронних цілей. Крім того, національна безпека та діяльність служб безпеки значною мірою виходять за рамки законодавства ЄС. Проте рішення Судової палати Європейського Союзу чітко вказує, що є необхідним попереднє незалежне затвердження запитів на доступ до даних зв'язку, щоб реалізація таких повноважень відповідала праву на приватне життя. Майже напевно буде застосовуватися таке ж обґрунтування, як і під час розгляду аналогічних заходів, у т.ч. у зв'язку зі службами безпеки, відповідно до статті 8 ЄКПЛ.

Розслідування порушень прав людини та забезпечення ефективного правового захисту

Держави зобов'язані забезпечити можливість звернення людей за ефективним правовим захистом у разі порушення їх прав (Article 13 ECHR; Article 2(3) ICCPR; Articles 13 and 14 UNCAT). Це вочевидь стосується контролю за службами безпеки, оскільки один або кілька інститутів, відповідальних за контроль, повинні розслідувати обвинувачення в порушенні прав людини та забезпечу-

38. Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria [85] [87].
39. Lordachi and Others v. Moldova [49].
40. Kennedy v. the United Kingdom [166] [167].
41. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others [62].

вати ефективний правовий захист жертв. Важливість забезпечення ефективного правового захисту підтвердив Комітет ООН з прав людини, заявивши, що нерозслідування заяв про порушення прав людини саме по собі може бути порушенням МПГПП (Комітет ООН з прав людини 2004: § 15).

У світлі обвинувачень у катуваннях, UNCAT встановлює детальніші вимоги, включаючи «систематичний розгляд правил, інструкцій, методів і практик допиту, а також правил утримання під вартою та поводження з особами, підданими будь-якій формі арешту, затримання або ув'язнення», і проведення негайного розслідування обвинувачень у катуваннях[42].

У країнах, де службам безпеки дозволено допитувати та/або затримувати людей (або вони роблять це без правових підстав), ці зобов'язання навряд чи будуть дієвими.

Не вважається гарною практикою, коли служби безпеки мають повноваження щодо арешту, допиту та затримання, і застосування цих повноважень не повинне дозволятися, якщо служби не мають правоохоронних функцій. За будь-яких обставин, в яких служби користуються такими повноваженнями, вважається важливим, щоб вони підлягали тим же стандартам, що застосовуються до правоохоронних органів, що виконують ті ж функції[43].

Стаття 13 ЄКПЛ і практика її застосування накладають такі ж вимоги на розслідування й усунення порушень прав людини службами безпеки. Крім того, Суд ухвалив, що якщо у людини є аргументована претензія до служб безпеки (або будь-якого іншого державного органу) у зв'язку з порушенням статті 3 або 5, відповідну статтю слід читати разом зі статтею 13, щоб вимагати ефективного офіційного розслідування[44]. Це потребує серйозних зусиль для з'ясування того, що відбулося, вжиття усіх обґрунтованих заходів для збереження доказів, дозволу жертві фактично брати участь у розслідуванні та незалежності будь-якого розслідування від виконавчої влади[45].

Суд давно визнав, що концепція ефективного правового захисту не може мати такий же зміст при проведенні таємних заходів, пов'язаних із втручанням, оскільки ефективність таких заходів залежить від збереження їх в таємниці. Зважаючи на це, Суд погодився, що якщо таємні заходи стеження тривають або особі не може бути повідомлено про них на інших законних підставах, правовий захист повинен бути настільки дієвим, наскільки це можливо за даних обставин.[46] Однак Суд ухвалив, що той факт, що людину неможливо поінформувати про те, чи стежать за нею, не повинен перешкоджати можливості

42. Конвенція ООН проти катувань та інших жорстоких, нелюдських або таких, що принижують гідність, видів поводження і покарання, 10 грудня 1984 р. (уведена в дію 26 червня 1987 р.), Статті 11-12.
43. ООН 2010a: практичні методи 27-28; International Commission of Jurists 2009: 89.
44. Assenov and Others v. Bulgaria [102]; El Masri v. «the former Yugoslav Republic of Macedonia» [182] [242].
45. Assenov and Others v. Bulgaria [102-103]; El Masri v. «the former Yugoslav Republic of Macedonia» [182-184].
46. Klass and Others v. Germany [69].

подати скаргу до контролюючого органу. Такий орган повинен бути здатним провести розслідування, щоб гарантувати реалізацію всіх заходів відповідно до закону, не інформуючи скаржника[47]. Щойно людині стане відомо про заходи, внаслідок юридичної вимоги щодо його інформування або в інший спосіб, вона повинна мати право звернутися до органу, здатного забезпечити ефективний правовий захист. Суд підкреслив, що такий правовий захист повинен здійснюватися не тільки за законом, але й на практиці[48].

За аналогією з вимогами щодо контролю за заходами стеження (описаними вище), немає вимоги, щоб орган, відповідальний за розслідування скарг і забезпечення правового захисту, був судовим органом. Однак такі органи повинні мати достатні повноваження і процедурні гарантії для забезпечення ефективності правового захисту[49]. Зокрема, від того, чи має орган повноваження запроваджувати юридично обов'язкові заходи правового захисту (а не рекомендації), залежить оцінка його ефективності в контексті статті 13[50]. Повноваження давати розпорядження стосовно знищення файлів або зібраної інформації є важливою супутньою обставиною[51]. При оцінці наявності ефективного правового захисту можна брати до уваги сукупність наявних заходів правового захисту[52], які можуть надавати різні органи.

3.2. Необов'язкові рекомендації та принципи

Існує зростаючий масив актів міжнародного і європейського «м'якого права», що стосуються контролю за службами безпеки. Хоча обов'язкових принципів «твердого права», що стосуються контролю, відносно небагато, необов'язкові пропозиції і рекомендації формують детальну основу для систем розробки, посилення й оцінки контролю за службами безпеки. Багато документів, розглянуті в цьому розділі, мають велике значення, з огляду на те, що вони були видані серйозними міжнародними інститутами й засновані на існуючих гарних практиках, а не «мріях». У цьому розділі розглянуто ряд ключових положень та інновацій кожного набору принципів.

3.2.1. Спеціальні органи ООН і Верховний комісар з прав людини

У 2009 р. Рада ООН з прав людини доручила спеціальному доповідачу з питання заохочення та захисту прав людини при боротьбі з тероризмом підготувати «добірку оптимальних практичних методів, що застосовуються щодо законодавчої та інституціональної основи спеціальних служб і заходів з контролю за

47. Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria [100].
48. Segerstedt-Wiberg and Others v. Sweden [117]. Див. також: Venice Commission 2007: § 129.
49. Klass and Others v. Germany [67]; Segerstedt-Wiberg and Others v. Sweden [117]; Leander v. Sweden [83].
50. Leander v. Sweden [82].
51. Segerstedt-Wiberg and Others v. Sweden [120]; Kennedy v. the United Kingdom [167].
52. Klass and Others v. Germany [72]; Leander v. Sweden [77].

їх діяльністю» (Рада ООН з прав людини 2009; ООН 2010a). Вона була розроблена у ході консультацій з багатьма сторонами, включаючи колишніх керівників розвідок, правозахисників, з урахуванням думки урядів багатьох країн. Ці принципи згодом були схвалені Європейським парламентом і Парламентською асамблеєю Ради Європи.

Добірка ООН містить змістовні рекомендації з контролю, включаючи визнання важливості спеціального контролю (у цій доповіді він іменується експертним контролем), на додаток до парламентського, судового, виконавчого, внутрішнього контролю та контролю (*у вузькому значенні)*. У добірці також підкреслюється важливість існування контролюючого органу, чиї обов'язки включають перевірку використання персональних даних розвідувальними органами та отримання скарг з таких питань (ООН 2010a: практичні методи 25-26).

Не менш важливими є рекомендації щодо необхідності зосередитися на всебічній діяльності служб, причому контроль повинен охоплювати (як мінімум):

- відповідність закону;
- ефективність і дієвість їх діяльності;
- їх фінанси; та
- їх адміністративні практики (ООН 2010a: практичний метод 6).

Нарешті, рекомендації, щоб контролюючий орган міг контролювати співробітництво з іноземними розвідувальними службами та службами безпеки (включаючи договори про співробітництво), є важливими, беручи до уваги бурхливий розвиток співробітництва і наслідки такого співробітництва для прав людини (Born, Leigh and Wills, forthcoming).

У 2014 р. спеціальний доповідач ООН з прав людини та боротьби з тероризмом запропонував рекомендації з контролю за масовим стеженням, що включали наступне:

- незалежний контролюючий орган має отримати право санкціонувати стеження (у т.ч. масове стеження), беручи до уваги не лише національне законодавство, але й вимоги необхідності та пропорційності міжнародного правозахисного права;
- необхідність доступу окремих осіб до ефективного правового захисту у разі можливих порушень прав на приватне життя в Інтернеті. Підкреслюється, що органи, відповідальні за розгляд таких скарг, можуть мати різні форми, аби тільки вони мали доступ до всієї відповідної інформації, необхідні ресурси і могли давати розпорядження щодо обов'язкових заходів правового захисту (ООН 2014: §§ 48-50 and 61). Таке підтвердження того, що значення має зміст, а не форма контролюючих органів, є важливим для вироблення принципів застосування відносно країн з різними конституційними (правовими) системами – що збігається й з підходом, прийнятим у добірці ООН.

Рекомендації спеціального доповідача ООН з питань свободи слова 2013 р. ідуть далі, закликаючи до того, щоб стеження за лініями зв'язку здійснювали-

ся лише під контролем судового органу (ООН 2013: § 81). Це більше, ніж вимоги ЄКПЛ, вироблені на основі прецедентного права (див. вище). Франк Ла Рю (Frank La Rue) також рекомендував, щоб надання приватними компаніями даних зв'язку державним відомствам, включаючи служби безпеки, відслідковував незалежний контролюючий орган або суд (ООН 2013: § 86).

Верховний комісар ООН з прав людини у 2014 р. опублікував доповідь, в якій пропонувалося, щоб процес санкціонування включав «позиції захисту суспільних інтересів». Мова йде про адвокатів, призначених, щоб представляти інтереси майбутнього об'єкта стеження (Управління Верховного комісара ООН з прав людини 2014: § 38).

Генеральна Асамблея ООН

Генеральна Асамблея ООН у 2014 р. відреагувала на викриття Сноудена, закликавши держави, зокрема:

«заснувати нові або продовжувати використовувати вже наявні незалежні, ефективні, забезпечені належними ресурсами та неупереджені внутрішні механізми судового, адміністративного та/або парламентського контролю, здатні забезпечувати у відповідних випадках прозорість і підзвітність відносно спостереження держав за повідомленнями, їх перехоплення і збору особистих даних; надавати особам, чиє право на недоторканність особистого життя було порушено в результаті незаконного або довільного спостереження, доступ до ефективних засобів правового захисту відповідно до міжнародно-правових зобов'язань в галузі прав людини» (Генеральна Асамблея ООН 2014: § 4).

3.2.2. Венеціанська комісія Ради Європи

Венеціанська комісія Ради Європи зіграла провідну роль у забезпеченні демократичного контролю за службами безпеки. Доповідь Венеціанської комісії 1998 р. про служби внутрішньої безпеки була першим документом, підготовленим міжнародною організацією на цю тему (Venice Commission 1998). У всебічній доповіді 2007 р. Венеціанська комісія представила повний аналіз різних форм і моделей контролю. Доповідь містить докладний аналіз внутрішнього, парламентського, судового й експертного контролю.

Венеціанська комісія виявила необхідність ефективних заходів внутрішнього контролю в службах безпеки, включаючи контроль нижньої ланки керівництва, процедури обов'язкового затвердження на рівні керівництва запитів на надання дозволу щодо заходів, пов'язаних із втручанням, і навчання правам людини та демократичним цінностям (Venice Commission 2007: §§ 131-133). Стосовно парламентського контролю, Венеціанська комісія рекомендує, щоб: членів комітету обирав парламент (а не виконавча влада), були представлені різні партії і забезпечувалася підтримка досить кваліфікованим персоналом (там само, §§ 21, 24). Що стосується судового контролю, то Венеціанська комісія рекомендує спеціальну підготовку з питань безпеки та вивчення можливості призначення спеціальних адвокатів, що представляють інтереси май-

бутніх об'єктів стеження в контексті дозвільних процедур (там само, §§ 28, 31). Серед рекомендацій органам експертного контролю – призначати їх членів і приймати їх звіти парламентом (а не виконавчою владою), та уникати контролю уряду за звітами (там само, § 34).

Також рекомендовано відокремити функції розгляду скарг від функцій ширшого контролю (там само, § 247). Нарешті, у доповіді міститься важливе нагадування про те, що механізми контролю мають існувати не лише на папері – вони повинні реалізовуватися й аналізуватися (там само, § 260). Вказівки щодо того, яким чином проводити аналіз, не пропонуються.

У 2015 р. Венеціанська комісія оновила свою доповідь у світлі викриттів Сноудена (Venice Commission 2015). Доповідь містить детальні рекомендації стосовно обмежень і механізмів контролю, які можуть бути адаптовані для використання під час невибіркового стеження та використання метаданих. Венеціанська комісія підкреслила особливу необхідність введення обмежень на двох етапах:

- коли вибирають налаштування для визначення інформації, що відбирається з матеріалів, зібраних під час масового стеження. Хоча це може дозволити судовий орган, відповідно до рекомендації, із цим завданням найкраще може впоратися гібридний зовнішній орган, що складається з експертів і суддів, оскільки це включає не тільки правову оцінку, але й (зовнішньо)політичні і технічні міркування;
- коли аналітики ухвалюють рішення щодо того, чи потрібно зберігати інформацію, зібрану шляхом невибіркового стеження та відібрану за допомогою налаштувань – процес мінімізації.

Венеціанська комісія рекомендує, щоб за цією функцією надалі стежив зовнішній орган (Venice Commission 2015: §§ 46-48, 120-121).

Парламентська асамблея Ради Європи (ПАРЄ)

ПАРЄ також запропонувала принципи контролю за службами безпеки у формі резолюцій, рекомендацій і звітів комітетів. Їх можна сформулювати на основі роботи Комітету з правових питань і прав людини над таємними затриманнями, видачами, масовим стеженням і державною таємницею. Складаючись із парламентаріїв з 47 країн Європи, ПАРЄ природно зосередилася в своїх рекомендаціях на необхідності посилення парламентського контролю, порекомендувавши, зокрема, всім парламентам створити спеціальні комітети з питань контролю за службами безпеки[53].

Асамблея виявила особливу цікавість до доступу до інформації для спеціальних і постійних парламентських комітетів, підтвердивши необхідність доступу парламентських комітетів до всієї інформації, що стосується виконання їх функції, а також чітких слідчих повноважень для одержання таких матеріалів (ПАРЄ 2013: § 9). У недавньому проекті резолюції Комітет з правових питань і

53. ПАРЄ 2011: § 13; ПАРЄ 2005: § 10.i.b.

прав людини підкреслив необхідність наявності механізмів контролю для доступу (і права розгляду) до інформації, що стосується міжнародного співробітництва між службами безпеки (розвідувальними службами) безвідносно до принципу контролю джерела[54]. Це вкрай важливо з огляду на обсяг інформації, що одержується і передається закордонним партнерам[55].

Асамблея також рекомендувала країнам-учасницям розробити змагальні процедури для арбітражу у зв'язку із суперечками щодо публікації інформації парламентськими комітетами (і розслідування судовими органами справ, що стосуються служб безпеки) (ПАРЄ 2011: § 13). Цей специфічний аспект прозорості контролюючих органів не був охоплений іншими принципами і являє собою цінне доповнення, оскільки часто виникають ускладнення у зв'язку з тим, що може публікувати комітет з питань контролю і як повинні вирішуватися будь-які суперечки з виконавчою владою. Можливо, найінноваційнішою рекомендацією Асамблеї була її пропозиція 2005 р., щоб Комітет міністрів прийняв кодекс етики для служб безпеки на зразок Європейського кодексу поліцейської етики (ПАРЄ 2005: § 10.i.e). Хоча цю рекомендацію не було реалізовано, вона залишається важливим побажанням, до якого варто повернутися.

Колишній член ПАРЄ Дік Марті скористався своєю підсумковою доповіддю, щоб підтримати принципи, викладені у вищезгаданій добірці ООН (ООН 2010a) і в доповіді Венеціанської комісії про демократичний контроль за службами безпеки 2007 р. (Marty 2011: §§ 48-49). Марті також рекомендував надати контролюючим органам чіткі слідчі повноваження, що дозволили б їм перевіряти діяльність служб безпеки, навіть якщо уряд виступає проти такої перевірки. Крім того, він підкреслив часто згадувану важливість належного ресурсного забезпечення контролюючих органів та їх повної незалежності від виконавчої влади (Marty 2011: § 55).

Комісар з прав людини

Комісар з прав людини також давав рекомендації щодо контролю за службами безпеки у відповідь на викриття масового стеження.

Він підкреслював важливість формування культури поваги до прав людини та верховенства права в службах безпеки для створення ефективної системи демократичного контролю (Commissioner for Human Rights 2014a: 22). Це пов'язано з необхідністю зосередитися на внутрішньому управлінні і контролі, як підкреслила Венеціанська комісія. Комісар також використав свої візити в різні країни для того, щоб дати рекомендації, включаючи заяви про те, що правова база з питань контролю за службами безпеки повинна охоплювати нові технології стеження (Commissioner for Human Rights 2014c: 71-72). Ця рекомендація є особливо актуальною, оскільки одна із причин, чому деякі контр-

54. Відповідно до цього принципу служба, від якої виходить інформація, має право визначати, кому передавати цю інформацію.

55. Omtzigt 2015; LAHRC 2015: § 17.2.

олюючі органи прагнули розв'язати проблеми, створені масовим стеженням і хакерством, полягає в тому, що вони не мають техніки для контролю за діяльністю служб безпеки із застосуванням нових технологій.

Генеральний секретар

Зусилля інститутів Ради Європи доповнив колишній генеральний секретар Ради Європи Террі Девіс (Terry Davis), що також дав рекомендації щодо контролю в 2006 р. Це відбулося після повідомлень про таємні затримання та видачі в Європі. Девіс підкреслив недостатність перевірки діяльності іноземних служб (на території країн-учасниць Ради Європи) контролюючими органами[56]. Хоча він не вдавався в деталі, яким чином це потрібно робити, цей бік контролю раніше не охоплювався іншими рекомендаціями і принципами.

3.2.3. Європарламент Європейського Союзу

У своїй доповіді про масове стеження 2014 р. (European Parliament 2014: §§ 74-79) комітет Європарламенту з питань громадянських свобод, правосуддя і внутрішніх справ (Комітет LIBE) запропонував рекомендації щодо контролю на національному рівні (European Parliament 2007). Комітет закликав, за його словами, до «змістовного контролю», здійснюваному парламентським та/або експертним органом контролю. Таке визнання експертного контролю підтверджує зрушення в напрямку більш плюралістичного розуміння контролю – не тільки парламентського і судового. Ураховуючи проблеми, що супроводжують контроль за масовим стеженням за електронними засобами зв'язку, комітет підкреслив необхідність надання контролерам достатніх технічних можливостей, знань і ресурсів. У цьому зв'язку учасники закликали надати контролюючим органам повноваження відвідувати об'єкти для розслідування.

Комітет Європарламенту з питань громадянських свобод, правосуддя і внутрішніх справ також рекомендував, щоб контролюючі органи зверталися до громадськості у формі звітів. Це має особливе значення, оскільки контролери покликані відігравати ключову роль у роз'ясненні роботи служб громадськості і, де це необхідно, зміцненні суспільної довіри. Нарешті, що стосується контролю за стеженням, парламентарії підкреслили, зокрема, необхідність як попереднього, так і подальшого контролю; це відповідає підходу Суду (European Parliament 2014).

Узагальнюючи все це, Комітет з питань громадянських свобод, правосуддя і внутрішніх справ закликав утворити групу високого рівня для розробки в ЄС мінімальних стандартів щодо контролю на основі принципів і кращого досвіду, запропонованих ООН і Радою Європи (European Parliament 2014: § 77). На момент написання нових повідомлень щодо цього не було.

56. Council of Europe 2006a: § 101(iv); Council of Europe 2006b: §§ 46 and 68.

«Робоча група щодо статті 29»

Також під егідою Європейського Союзу «Робоча група щодо статті 29» у складі представників національних комісій із захисту даних у 2014 р. прийняла декларацію європейських цінностей щодо захисту персональних даних у контексті стеження силами національної безпеки. Декларація містить заклик до незалежного й ефективного контролю за стеженням, включаючи реальну участь національних органів захисту даних (DPA) (European Data Protection Authorities 2014: § 8). Раніше Робоча група рекомендувала, щоб у державах, де над використанням захисту даних службами безпеки контроль здійснює національний орган з питань захисту даних, відмінний від контролюючого органу, були «регулярні контакти між цим органом і національним органом з питань захисту даних для забезпечення однакового та узгодженого застосування принципів захисту даних» (Article 29 2014a: § 8). Це важливо, оскільки в багатьох країнах-учасницях Ради Європи органи захисту даних не допускаються до контролю за службами безпеки (див. нижче), тому їх досвід захисту не використовується у сфері, в якій захист даних є досить складним.

Який би орган не відповідав за контроль за використання персональних даних, «Робоча група щодо статті 29» підкреслила необхідність надання їм обом дозволу вивчати питання за власною ініціативою й реагувати на скарги, а також мати повноваження реалізовувати свої рішення (Article 29 2014a: § 8, Recommendation B2). Нарешті, «Робоча група щодо статті 29» рекомендувала систематизувати і зберігати персональні дані так, щоб це спрощувало незалежний контроль (Article 29 2014b: § 11). Тим самим визнається, що ефективний контроль залежить не лише від повноважень і ресурсів контролюючих органів, але й від того, яким чином такі інститути, як служби безпеки, можуть сприяти контролю та підзвітності під час ведення даних.

3.2.4. Ініціативи громадянського суспільства

Ініціативи громадянського суспільства привели до розробки ряду важливих наборів міжнародних принципів з питань контролю за службами безпеки.

Принципи Цване

Глобальні принципи національної безпеки і права на інформацію (Принципи Цване, Global Principles on National Security and the Right to Information, Tshwane Principles) були розроблені в 2013 р. за участі більш ніж 500 експертів з усього світу, включаючи численних фахівців у сфері безпеки, під егідою Правової ініціативи відкритого суспільства (*Open Society Justice Initiative*, Open Society Foundations 2013). Принципи Цване містять докладні вказівки щодо доступу до інформації для органів, що здійснюють контроль за сферою безпеки, включаючи служби безпеки. Починаючи із принципу, що контролери повинні мати доступ до всієї інформації, необхідної для виконання їх законних обов'язків, принципи містять докладні вказівки про: види інформації (матеріалів), до яких контролери повинні мати доступ; слідчі повноваження, фінансові і людські ресурси, необхідні для забезпечення такого доступу та належного ви-

користання інформації; та заходи із захисту інформації, що підлягає контролю (Open Society Foundations 2013: Principles 32, 33, 35). Принципи Цване також містять докладні вказівки стосовно звітності і сфери діяльності контролюючих органів, включаючи потребу в публічних версіях доповідей і механізми забезпечення публічного доступу до процедури розгляду скарг (Open Society Foundations 2013: Principle 34).

Принципи Цване найбільш відомі завдяки їхнім детальним рекомендаціям щодо публічного доступу до інформації органів влади, включаючи служби безпеки та їх органи контролю. Особливу важливість для неформального контролю за службами безпеки, зокрема, з боку ЗМІ та НУО, мають такі вказівки:

- органи влади повинні надавати інформацію на запит, за винятком обмежень, регламентованих законом і необхідних для запобігання конкретній шкоди, що підлягає визначенню, законним інтересам, у т.ч. національній безпеці;
- не можна вводити обмеження на право на інформацію, виходячи з міркувань національної безпеки, якщо уряди не можуть підтвердити, що обмеження визначені законом і є необхідними в демократичному суспільстві для захисту законних інтересів національної безпеки;
- недостатньо, щоб орган влади просто вважав, що існує ризик шкоди; влада повинна вказати конкретні, ґрунтовні причини щодо підтвердження своєї позиції;
- особа або організація, що запитують інформацію, мають право на швидкий і недорогий розгляд незалежним органом відмови в наданні інформації або питань, пов'язаних із запитом (Open Society Foundations 2013: Principles 1-5, 26).

Хоча Принципи Цване є продуктом громадянського суспільства, можна сказати, що вони мають чималу вагу в Європі, оскільки вони були підтримані в резолюції ПАРЄ, і Європарламент також високо оцінив ці принципи[57].

Оттавські принципи

Оттавські принципи щодо боротьби з тероризмом і прав людини (Ottawa Principles on Anti-terrorism and Human Rights*)* були розроблені групою експертів з прав людини та боротьби з тероризмом у 2006 р.

Ці принципи закликають до плюралістичного підходу до контролю за службами безпеки, включаючи заходи внутрішнього контролю в службах безпеки; виконавчу владу; незалежний орган контролю; законодавчу владу; судову перевірку; інститути прав людини, захисту даних, свободи інформації та аудиту; і громадянське суспільство (Ottawa Principles 2006: 9.1.1).

Особливо корисним є перерахування в Оттавських принципах завдань системи контролю, серед яких – забезпечення правомірності; ефективності; прозо-

57. ПАРЄ 2013: §§ 7-8; European Parliament 2014, § 77.

рості; легітимності й підзвітності діяльності служб безпеки (Ottawa Principles 2006: 9.1.2).

Оттавські принципи розглядають незалежний орган розгляду (тобто експертний непарламентський інститут) як центральний елемент системи контролю. Вони пропонують, щоб такий орган як мінімум розглядав правомірність (законність) діяльності служб безпеки і мав повноваження щодо розгляду скарг (Ottawa Principles 2006: 9.3). Як і в багатьох інших рекомендаціях, ці принципи також підкреслюють необхідність наявності у контролерів належних ресурсів, доступу до інформації та слідчих повноважень, а також видання публічних звітів (Ottawa Principles 2006: 9.1.5, 9.3.3.b, d).

Принципи необхідності і пропорційності

Міжнародні принципи застосування прав людини під час спостереження за лініями зв'язку (*International Principles on the Application of Human Rights to Communications Surveillance*) 2013 р., розроблені провідними експертами в галузі приватного життя та безпеки і підтримані більш ніж 400 НУО та науковими установами, дають рекомендації із застосування існуючих міжнародних правових стандартів до цифрового спостереження. Важливим доповненням до лексикону міжнародних принципів контролю за службами безпеки є заклик надати незалежному контролюючому органу право «оцінювати, чи публікує держава повну й точну інформацію про використання та масштаб методів і повноважень із спостереження за лініями зв'язку відповідно до зобов'язань щодо прозорості …, і публікувати періодичні доповіді й іншу інформацію, що стосується спостереження за лініями зв'язку»[58]. Тим самим визнано, що контролюючі органи повинні відігравати важливу роль у забезпеченні більшої прозорості служб безпеки, що є важливим для формування (відновлення) довіри до служб безпеки.

58. https://en.necessaryandproportionate.org/text, Principle 10.

Розділ 4

НАЦІОНАЛЬНІ ПРАКТИКИ КРАЇН-ЧЛЕНІВ РАДИ ЄВРОПИ

Країни-учасниці Ради Європи практикують різні підходи до структури і здійснення контролю за своїми службами безпеки. У цій главі буде розглянуто національні підходи до контролю з боку: (i) парламентських комітетів; (ii) інститутів незалежного контролю, включаючи органи експертного контролю за безпекою (розвідкою) та інститути, що мають ширшу юрисдикцію, такі як омбудсмени й уповноважені з питань даних (інформації); а також (iii) судових органів, включаючи квазісудові органи. Менше уваги буде приділено ролі політичної виконавчої влади та механізмів внутрішнього контролю служб безпеки. Ця глава закінчується рядом прикладів, що показують роль неформальних контролерів: громадянського суспільства та ЗМІ.

Про розгляд скарг, що стосуються служб безпеки, мова йде в кількох главах, оскільки країни-учасниці Ради Європи наділили цими функціями різні контролюючі органи. Хоча в контексті контролю за службами безпеки важливими є спеціальні запити, у цьому документі розглядаються тільки постійні контролюючі органи, що працюють на регулярній основі. Замість розгляду цілісних національних систем контролю, взято приклади із систем різних країн. Це зроблено для того, щоб підкреслити різницю в підходах і гарному досвіді.

У жодній з країн-учасниць Ради Європи система контролю не відповідає всім міжнародно й регіонально визнаним принципам і гарному досвідові, що розглядаються у Главі 5. Також варто підкреслити, що не існує одного, найкращого підходу до організації системи контролю за службами безпеки. Різні конституційні норми, правові та політичні системи, історичні ситуації обумовлюють різні підходи на території Ради Європи. Відповідно необхідно з обережністю підходити до огульного запозичення або копіювання досвіду інших країн. Разом з тим немає сумніву, що існують моделі і досвід, які можна вважати ефективнішими для захисту прав людини у ході діяльності служб безпеки. Ці приклади буде розглянуто в цій главі.

4.1. Парламентські комітети

У більшості країн-учасниць Ради Європи або створено парламентський комітет (підкомітет) з питань контролю за службами безпеки (як в Італії, Німеччині, Польщі), або ці функції надано комітету з ширшими повноваженнями, наприклад, внутрішніх справ, національної безпеки чи оборони (як у Грузії та Чорногорії). Багато парламентських комітетів також можуть мати законодавчі функції, але вони перебувають за межами цієї доповіді.

На території Ради Європи спостерігається тенденція доручати парламентський контроль за службами безпеки одному комітету, що займається лише контролем над службами безпеки. У деяких державах створено кілька комітетів з питань контролю, кожен з яких відповідає за конкретну службу безпеки. Наприклад, у парламенті Румунії є окремі комітети з контролю за службою внутрішньої безпеки і службою зовнішньої розвідки, а також комітет з питань оборони, чиї обов'язки включають певні аспекти роботи обох служб. Так само виглядає ситуація в Словаччині, де є окремі комітети з питань контролю за Словацькою інформаційною службою і Бюро національної безпеки. Такий поділ праці може забезпечити вищий рівень спеціалізації та зосередження досвіду членів комітетів.

З іншого боку, недоліки такого підходу містять ризик того, що деякі питання (наприклад, обміну інформацією між двома службами безпеки/розвідувальними службами) можуть перебувати на стику повноважень двох або декількох комітетів (Venice Commission 2007: § 154), і ресурси можна буде вигідніше концентрувати на розвитку одного комітету.

Повноваження і сфера контролю

У більшості країн-учасниць Ради Європи повноваження комітетів парламентського контролю сформульовано нечітко, внаслідок чого комітет може контролювати (відслідковувати, перевіряти) тільки визначені служби безпеки. Наприклад, у Франції парламентська делегація з питань розвідки (*Délégation Parlementaire au Renseignement*) має завдання з контролю за «загальною діяльністю і методами» різних розвідувальних служб і служб безпеки. У Німеччині орган парламентського контролю (*Parlamentarische Kontrollgremium*) має завдання з контролю за «діяльністю» служб безпеки та розвідувальних служб[59].

Більшість комітетів парламентського контролю займається різними питаннями, включаючи політику, фінанси та керівництво службами, а також деякими аспектами проведених операцій (Wills and Vermeulen 2011: 92-95, 102-110, 115-116). Перевірка дотримання закону – постійне завдання, що є в усіх цих сферах. Однак деякі парламентські комітети, наприклад, комітет парламентського контролю за розвідувальними операціями литовського Сейму, мають

59. France 2007: Section 1.

спеціальні повноваження з перевірки дотримання службами безпеки конституційних прав і свобод (на додаток до інших питань)[60].

Хоча «глибина» контролю різних парламентських комітетів є різною, природа цих органів є такою, що більшість із них не в змозі здійснювати регулярний, детальний контроль за оперативною діяльністю, включаючи збір, обмін і використання персональних даних. Такий моніторинг усе більше здійснюють непарламентські незалежні контролюючі органи.

Головна причина полягає в тому, що такого роду перевірка займає дуже багато часу, є досить специфічною і вимагає ресурсів. Тому деякі країни-учасниці Ради Європи воліють доповнювати парламентський контроль детальнішою постійною перевіркою оперативної діяльності і, особливо, використання та поводження з персональними даними (див. нижче).

Що стосується тимчасових аспектів контролю, парламентські комітети європейський країн здійснюють контроль майже виключно постфактум, розглядаючи те, що вже відбулося. Немає аналога американської практики – попередньо інформувати обраних членів комітетів конгресу з питань розвідки про конкретні операції або програми. З погляду прав людини та підзвітності є небажаним залучати контролюючі органи заздалегідь, ураховуючи, що їм, можливо, доведеться розглядати цю діяльність й у подальшому – при цьому може виникнути конфлікт інтересів.

Розгляд скарг

Деякі парламентські комітети з питань контролю (наприклад, у Польщі, Угорщині й Словаччині) також зобов'язані розглядати скарги на служби безпеки[61]. Однак вони навряд чи є здатними забезпечити ефективний правовий захист, як того вимагає ЄКПЛ, оскільки вони, як правило, не можуть давати обов'язкових для виконання розпоряджень. Може також виникати питання, чи здатні політичні органи забезпечити неупереджене розслідування скарг на порушення прав людини. Існує явний ризик того, що розгляд скарг може бути політизовано і що скаржники не зможуть домогтися задоволення через прагнення правлячих партій вигородити колег у політичному керівництві.

Відносини з органами експертного контролю

Комітети парламентського контролю також можуть відігравати важливу роль у моніторингу роботи органів експертного контролю (див. нижче); іншими словами, у контролі над контролерами. Ця роль може включати: постановку органам експертного контролю завдань щодо розгляду питань, на вивчення яких у

60. Lithuania 2002: Article 23.

61. Докладніше див.: Forcese 2012: 189-190.

парламентських комітетів може не вистачати часу, ресурсів або знань[62]; оцінку їх ефективності; призначення членів цих органів; забезпечення наявності у них належних повноважень і ресурсів; проведення заслуховування їх звітів і реалізацію (або забезпечення реалізації виконавчою владою) рекомендацій, запропонованих цими органами. У Норвегії, наприклад, цю роль виконує Постійний комітет Стортингу з контролю та конституційних питань (*Kontroll- og konstitusjonskomité*)[63], а в Нідерландах – Комітет з питань розвідки та безпеки другої палати, спеціальний парламентський комітет у складі керівників політичних партій у палаті (Verhoeven 2011: 254-255).

Доступ комітетів парламентського контролю до секретної інформації

Всі комітети парламентського контролю мають певний доступ до секретної інформації, і в більшості випадків їх доступ є ширшим, ніж у будь-якого іншого члена парламенту (Wills and Vermeulen 2011: 117-121). Хоча потреби будь-якого контролюючого органу в точній інформації визначає його мандат, гарна практика комітетів парламентського контролю передбачає доступ до всієї інформації, яку вони вважають необхідною для виконання їх функцій, а обмеження (якщо вони є) повинні бути визначені якомога вужче. Спільний постійний комітет зі здійснення парламентського контролю за румунської розвідувальною службою (внутрішня служба безпеки) у Румунії і Комітет з питань національної безпеки Латвії є прикладами контролюючих комітетів, що мають необмежений доступ до інформації[64]. Крім того, є корисним, коли доступ комітетів парламентських контролю до інформації підкріплений обов'язком з попереднього надання інформації з боку служб безпеки та/або виконавчої влади.

Особливо важливими для захисту прав людини є вимоги щодо попереднього надання інформації про діяльність, що впливає на право на приватне життя. Прекрасним прикладом цього є Німеччина, де федеральний уряд зобов'язаний кожні шість місяців передавати контрольному органу Бундестагу список виконаних заходів стеження, запитів інформації у приватних компаній, тривожних оповіщень у рамках Шенгенської угоди, введених до поліцейської інформаційної системи, і персональних даних, переданих іноземним органам[65].

У деяких країнах-учасницях Ради Європи є побоювання щодо надання допуску парламентаріям, включаючи членів комітетів парламентського

62. Наприклад, після викриттів Сноудена парламент Нідерландів зажадав, щоб голландський Комітет з питань контролю за службами розвідки і безпеки (CTIVD) розглянув, зокрема, масовий збір даних голландськими службами і його наслідки для прав людини: CTIVD 2014: 1.
63. Докладніше: Norway 2014: 5.
64. Див. Wills and Vermeulen 2011: 128-129. У Румунії є обмеження на інформацію про майбутні і поточні операції.
65. Germany 2001a: Section 14(1); Germany 1990b: Sections 8(a)(g), 17(3), 18(1)(a). Див. також: With and Kathmann 2011: 219-220.

контролю, до особливо делікатної інформації, особливо інформації про операції служб безпеки.

Такі побоювання є найпоширенішими у поставторитарних країнах і країнах, у парламентах яких представлені сепаратистські політичні партії. Щоб розвіяти ці побоювання, було розроблено різні механізми, найпоширенішим з яких є вимога щодо перевірки членів комітетів парламентського контролю й одержання ними допуску до того, як стати членом комітету.

Ця практика є неоднозначною, з ряду причин. По-перше, службам безпеки, можливо, доведеться перевіряти своїх майбутніх контролерів, що ставить ці служби (а отже й виконавчу владу) у становище, коли вони де-факто отримують право ветувати членів комітетів парламентського контролю. Таку ситуацію може бути використано, наприклад, задля недопущення призначення потенційно критично налаштованого члена парламенту до контролюючого комітету. По-друге, виникає більш широке питання щодо розподілу влади через те, що виконавча влада отримує можливість впливати або обмежувати роботу членів парламенту, обраних виборцями, через процедуру допуску. Якщо необхідна перевірка членів парламенту, гарною практикою може вважатися рекомендаційний характер доповіді служб безпеки про перевірку, у той час як остаточне рішення про призначення парламентарія до контролюючого комітету з приймається парламентом.

Наприклад, в Угорщині парламентський комітет з питань національної безпеки приймає остаточне рішення, чи буде призначено члена парламенту до складу комітету, незалежно від результатів перевірки (Foldvary 2011: 231). Нарешті, процедура перевірки неминуче вимагає, щоб служби безпеки прагнули одержати делікатні персональні дані від усіх і про всіх членів парламенту. Можуть виникнути питання про те, як надалі може бути використана така інформація, особливо в ситуаціях, коли служби безпеки або політична виконавча влада незадоволені підходом того або іншого члена контролюючого комітету.

У різних країнах-учасницях Ради Європи існують альтернативи перевірці. У Німеччині й Іспанії затверджено заходи з добору членів комітетів парламентського контролю, покликані забезпечити призначення і доступ до секретної інформації тільки парламентаріїв, здатних заручатися підтримкою (довірою) законодавчого органу. В обох країнах імовірний член комітету парламентського контролю повинен одержати підтримку кваліфікованої більшості парламенту для призначення в комітет[66]. Після одержання такої підтримки вже немає вимоги щодо отримання допуску.

В інших країнах побоювання з приводу захисту інформації намагалися вирішити, вимагаючи, щоб комітети парламентського контролю могли одержувати доступ тільки до деяких категорій секретної інформації, якщо вони проголосують за це кваліфікованою більшістю. Наприклад, члени комітету з питань безпеки республіки в італійському парламенті можуть більшістю у дві третини проголосувати за скасування будь-яких обмежень щодо державної таємниці,

66. Sanchez Ferro 2011: 269; With and Kathmann 2011: 219.

які в іншому разі не дозволяли б їхній доступ до оперативної інформації при розслідуванні порушень з боку офіцерів розвідки (Italy 2007: Article 31(9)). Аналогічним чином, комітет з питань національної безпеки парламенту Угорщини (члени якого теж повинні мати допуск), як правило, не мають доступу до найбільш критичної інформації про оперативні методи, але можуть проголосувати більшістю у дві третини за скасування цього обмеження для того або іншого розслідування (Hungary 1995: Section 16(2)). Хоча такі заходи можуть не дозволити ненадійним членам комітету самостійно «вивуджувати» інформацію, існує реальний ризик того, що правлячі партії можуть використати свої позиції в контролюючих комітетах, щоб блокувати доступ до найбільш важливих видів інформації й у такий спосіб перешкодити розслідуванню діяльності.

Переваги і недоліки парламентського контролю

Головні переваги парламентського контролю за службами безпеки можна узагальнити таким чином. По-перше, будучи обраними представниками, контролери користуються демократичною легітимністю, перевіряючи служби безпеки від імені тих, хто їх обрав.

По-друге, парламенти мають важелі щодо затвердження бюджету законодавцями та, іноді, повноваження з розподілу бюджету, якими можна скористатися для того, щоб виконавча влада і служби безпеки змінили свою політику або практику, що порушують права людини.

Нарешті, парламентарії в цілому мають найкращі позиції для контролю за роллю виконавчої влади в управлінні та контролі над службами безпеки, оскільки в більшості країн-учасниць Ради Європи парламент має конституційний обов'язок і право притягати виконавчу владу до відповідальності.

Існує й ряд недоліків, пов'язаних з парламентським контролем[67].

Головний недолік полягає в тому, що члени парламентських комітетів можуть одночасно мати багато обов'язків, і їм може бути важко приділяти достатньо уваги контролю за службами безпеки. Це впливає на здатність комітетів парламентського контролю здійснювати глибоку перевірку діяльності служб безпеки, що є вкрай необхідним для контролю за законністю оперативної діяльності. Друга, пов'язана з ним риса парламентського контролю, – те, що в більшості випадків парламентарії не мають знань про служби безпеки. Це посилюється нестачею часу і, у багатьох країнах, коротким терміном перебування у комітеті, що не дає змоги набути досвіду.

Цей недолік посилюється тим, що служби безпеки розширюють використання складних технологій, які необхідно чітко розуміти для повної оцінки наслідків для прав людини.

Найістотнішим недоліком парламентського контролю з погляду захисту прав людини – є те, що перевірці служб безпеки може зашкодити політизація контр-

67. Докладніше див.: Wills and Vermeulen 2011: 88-89; і Farson 2012: 38-40.

олюючих комітетів[68]. Парламентарії не завжди підходять для вирішення завдань щодо неупередженої перевірки додержання закону службами безпеки. Партійно-політичні міркування можуть спонукати парламентських контролерів або захистити служби безпеки і політичну виконавчу владу від критичної перевірки, або здійснювати контроль так, щоб завдати максимальної політичної шкоди опонентам, замість забезпечення законності (і ефективності) діяльності служб безпеки. Навіть якщо контролюючі комітети очолюють члени опозиції, правлячі партії потенційно можуть використати більшість у таких комітетах, щоб обмежити перевірку тих аспектів діяльності служб безпеки, які можуть бути політично невигідними. Це є вкрай проблематичним у країнах, де служби безпеки, як і раніше, використовуються і розглядаються як інструменти правлячих політичних партій (фігур).

Оцінка додержання закону не є тією сферою контролю, що повинна служити партійній політиці, і навіть пошук політичного компромісу в таких комітетах може зашкодити ефективному захисту прав людини[69].

Інші зацікавлені парламентські комітети

Хоча в цій главі розглядаються контролюючі комітети як такі, слід зазначити, що в деяких країнах утворено комітети (підкомітети) з вузькими повноваженнями для контролю за окремими сторонами діяльності служб безпеки. Серед прикладів – комітет з таємних фондів іспанських Кортесів і конфіденційний комітет німецького Бундестагу. Обидва відповідають за перевірку бюджету (фінансування) служб безпеки[70]. Хоча може здаватися, що такий бюджетний контроль прямо не пов'язаний із захистом прав людини, існує важливий взаємозв'язок, оскільки фінансові практики часто вказують на правомірність програм або операцій у цілому.

Діяльність, що порушує права людини, часто залишає фінансові сліди, аналіз яких може розкрити інформацію про таку діяльність.

Крім цих комітетів з вузькими повноваженнями, у багатьох парламентах є й інші комітети, чиї повноваження охоплюють різні аспекти політики або діяльності служб безпеки. Гарним прикладом є робота спільного комітету з прав людини британського парламенту. Комітет, зокрема, розглядав політику служби безпеки в контексті більш широкого тематичного вивчення або законодавчої перевірки таких аспектів, як боротьба з тероризмом, використання закритих матеріалів у судах і зобов'язання щодо прав людини у відносинах з іноземними державами з незадовільним станом прав людини[71]. Головне обмеження контролю цих «загальних» комітетів полягає в тому, що в багатьох випадках вони не мають таких прав з доступу до інформації, як спеціалізова-

68. Див., наприклад: Marty 2011: § 45.
69. Commissioner for Human Rights 2013a: §12; Управління Верховного комісара ООН з прав людини 2014: § 38.
70. Докладніше див.: Wills 2012a: 163-164; Sanchez Ferro 2011: 271.
71. Див.: www.parliament.uk/business/committees/committees-a-z/joint-select/human-rights-committee/, accessed 28 March 2015.

ні контролюючі комітети, а крім того, їм може не вистачати знань комітетів з контролю в сфері безпеки.

4.2. Інститути незалежного контролю

Органи експертного контролю за безпекою/розвідкою

Органи експертного контролю – це непарламентські органи, що створюються спеціально для контролю за службами безпеки. Визнаючи цінність постійного експертного позапартійного контролю, усе більше країн-учасниць Ради Європи створюють органи експертного контролю в сфері безпеки/ розвідки. Такі органи зазвичай уповноважені розглядати насамперед законність діяльності і політики служб безпеки, включаючи дотримання ними правозахисного права. Наприклад, такою є ситуація в Норвегії, Нідерландах і Португалії[72]. Однак існують й винятки з цього правила, наприклад, постійний комітет з питань контролю за розвідувальними службами (1-й комітет) у Бельгії, що має дуже широкі повноваження, які охоплюють у тому числі ефективність діяльності служб безпеки і координацію між службами безпеки[73]. На відміну від їх парламентських колег, органи експертного контролю в основному або повністю зосереджені на службах безпеки, а не на керівництві виконавчої влади цими службами.

На відміну від комітетів парламентського контролю, експертні органи працюють на (практично) постійній основі. Загалом це означає, що вони здатні забезпечити більш повну й глибоку перевірку, ніж їх парламентські колеги.

Постійний і безперервний контроль є особливо важливим для моніторингу законності роботи служб безпеки, оскільки зазвичай це є складною і кропіткою роботою, що забирає багато часу. Там, де існують органи експертного контролю, вони в основному займаються повсякденною перевіркою служб безпеки і є головним елементом зовнішнього контролю за службами безпеки, наприклад, у Нідерландах, Бельгії, Хорватії, Норвегії, Швеції й Португалії[74].

Склад

Органи експертного контролю зазвичай мають від одного до п'яти членів, серед яких завжди є люди з юридичними (судовими) знаннями. У багатьох випадках їх члени є колишніми суддями, прокурорами та політиками. Цих людей як правило перевіряють і дають їм найвищий рівень допуску. Однією з важливих переваг підходу органу експертного контролю полягає в тому, що контролерів можуть (у теорії, хоча не завжди на практиці) обирати, виходячи з їх знань і досвіду. У комітетах парламентського контролю ситуація є зазвичай іншою.

72. Portugal 2004: Article 9(1); Norway 1995: s2; Netherlands 2002: Article 64(2).
73. Belgium 1991: Article 33; див. також: http://comiteri.be/images/pdf/engels/w.toezicht%20-%20l.control.pdf; Committee I's website: http://comiteri.be/, both accessed 28 March 2015.
74. Portugal: www.cfsirp.pt/; докладніше див.: www.ennir.be/portugal/intelligence-review-portugal-0, both accessed 28 March 2015.

Статут або прийнята практика можуть вимагати, щоб до комітету входили люди з певними знаннями й досвідом. Наприклад, у Нідерландах комітет з контролю за службами розвідки і безпеки (CTIVD) виробив практику включення до свого складу колишнього співробітника правоохоронних органів і двох членів з юридичною підготовкою[75]. Визнаючи політичний характер діяльності контролю і розвідки, деякі експертні органи, наприклад, комітет з контролю за службами розвідки, спостереження та безпеки (*EOS-Utvalget*) у Норвегії, включають колишніх парламентаріїв і міністрів, поряд із правознавцями. У Хорватії прийнятий особливо передовий підхід – їх Рада з питань цивільного контролю за службами безпеки і розвідки повинна включати членів, які мають наукову підготовку з політології, права й електроніки[76]. Серед членів цього органу були чільні фігури громадянського суспільства та правозахисники. Залучення до процесу контролю людей з різним досвідом забезпечує представництво конкуруючих і критичних позицій, що своєю чергою може сприяти довірі суспільства до органів контролю[77].

Експертні органи можуть призначатися парламентом (наприклад, норвезький комітет EOS-Utvalget і Рада з питань контролю за системами інформації Португальської Республіки), виконавчою владою (наприклад, уповноважений з розвідувальних служб Великобританії та Комісія з безпеки і захисту інформації Швеції) або ними обома (як голландський CTIVD). Оскільки члени органів експертного контролю не засідають у парламенті, іноді вважають, що цим інститутам не вистачає демократичної легітимності. Щоб розвіяти такі побоювання і переконати громадськість у незалежності органів експертного контролю від виконавчої влади, може бути доцільним задіяти парламент до вибору й призначення їх членів. Такий зв'язок із законодавчим органом можна ще більше зміцнити їх звітністю безпосередньо перед відповідним комітетом парламенту, як це відбувається в Бельгії, де роботу 1-го комітету контролює комітет палати представників.

Сфера їх діяльності

Органи експертного контролю, як правило, мають право перевіряти законність діяльності служб безпеки, включаючи збір і використання персональних даних службами безпеки.

Повна оцінка дотримання прав людини вимагає перевірки:

- дозволу на збір даних;
- самого процесу збору (включаючи дотримання всіх ордерів);
- повторного дозволу на проведення заходів;
- зберігання, використання і передачі даних службами безпеки;

75. CTIVD website: www.ctivd.nl/?English, accessed 28 March 2015.
76. Croatia 2006: Article 110(2); докладніше див.: Cvrtila 2012.
77. Див., наприклад, коментарі колишнього керівника британської розвідувальної служби SIS: (Norton-Taylor 2015).

- вимог щодо мінімізації та/або видалення отриманих даних (особливо шляхом невибіркового спостереження); та
- дотримання всіх вимог стосовно інформування людей про спостереження за ними (якщо такі вимоги можуть бути застосовані).

Прикладами органів експертного контролю, повноваження яких охоплюють широкий спектр діяльності служб безпеки, пов'язаної з персональними даними, є німецька комісія G10, голландський CTIVD і Комісія з безпеки та захисту інформації Швеції (SIN)[78]. Деякі органи експертного контролю, навпаки, мають більш вузькі повноваження, зосереджуючи увагу на окремих аспектах збору та використання даних. Наприклад, у Великобританії уповноважений з питань перехоплення ліній зв'язку та уповноважений з питань розвідувальних служб займаються в основному процесом надання дозволу. Інспекція військової розвідки Швеції стежить за перехопленням міжнародних ліній зв'язку, а також якістю й мінімізацією даних, зібраних у ході такого перехоплення[79].

Доступ до інформації та слідчі повноваження

У різних країнах-учасницях Ради Європи закон вимагає, щоб органи експертного контролю мали повні права доступу до інформації, яку вони можуть вважати такою, що входить до їх повноважень, незалежно від джерел такої інформації[80].

Ураховуючи обсяг інформації, одержуваної від іноземних органів, важливо, щоб доступ органів контролю не обмежувався інформацією, яка генерується службами безпеки, над якими вони здійснюють контроль, що означало б, що вони не можуть розглядати інформацію, що надійшла з-за кордону.

Оскільки служби більше, ніж раніше, співробітничають з іноземними партнерами і зберігають більше інформації, що надійшла від зарубіжних служб, це закрило б деякі операції або сфери діяльності для незалежної перевірки. Визнаючи це, деякі контролюючі органи давали зрозуміти, що правило «третьої сторони» (іншими словами, принцип контролю джерела) до них не може бути застосовано, оскільки вони мають гарантований законом доступ до інформації, що зберігається у служб/виконавчої влади, над якими вони здійснюють контроль[81].

Доступ до інформації може бути підкріплений слідчими повноваженнями, включаючи повноваження викликати до суду людей і запитувати документи та право оглядати приміщення без повідомлення. Хоча ці повноваження використовуються рідко, вони підсилюють позицію контролюючого органу, коли служба безпеки опирається вивченню певних питань[82]. У Бельгії 1-й комітет

78. Germany 2001a: Section 15(5); Cameron 2011: 280.
79. Bigo et al. 2013: 61; Cameron 2011: 281.
80. Наприклад, UK 2000: Sections 58(1)(2) and 60(1); Netherlands 2002: Section 73(1); Norway 1995: Section 4.
81. Наприклад: Norway 2014: 1; Laethem 2011: 199; Wills and Vermeulen 2011: 125.
82. Netherlands 2002: Article 74; Belgium 1991: Article 48(2); загальний огляд слідчих повноважень у деяких європейських країнах див. в Wills and Vermeulen 2011: 134-135.

має навіть спеціальну службу розслідувань, слідчі якої можуть застосовувати поліцейські повноваження, щоб забезпечити співробітництво посадових осіб служби безпеки (Belgium 1991: Articles 45, 49).

Іншим потужним інструментом контролю є право прямого доступу до систем і баз даних розвідувальних служб, як правило – в офісах у приміщеннях служб безпеки. Таке право мають норвезький комітет EOS-Utvalget і голландський CTIVD[83]. Цей інструмент дає контролерам право доступу та безпосередньої перевірки всіх файлів, систем і кореспонденції, що стосується розслідування, що ускладнює службі безпеки приховування чогось від перевірки. Очевидно, що такі інструменти варто використовувати сумлінно й у повній відповідності із законним мандатом контролюючого органу.

Додатковим інструментом/повноваженням, що став особливо актуальним, є право залучати незалежних експертів (допущених службою безпеки після перевірки) для консультацій з технічних питань.

З ускладненням технологій безпеки і розвідки є необхідним вищий рівень технічних знань для розуміння й аналізу систем, що застосовуються для збору, обробки і зберігання інформації (включаючи персональні дані). Наслідки такої технології для прав людини не можна оцінити повністю без використання таких знань. Визнаючи важливість цього, деякі органи контролю отримали законне право залучати технічних фахівців для консультацій на постійній основі[84].

Розгляд скарг

Деякі країни-учасниці Ради Європи уповноважили органи експертного контролю розглядати скарги на діяльність служб безпеки, включаючи заяви про незаконне спостереження та/або використання персональних даних. Серед прикладів – 1-й комітет у Бельгії, шведський SIN і норвезький комітет EOS-Utvalget. У порівнянні з розглядом скарг органами, не пов'язаними з безпекою, наприклад, омбудсменами, перевага полягає в тому, що люди, які розглядають скарги, імовірно, є краще обізнаними з ситуацією в силу інших своїх функцій контролю, що може допомогти в розгляді скарг.

Такі органи також мають (повинні мати) доступ до найбільш делікатної інформації, а також процедури і досвід роботи з нею. Це спрощує оперативний розгляд скарг і може у такий спосіб дати істотну перевагу у порівнянні з більш загальними органами розгляду скарг, такими як омбудсмени (Forcese 2012: 186). З погляду захисту прав людини, слід зазначити, що органи експертного контролю взагалі-то не мають повноважень виносити юридично зобов'язуючі рішення після розгляду скарги. Як правило, вони можуть тільки давати рекомендації і вносити подання службам і політичній виконавчій владі, але не можуть розпорядитися про виплату або компенсацію чи вида-

83. Verhoeven 2011: 257; Norway 2014: 5.
84. Norway 2012, Norway 2013 and Norway 2014; див. також: With and Kathmann 2011: 221; Cameron 2011.

лення (корегування) персональних даних[85]. Так, у Швеції SIN може зробити висновок про те, що, наприклад, персональні дані скаржника оброблялися не у відповідності із законом. Однак SIN потім повинен повідомити про цю людину міністрові юстиції, який ухвалює рішення щодо необхідності виплати компенсації, і, за необхідності, справу потрібно передати до органу захисту даних, який дасть розпорядження про видалення персональних даних (Cameron 2011: 284).

Винесення необов'язкових рекомендацій є недостатнім для ефективного правового захисту скаржника. Вимога про видалення або корегування персональних даних та/або виплату компенсації є найпоширенішим і необхідним засобом правового захисту у контексті збору і використання службами безпеки персональних даних. Ураховуючи, що більшість органів експертного контролю не можуть приймати зобов'язуючих рішень, людям, чиї права були порушені службами безпеки, доводиться одночасно або згодом звертатися до якогось органу, що може забезпечити такий правовий захист. Вирішуючи, чи забезпечується ефективний правовий захист, має сенс всебічно розглянути систему контролю.

Омбудсмени

Повноваження омбудсменів у різних країнах Європи істотно відрізняються, і більшість із них не грають помітної ролі в контролі над службами безпеки. У багатьох країнах омбудсмен має можливість розслідувати скарги на служби безпеки, але вони рідко роблять це на практиці. Омбудсмени, однак, можуть зіграти важливу роль як при розгляді скарг, що стосуються служб безпеки, так і розслідуючи дії служб безпеки за власною ініціативою. Особливо це стосується держав, що не мають органів експертного контролю за безпекою/розвідкою або сильних комітетів парламентського контролю.

Вартим уваги прикладом омбудсмена, що грає активну роль у контролі над службами безпеки, є сербський захисник громадян. Його офіс розслідує скарги, що стосуються служб безпеки, діє на випередження, за власною ініціативою починаючи розслідування діяльності служб безпеки, й успішно оскаржував закони про службу безпеки в конституційному суді[86]. Сербія показала, що надання омбудсмену права оскаржувати неконституційні закони є корисним для захисту прав людини. При такому оскарженні омбудсмен може мати набагато вигіднішу позицію, ніж приватні особи або НУО. У Нідерландах омбудсмен теж розглядає скарги, що стосуються служб безпеки і розвідки, але скаржники можуть звертатися до омбудсмена тільки після подання скарги у відповідне міністерство і не одержавши задовільної відповіді.

Як і в багатьох органів експертного контролю за безпекою/розвідкою, один із недоліків моделі омбудсмена полягає в тому, що більшість із цих інститутів

85. Обговорення цього питання див. у: Forcese 2012: 192-193; Hernes 2008: 81-82.
86. Див., наприклад: Protector of Citizens of the Republic of Serbia 2010; Protector of Citizens of the Republic of Serbia 2014: 14-15, 207-211.

може лише давати рекомендації. Це є недостатнім, коли права людини порушені, і людина чекає ефективного правового захисту.

Органи захисту даних і комісії з питань інформації

Органи захисту даних і комісії з питань інформації – це незалежні контролюючі органи, відповідальні за перевірку дотримання державними органами (а в деяких випадках – і приватними організаціями) законодавства про захист даних та/бо про свободу доступу до інформації. Ці функції часто виконує один орган.

Рамки, в яких органи захисту даних здійснюють контроль за використанням персональних даних службами безпеки, залежать від того, чи охоплює законодавство про захист даних служби безпеки, чи поширюється мандат органів захисту даних на служби безпеки, обмеження права людей на доступ до персональних даних, що зберігаються службами безпеки, і обмеження доступу органів захисту даних до секретної інформації. Недавнє дослідження Робочої групи ЄС щодо статті 29 показало, що далеко не в усіх європейських країнах органи захисту даних повністю контролюють використання персональних даних службами безпеки і що дуже часто вони зовсім не допущені до цієї сфери. Проте деякі із цих інститутів мають повноваження й активно контролюють використання службами безпеки персональних даних та/або запити про доступ до інформації, що зберігається службами безпеки (Article 29 2014a: §§ 9-10).

Функції органів захисту даних можуть включати перевірку розгляду і прийняття рішень по індивідуальних запитах про доступ до персональних даних, що зберігаються службами безпеки. Вони можуть також за власною ініціативою проводити розслідування і перевірку роботи служб безпеки з даними. Наприклад, у Німеччині федеральний уповноважений із захисту даних вивчає додержання службами безпеки закону про захист даних, за винятком даних, зібраних у ході спостереження (якими займається інший орган – Комісія G10), ці питання охоплюють її дворічні звіти (With and Kathmann 2011:227). Словенська і сербська комісії з питань інформації мають схожу контролюючу роль[87].

У багатьох європейських країнах служби безпеки повністю виключені зі сфери дії законодавства про свободу інформації/доступу до інформації (Jacobsen 2013: 9-10). Це означає, що громадяни не можуть вимагати доступу до конкретних документів, а уповноважені з питань інформації не мають повноважень рекомендувати або вимагати розкриття інформації. Швейцарія є прикладом країни, де служба безпеки не є виключеною зі сфери дії закону про свободу інформації. У ході процесу, ініційованого журналістом, який намагався одержати доступ до резюме звітів розвідувальної служби, федеральний адміністративний трибунал нещодавно підтвердив, що навіть секретна інформація може підлягати розкриттю[88]. Федеральний уповноважений з питань захисту даних

87. Slovenian Information Commissioner: www.ip-rs.si/?id=195, accessed 28 March 2015; Serbian Information Commissioner: www.poverenik.rs/index.php, accessed 28 March 2015; див. також: Petrovic 2012: 21-23.

88. Stoll 2014; Goumaz 2014.

та інформації здійснює контроль за розглядом запитів громадян на інформацію. Такою самою є ситуація в Словенії, де уповноважений з питань інформації перевіряє обґрунтованість нерозголошення інформації службами безпеки і може розпорядитися розсекретити інформацію за відповідних обставин (Jacobsen 2012: 17).

Нарешті, і словенський, і сербський уповноважені з питань інформації використали свої повноваження, щоб оскаржити закони про зберігання даних і спостереження у своїх конституційних судах. Це є яскравими прикладами здатності незалежних органів контролю проводити перевірки не тільки дотримання прав людини у практиці служб безпеки, але й правової бази діяльності цих служб.

4.3. Судові органи

Хоча суди можуть перевіряти і розглядати дії служб безпеки та їх наслідки у багатьох ситуаціях, у цьому розділі ми зосередимося на ролі судових органів в санкціонуванні заходів спостереження, пов'язаних із втручанням, службами безпеки, і розгляді скарг на (можливу) діяльність служб безпеки.

Скарги на служби безпеки

Що стосується скарг на служби безпеки, у більшості країн-учасниць Ради Європи приватні особи теоретично мають можливість порушити справу для отримання правового захисту. Справу може бути порушено безпосередньо, коли особа намагається оскаржити арешт, допит або затримання (у тих небагатьох країнах, де службам безпеки надано ці повноваження). Однак, як зазначено вище (див. розділ 2.4 про право на справедливий суд), часто виникають істотні перешкоди для судочинства проти служб безпеки.

Використання судів для оскарження спостереження служби безпеки або використання даних є ще складнішим, оскільки в більшості випадків людина не знає про таке порушення своїх прав (Venice Commission 2007: § 243). Справу звичайно можна порушити, лише якщо людина довідається про такі заходи на підставі якихось вимог про повідомлення, випадково, від інформатора або в ході іншого судового процесу. Іноді є прямі обмеження на оскарження людьми таємного спостереження у звичайних судах до того, як їх спеціально повідомлять про стеження (Germany 2001a: Section 13).

У Великобританії створено спеціальний судовий орган, Трибунал з питань слідчих повноважень (*Investigatory Powers Tribunal*, *IPT*), для розгляду скарг про спостереження й усіх пов'язаних з правами людини претензій до служби безпеки[89]. Він має виняткові повноваження розглядати такі претензії. Перевагою цієї моделі є те, що вона дозволяє розслідувати позови у зв'язку з (імовірним) спостереженням, навіть якщо це спостереження триває, і він може давати

89. UK 2000: Sections 65-67; веб-сайт IPT див.: www.ipt-uk.com/, accessed 28 March 2015.

обов'язкові для виконання розпорядження, якщо заходи виявляться незаконними. У 2015 р. Трибунал виніс своє перше рішення проти служб безпеки і розвідки, дійшовши висновку, що деякі аспекти міждержавного обміну розвідувальною інформацією порушували статті 8 і 10 Європейської конвенції з прав людини, оскільки вони «не відповідали закону»[90]. Незважаючи на цей успіх, у моделі цього трибуналу існують серйозні недоліки, і її різко критикували[91]. А саме: скаржників можна не інформувати про слухання, вони не мають автоматичного права бути присутніми на слуханнях або бути представленими адвокатом, за їх вибором, причини рішення можуть не пояснюватися, і рішення IPT не можна оскаржити або змінити в суді.

Санкціонування інтрузивних заходів

У більшості країн-учасниць Ради Європи існує вимога, щоб їх служби безпеки одержали ордер суду на проведення заходів для збору інформації, що вважаються особливо безцеремонними в аспекті права на приватне і сімейне життя.

Серед винятків із виключно судової моделі санкціонування – Великобританія і Нідерланди (санкціонує виконавча влада), Польща (згода судді і незалежного генерального прокурора, що не належить до виконавчої влади) (Poland 2002: Article 27), Бельгія та Німеччина (різні форми квазісудових санкцій), і Румунія (санкція спеціальних прокурорів)[92].

Хоча види заходів, що потребують зовнішньої санкції, бувають різними, зазвичай вони включають цілеспрямоване перехоплення зв'язку (якщо особа/організація, чиї лінії зв'язку планується перехоплювати, відома із самого початку), пошук та арешт майна й установлення записуючих пристроїв в оселях. У той же час у більшості країн судової санкції не потрібно, наприклад, для збору інформації за допомогою людей, невибіркового масового стеження, використання комп'ютерних мереж, пошуку по вже існуючих банках даних, зібраних шляхом масового стеження, одержання даних, зібраних іншими урядовими відомствами, і доступу до даних, збережених приватними компаніями. Помітним винятком є Сербія, де служба безпеки зараз повинна одержати санкцію суду не тільки на таємне спостереження або запис будь-якої форми переговорів, але й на тримання даних зв'язку і здійснення пошуку в даних, уже отриманих з використанням повноважень, пов'язаних із втручанням (Serbia 2014: Articles 13 and 15). Цей підхід є корисним прикладом у світлі нинішніх дебатів про те, як краще контролювати доступ служб безпеки до даних, зібраних шляхом, наприклад, масового збору, а також доступ до даних зв'язку.

Викриття Сноудена порушили питання про межі судових санкцій на невибіркове масове стеження за кабельними і бездротовими лініями зв'язку. Хоча за-

90. Liberty & Others vs. the Security Service, SIS, GCHQ.
91. Див., наприклад: JUSTICE 2011: 133-153; Leigh 2012: 438-439.
92. Romania 1991: Article 13. Слід звернути увагу на критику судом цього підходу до видачі санкцій, як не повністю незалежного від виконавчої влади: Dumitru Popescu v. Romania [69-73].

гальнодоступна інформація про це є обмеженою, закони більшості країн-учасниць Ради Європи прямо не вимагають санкції суду на такі заходи (якщо вони дозволені національним законодавством і перебувають у межах можливостей служби безпеки). Однак у Швеції є спеціальний суд, що дає дозвіл на невибіркове масове перехоплення кабельних і бездротових міжнародних ліній зв'язку (тобто тих, що не вважаються повністю внутрішніми). Суд військової розвідки у складі двох суддів і шести засідателів видає радіослужбі міністерства оборони (FRA) ордери на використання конкретних налаштувань (потоків для пошуку) у тих чи інших міжнародних кабелях[93].

Хоча точні модальності застосування і розгляду судових ордерів у різних країнах різняться, у більшості випадків цю роль виконує старший суддя, спеціально призначений згідно із законом або обраний за передбаченою законом процедурою. Наприклад, у Боснії і Герцеговині такий суддя є головою суду Боснії і Герцеговини або призначеним ним суддею. В Угорщині – це суддя, призначений головою столичного суду, а в Чехії – суддя, який очолює колегію суддів вищого суду у відповідному географічному регіоні[94]. Хорватія передбачає додаткове обмеження при видачі повторної санкції (продовженні санкції) на заходи, пов'язані із втручанням: це повинна робити колегія у складі трьох суддів, а не один суддя, як у випадку первинної санкції (Croatia 2006: Articles 36 and 37(2)).

Загалом судді ухвалюють рішення щодо дозволу на основі письмових заяв, але в деяких країнах передбачені слухання по заявах, по яких виникають складні питання або судді хочуть поставити питання представникові служби безпеки. Засідання завжди проводяться постфактум, і в більшості країн майбутній об'єкт заходів, пов'язаних із втручанням, ніяк не представлений. Інноваційний підхід прийнятий у Норвегії, де інтереси майбутнього об'єкта заходів спостереження з боку поліції безпеки представляє допущений службами безпеки адвокат, який може оскаржити підстави для ордера, наведені службою безпеки[95]. Це робиться на основі письмового подання. Суд військової розвідки Швеції (див. вище), відповідно до повідомлень, використовує подібну систему для видачі ордерів на перехоплення міжнародних ліній зв'язку (Pond 2013). За межами Європи, група з вивчення технологій розвідки та зв'язку при президенті США закликала до створення посади адвоката із захисту інтересів громадськості «для представлення інтересів тих, чиї права на приватне життя або громадянські свободи можуть бути під загрозою»[96]. Участь такої особи у процесі санкціонування заходів, пов'язаних із втручанням, забезпечує кращий захист прав людини, оскільки це дозволяє органу, що дає санкцію, вислухати різні точки зору, включаючи тлумачення положень закону, що допомагає забезпечити критичний аналіз обґрунтування, запропонованого службами безпеки.

93. Cameron 2011: 281; Bigo et al. 2013: 61; Pond 2013.
94. Bosnia and Herzegovina 2004: Article 77; Hungary 1995: Section 58; Czech Republic 1994 § 9(1).
95. Norway 1981: Section 100a; Norway 2014: 8.
96. Review Group on Intelligence and Communications Technologies 2013: 203-204 and Recommendation 28.

Санкція суду часто вважається найкращим захистом прав людини, насамперед тому, що суддів зазвичай вважають незалежними, неупередженими і менш залежними від політичних міркувань, що оточують діяльність служб безпеки, що може вплинути на рішення міністра про надання дозволу.

Суддів також вважають здатними краще оцінити правові критерії, зокрема, необхідності і пропорційності, що є досить важливим, коли заходи, щодо яких робиться запит, можуть мати істотні наслідки для прав людини.

Санкція суду, однак, не є панацеєю, що гарантує дотримання прав людини при дозволі і застосуванні заходів, пов'язаних із втручанням, службами безпеки (Venice Commission 2012: § 35). У санкцій суду є ряд потенційних недоліків. По-перше, ефективність санкції суду як засобу захисту прав людини значною мірою залежить від незалежності конкретних суддів. У країнах, де судді не є незалежними, малоймовірно, що вони будуть дуже критично підходити до запитів служб безпеки про використання пов'язаних із втручанням заходів.

По-друге, знання є так само необхідними для ефективності санкції суду (Venice Commission 2007: §§ 205-206). Судді, чий досвід у питаннях безпеки є обмеженим (і навіть досвідчені судді), можуть бути не схильними критикувати оцінки національної безпеки чиновниками служби безпеки, які звертаються за ордером (Cameron 2008: 45). Іноді це доповнює схильність деяких суддів шанобливо ставитися до виконавчої влади щодо питань національної безпеки. По-третє, також висловлювалися побоювання, що у багатьох країнах санкція суду є рівнозначною штампуванню рішень, прийнятих службами безпеки, і дуже мало запитів на ордери відхиляються (Управління Верховного комісара ООН з прав людини 2014: § 38). Нарешті, у тісному зв'язку із проблемою «штампування», фактом є те, що суддів зазвичай не можна притягти до відповідальності за ордери, видані ними службам безпеки. Щоб зберегти незалежність суду й розподіл повноважень, процедура видачі ордерів як правило не підлягає подальшій перевірці контролюючим органом (Cameron 2011: 285).

Навпаки, міністра або квазісудовий орган, який дає санкцію, легше притягти до відповідальності в парламенті або незалежному контролюючому органі за прийняті ними рішення, і ця можливість може мати сприятливий ефект на прийняття рішень (Borger 2014).

4.4. Квазісудові дозвільні органи

На території Ради Європи є кілька держав, де заходи, пов'язані із втручанням, повинні бути санкціоновані квазісудовим органом. У Бельгії нещодавно був прийнятий новий підхід до надання дозволу (і контролю) щодо здійснення деяких заходів, пов'язаних із втручанням.

Адміністративна комісія (*SIM Commission*)[97] у складі трьох допущених службою безпеки мирових суддів (які діють не як судді), призначена виконавчою

97. Її повна назва: La commission administrative chargee de la surveillance des methodes specifiques et exceptionnelles de recueil de donnees par les services de renseignement et de securite.

владою, дає «обов'язкову для виконання пораду» службам безпеки, коли ті звертаються з проханням про застосування «виняткових заходів» (найбільш крайніх із трьох категорій заходів)[98]. Ці виняткові заходи включають спостереження й обшук приватного житла; проникнення до електронних систем; перехоплення зв'язку; використання агентів, у т.ч. шляхом створення фейкових облікових записів. У розвідувальних операціях за участю людей, наприклад, при використанні інформаторів або упровадженні в організації, не прийнято запитувати дозвіл незалежного органу, й у зв'язку з цим бельгійське законодавство визнає наслідки розвідувальних операцій за участю людей для прав людини.

Важливішим є те, що бельгійське законодавство визнає наслідки хакерства для прав людини і вимагає, щоб такі заходи санкціонував зовнішній орган. Є й інша категорія менш безцеремонних «специфічних заходів» (включаючи ідентифікацію користувача послуг зв'язку і доступу до даних електронного зв'язку), які можуть бути дозволені керівником відповідної служби безпеки. Однак вони мають спочатку повідомити комісію SIM, а служби також повинні щомісяця звітувати про застосування таких заходів[99].

Складна бельгійська система санкціонування заходів, пов'язаних із втручанням, також передбачає поточний контроль за застосуванням заходів, дозволених Комісією SIM, для оцінки їх законності (включаючи, зокрема, їх пропорційність). Комісія має повноваження призупинити застосування заходів, пов'язаних із втручанням, або, у разі менш безцеремонних заходів, санкціонованих директором служби, може розпорядитися про заборону використання зібраних даних. Комісія SIM, зі свого боку, повинна інформувати орган експертного контролю (1-й комітет – див. вище) про видачу або відмову у видачі дозволів та їх продовження.

1-й комітет розглядає всі дозволи і проведення заходів службами безпеки. Цей орган експертного контролю може фактично скасувати рішення Комісії SIN про надання дозволу, відмову в дозволі або призупинення заходу[100].

Такий контроль за дозвільним органом забезпечує додатковий захист прав людини.

Німецький підхід до санкціонування заходів, пов'язаних із втручанням, також заслуговує розгляду.

Проведення таких заходів може в першу чергу дозволити призначений урядом міністр, який потім звертається за дозволом до органу під назвою Комісія G10 (іноді – заднім числом). Це стосується не тільки цілеспрямованого спостереження, але й невибіркового спостереження із застосуванням налаштувань або умов пошуку, законність (включаючи пропорційність) яких оцінює Комісія G10. Що стосується невибіркового спостереження, то Комісія G10 також пере-

98. Belgium 2010: Articles 18 (2)(3)(9)(10), 43(1).

99. Belgium 1998: Articles 18 (2) (3).

100. Докладний аналіз перевірки цих заходів 1-м комітетом див. у: Belgian Standing Intelligence Agencies Review Committee 2012: 143-169; Belgium 1998: Articles 43(3) (3)(4)(5).

віряє мінімальність даних, отриманих шляхом спостереження[101]. Комісія G10, призначена комітетом парламентського контролю, може вважатися квазісудовою, оскільки її очолює особа, яка має право на судову посаду (але діє не як суддя); три інших члени можуть бути або не бути депутатами Бундестагу[102].

Необхідність дозволу і від члена виконавчої влади, і від незалежних органів, включаючи суддів[103] або квазісудовий орган, дає значні переваги з погляду прав людини. Вона гарантує подвійну «перевірку» поза службою безпеки і потенційно гарантує, що в процесі задіяні якості і виконавчої, і судової санкції.

4.5. Виконавча влада

Політична виконавча влада є споживачем, постановником завдань, контролером і наглядачем за службами безпеки. Її не можна вважати зовсім стороннім наглядачем, оскільки органи виконавчої влади беруть участь у процесі розвідки – вони ставлять завдання, надають дозволи, визначають політику і пріоритети службам безпеки (Venice Commission 2007: § 129). У всіх країнах-учасницях Ради Європи за служби безпеки відповідає один або декілька представників виконавчої влади. У цілому служби безпеки належать до ряду міністерств – оборони, юстиції, внутрішніх справ, але можуть підпорядковуватися прем'єр-міністру (наприклад, у Туреччині), президенту (наприклад, у Румунії) або можуть перебувати під спільним керівництвом президента та прем'єр-міністра (наприклад, у Хорватії). Контроль *(у широкову і вузькому значеннях)* з боку виконавчої влади може здійснювати й колективний орган, наприклад, рада національної безпеки, як у Хорватії та Сербії. У Хорватії, наприклад, Раді національної безпеки допомагає офіс Ради національної безпеки, що відповідає, зокрема, за моніторинг законності діяльності служб безпеки (Croatia 2006: Article 107(1)). Це доповнює контроль за законністю з боку зовнішнього органу експертного контролю (див. вище).

Обов'язки виконавчої влади включають також визначення вказівок, додаткових правил, загальної політики і пріоритетів служб безпеки. Ці функції включають надання вказівок про те, як ураховувати права людини й забезпечувати належний облік прав людини в політиці та пріоритетах. Наприклад, британський уряд давав службам безпеки і розвідслужбам вказівки щодо обміну інформацією про осіб, які утримуються в попередньому ув'язненні або допитуються іноземних службах безпеки (UK 2010). На виконавчу владу покладено основний обов'язок із забезпечення роботи служб безпеки з дотриманням прав людини.

---

101. Germany 2001a: Section 10(1); With and Kathmann 2011: 221-223; Venice Commission 2015: §§ 124-125.
102. Germany 2001a: Section 15.
103. Канада являє собою приклад країни, що не входить до Ради Європи, де також застосований дворівневий підхід до видачі дозволів – заступником міністра і суддею федерального суду. Див.: Canada 1984: § 21(1).

Через це зовнішні контролюючі органи можуть прагнути до того, щоб міністри використовували свої повноваження, наприклад, для розроблення кодексів етики або правил обміну інформацією із закордонними партнерами.

Нарешті, у деяких країнах-учасницях Ради Європи міністри також відповідають за надання дозволу на використання заходів спостереження[104] і визначення ключових слів (параметрів пошуку), які служби безпеки можуть використовувати під час пошуку в так званих даних зв'язку (Bigo et al. 2013: 74). Там, де міністри мають таку роль, є важливим, щоб у них був доступ до радників, здатних допомогти їм оцінити права людини і більш широкі правові наслідки будь-яких запропонованих заходів.

4.6. Заходи внутрішнього контролю

Хоча ця доповідь насамперед стосується зовнішнього контролю, керівники служб безпеки та їх персонал відіграють провідну роль у забезпеченні законності їх діяльності і додержанні прав людини. Саме співробітники служб безпеки, а не зовнішні контролери, присутні при прийнятті багатьох рішень, що мають важливі наслідки для прав людини. Тому найбільше значення мають цінності, етика і юридичні знання персоналу служб безпеки. Для цього керівники служб безпеки повинні застосовувати жорсткі критерії перевірки при доборі й набирати тільки людей з відповідними якостями. Вони також повинні організовувати постійну підготовку, у т.ч. з питань прав людини (Venice Commission 2007: § 132) і ролі зовнішніх контролюючих органів. Важливо, щоб зовнішні контролюючі органи перевіряли цю внутрішню політику і практику служб безпеки.

Зрештою, ефективні системи зовнішнього контролю мало значать, якщо служби безпеки не прагнуть працювати, поважаючи права людини й сприяючи контролю та підзвітності (Venice Commission 2007: §§ 130, 134). Аналогічно, для того, щоб зовнішній контроль сприяв дотриманню прав людини і підзвітності в службах безпеки, потрібно бажання співробітничати з контролюючими органами й ураховувати їх рекомендації.

Всі служби безпеки запроваджують внутрішні процедури надання дозволу на проведення певних заходів, розгляду своєї діяльності, належного обліку діяльності та звітності про проблеми[105]. У більшості випадків ці процедури запроваджує вище керівництво, але їх може вимагати й закон. Наприклад, у Німеччині служби безпеки зобов'язані забезпечувати застосування заходів спостереження під наглядом співробітника, який має право обіймати посаду в суді[106].

Деякі країни-учасниці Ради Європи, наприклад, Італія, Боснія і Герцеговина, Сербія, також законодавчо запровадили в службах безпеки пости генеральних інспекторів.

---

104. Наприклад: UK 2000: Sections 7 and 8; Netherlands 2002: Article 19 (за винятком пошти, на що має бути дозвіл суду, відповідно до статті 23).
105. Загальний огляд див. у: Born and Leigh 2005: 46-49.
106. Germany 2001a: Section 11(1).

Функції цих внутрішніх інспекторів включають оцінку законності діяльності служб[107]. Хоча ця контролююча функція може бути корисною для попередження керівників служб і законодавчої влади про всі проблеми, внутрішні генеральні інспектори не можуть замінити суворої зовнішньої перевірки.

4.7. Засоби масової інформації та громадянське суспільство

Роль ЗМІ у висвітленні питань безпеки на території Ради Європи є досить відрізною і залежить, зокрема, від власників ЗМІ, законів про захист джерел журналістської інформації та людських і фінансових ресурсів медійних організацій. ЗМІ часто випереджають офіційну «лінію» контролю, розкриваючи і розслідуючи такі питання, як таємні видачі й затримання, раніше, ніж це роблять постійні контролюючі органи (Priest 2005). У багатьох випадках робота журналістів призводила до проведення розслідувань з боку постійних і спеціальних контролюючих органів.

Журналісти грають дуже важливу роль у розкритті незаконної діяльності служб безпеки в ситуаціях, коли офіційні системи контролю не можуть виявити або припинити практику порушення прав людини (ПАРЄ 2011: § 8). Вони також можуть бути рупором для співробітників служб безпеки, які бажають донести до громадськості побоювання щодо незаконності, якщо у них немає можливості домогтися розгляду цих побоювань визначеними каналами, немає довіри до таких каналів або якщо немає іншого дозволеного зовнішнього каналу для викриттів.

Неурядові організації (НУО) також беруть участь у моніторингу й оприлюдненні роботи контролюючих органів. НУО на заході Балкан були особливо активними щодо цього, а ряд НУО спеціалізується на питаннях верховенства права у сфері безпеки. Наприклад, після прийняття закону про парламентський контроль за сферою безпеки і оборони у 2010 р. Чорногорський Institut Alternativa проводив щорічні дослідження реалізації закону, звертаючи першочергову увагу на ефективність роботи комітету, якому доручено контроль за сферою безпеки[108]. Важливо, щоб НУО (і ЗМІ) цікавилися не тільки службами безпеки, але й інститутами, які здійснюють контроль за ними.

НУО також відіграють важливу роль у притягненні до відповідальності й участі в судових процесах, що стосуються служб безпеки, у Європейському суді з прав людини і національних судах. Такі організації, як Open Society Justice Initiative, Reprieve і польський Гельсінський фонд з прав людини, брали участь у подачі позовів, що стосуються прав людини, у зв'язку з участю європейських держав у таємних затриманнях і видачах під керівництвом США. Кілька НУО, включаючи Privacy International, Big Brother Watch та Liberty, брали активну участь у порушенні справ проти урядів у національних і міжнародних судах у зв'язку із законами та практикою стеження. Одним із прикладів є справа Liberty та ін. проти Великобританії (в якому Страсбурзький

107. Bosnia and Herzegovina 2004: Article 33(1); Petrovic 2012: 14-15.

108. Див.: http://institut-alternativa.org/?lang=en, accessed 28 March 2015.

суд виявив невідповідність Конвенції раніше існуючої британської правової бази, що використовувалася під час масового перехоплення міжнародних ліній зв'язку). Роль НУО залишається життєво важливою в контексті безперервних проблем, пов'язаних з масовим стеженням, міждержавним обміном розвідувальною інформацією та хакерством служб безпеки.

НУО також можуть бути корисними, організовуючи кампанії за розслідування діяльності служб безпеки та пропонуючи свої знання для таких розслідувань, а також вносячи подання, коли парламент приймає або змінює закони про служби безпеки. За минуле десятиліття ці організації привертали увагу до ймовірних недоліків у процесах контролю та звітності і виступали за більш суворе, незалежне спеціальне розслідування діяльності служб безпеки (Townsend 2014).

Здатність ЗМІ та НУО здійснювати неформальний контроль за службами безпеки значною мірою залежить від наявності середовища, в якому вони можуть сперечатися з урядами з делікатних питань, не боячись залякування або розплати.

У деяких країнах-учасницях Ради Європи ситуація є іншою. Існування і сфера дії законів про свободу інформації також впливає на здатність ЗМІ та НУО займатися цими питаннями. Хоча в багатьох країнах-учасницях Ради Європи служби безпеки не охоплені цими законами, деякі національні закони дозволяють приватним особам (організаціям) запитувати інформацію у служб безпеки або про служби безпеки та вимагати, щоб служби обґрунтовували (під зовнішнім контролем) рішення про ненадання інформації. Такі підходи до свободи інформації дозволяють організаціям громадянського суспільства та ЗМІ одержувати інформацію, що може допомогти їм у їхній роботі, без ризику для національної безпеки.

Розділ 5

ДО ДЕМОКРАТИЧНОГО Й ЕФЕКТИВНОГО КОНТРОЛЮ ЗА НАЦІОНАЛЬНИМИ СЛУЖБАМИ БЕЗПЕКИ

Виходячи з міжнародних принципів і національних практик, розглянутих у цьому документі, очевидно, що системи контролю може бути побудовано дуже по-різному, переслідуючи при цьому схожі цілі. При плануванні й оцінюванні систем контролю є корисним зосередитися на суті, а не на формі контролю. Це дозволяє досягати однакових цілей, допускаючи різні конституційні та правові системи, а також різні національні традиції. Ціль цієї, останньої глави – показати ряд важливих принципів і завдань, що випливають із попереднього аналізу.

Головний принцип, який можна вивести з розглянутих вище міжнародних принципів і практик різних держав, полягає в тому, що всі аспекти діяльності, політики, фінансування, управління і правил служб безпеки повинні підлягати перевірці як мінімум однією організацією, що є зовнішньою та незалежною від служб безпеки і виконавчої влади. Міжнародні принципи і практика багатьох країн-учасниць Ради Європи показують, що така зовнішня перевірка повинна бути попередньою (там, де це можливо), поточною і наступною.

Широкі завдання систем контролю повинні включати відповідальність служб безпеки і (за необхідності) політичної виконавчої влади та сприяння підвищенню:

- ефективності служб безпеки при виконанні їх законних повноважень, включаючи участь у запобіганні загрозам правам людини, зокрема, внаслідок тероризму, шпигунства і кіберзлочинності;
- ефективності, фінансовій законності й ощадливості служб безпеки; і
- відповідності правил, стратегій і операцій законності та правам людини.

Третє завдання є предметом цієї доповіді та кінцевим завданням для всіх інших завдань, розглянутих у цій главі. Варто нагадати, що хоча ця доповідь стосується зовнішнього контролю за службами безпеки, внутрішні перевірки та заходи контролю в цих службах є дуже важливими для вирішення вищезгаданих завдань.

Демократичний контроль є важливим, оскільки служби безпеки (і відповідні органи виконавчої влади) надають публічні послуги суспільству та від імені суспільства, і тому обрані представники повинні брати участь у забезпеченні ефективного, діючого і законного надання цих послуг. Відповідно, «демократичний» аспект контролю забезпечується, насамперед, участю парламенту. Досвід країн-учасниць Ради Європи показує, що парламентарії роблять свій внесок:

- забезпечуючи всебічний контроль за службами безпеки в національному законодавстві;
- виділяючи необхідні бюджетні ресурси непарламентським інститутам контролю;
- контролюючи роботу органів експертного контролю;
- розглядаючи ефективність інститутів контролю (включаючи свої власні комітети);
- і проводячи поточні перевірки та спеціальні розслідування діяльності служб безпеки.

Парламентський контроль за службами безпеки залишається важливим у будь-якій демократичній країні, але, як показують міжнародні принципи і практика держав, росте розуміння того, що права людини і верховенство права найкраще захищені, коли контроль з боку парламенту доповнений експертним контролем. Органи експертного контролю в цілому мають кращі можливості здійснювати поточну, детальну і політично нейтральну перевірку, необхідну для захисту прав людини. Цей вид контролю є особливо необхідним при перевірці дій служб безпеки, що впливають на права на приватне життя, свободу слова, зборів та об'єднання.

Така діяльність включає збір, використання, зберігання, передачу (у т.ч. національним правоохоронним відомствам і закордонним органам) і видалення персональних даних. Оскільки органи експертного контролю грають все більшу роль у контролі над службами безпеки, важливо забезпечити вживання заходів для того, щоб ці інститути мали певну демократичну легітимність. Відповідно, у різних країнах-учасницях Ради Європи є парламентські комітети, що стежать за роботою експертів-контролерів, призначають (і звільняють) співробітників та одержують їх звіти.

5.1. Попереднє санкціонування інтрузивних заходів

Стосовно попереднього санкціонування збору інформації, права людини є найкраще захищеними, якщо санкціонувати інтрузивні заходи повинен орган, незалежний від служб безпеки і політичної виконавчої влади. Зростає розуміння того, що зовнішнє санкціонування має охоплювати:

- невибірковий масовий збір інформації;
- використання ключових слів або налаштувань для вилучення даних з інформації, зібраної шляхом масового перехоплення, особливо якщо вони стосуються людей, чию особистість можна встановити;
- збір і доступ до даних зв'язку (у т.ч. у приватному секторі);
- проникнення в комп'ютерні мережі.

Як показано вище, наслідки такої діяльності для прав людини є надто значними, щоб її дозволяла тільки виконавча влада або (ще гірше) служби безпеки, що привласнили собі це право. Зовнішню санкцію на ці заходи повинен надавати судовий або квазісудовий орган, або спільно один із цих органів та виконавча влада.

Залучення різного досвіду для участі в процесі санкціонування заходів, пов'язаних із втручанням, може забезпечити кращий захист, ніж санкція політичного або судового органу. Процес санкціонування безумовно повинен включати правову і правозахисну оцінку пропонованих заходів, але може бути корисним також розгляд усіх політичних ризиків, пов'язаних із запропонованими заходами. Відповідно, дворівневий процес санкціонування, що поєднує санкцію (квазі)судового органу та санкцію міністра, може запропонувати найбільш надійну модель попередньої перевірки.

Як і в будь-якому елементі процесу збору інформації, процес санкціонування або підтвердження інтрузивних заходів теж вимагає перевірки. Ураховуючи складнощі, що можуть виникати при спробах оцінити рішення суду про санкціонування інтрузивних заходів, можна розглянути квазісудові моделі. Квазісудове санкціонування, що є більш розповсюдженим на території Ради Європи, включає судовий досвід без судового статусу санкціонуючого органу. Як показує практика різних держав, роботу таких органів може перевіряти інший контролюючий орган без виникнення побоювань, пов'язаних з можливою наступною перевіркою рішень суду.

Захист прав людини шляхом процесу санкціонування також можна покращити, залучаючи адвокатів, які представляють інтереси майбутнього об'єкта (а у разі масового стеження – побічних жертв) спостереження й інших можливих форм безцеремонного втручання, наприклад, хакерства. Ця третя сторона може оскаржити запропоноване службою безпеки спостереження, і їхня участь знижує ризик того, що процес санкціонування перетвориться в просте «штампування».

5.2. Розгляд скарг

Усі країни-учасниці Ради Європи повинні забезпечувати, щоб їх системи контролю включали певний незалежний орган, якому можна направляти скарги на служби безпеки. Незалежно від того, чи йде мова про орган експертного контролю за безпекою/розвідкою або контролюючий орган, не пов'язаний з безпекою, такий як омбудсмен, скарги повинен розглядати орган, що має необхідний доступ і слідчі повноваження для ретельного розслідування. Більшість контролюючих органів можуть лише давати рекомендації службам безпеки та/або виконавчій владі. Оскільки ЄКПЛ вимагає, щоб особи, які вважають (або знають), що їх права були незаконно порушені службами безпеки, мали доступ до інституту, здатному надати ефективний правовий захист, держава повинна забезпечити цим людям також доступ до інституту, здатного давати юридично обов'язкові розпорядження. Повноваження такого органу повинні включати не тільки надання компенсації жертвам будь-яких порушень, але й повноваження скасовувати відповідні ордери та давати розпорядження про видалення незаконно зібраних персональних даних.

5.3. Доступ контролерів до інформації

Доступ контролерів до інформації має величезне значення і згадується майже у всіх міжнародних принципах, що стосуються контролю. Контролери, зокрема, не можуть давати повну та надійну оцінку законності операцій, програм і політики, якщо вони не мають доступу до всієї відповідної інформації. Хоча це не є самоціллю, доступ до всієї інформації, що стосується розслідування (і більш широкі повноваження такого контролюючого органу), є передумовою ефективної перевірки.

Право контролюючих органів на доступ до інформації повинне доповнюватися обов'язком служб безпеки та їх персоналу бути відкритими і співробітничати з контролерами, а також вимогою, щоб ці категорії інформації розкривалися автоматично. Використання таких слідчих повноважень, як виклик до суду, обшук і конфіскація, також зміцнює позицію контролерів у разі, якщо інформація не надається добровільно.

Надання контролерам доступу до інформації не означає, що контролюючі органи повинні постійно мати необмежений доступ до будь-якої інформації – підставою для доступу завжди має бути мандат і поточна діяльність певного контролюючого органу.

Виходячи з того, що кращою практикою вважається, коли принаймні один зовнішній контролюючий орган має повноваження щодо контролю за кожною сферою діяльності служб безпеки, принаймні один зовнішній контролер повинен мати необмежений доступ до інформації, що стосується кожної сфери. Відповідно, важливим завданням під час планування й удосконалення системи контролю є забезпечення того, щоб доступ контролерів до інформації був гарантований законом і забезпечений відповідними слідчими інструментами для полегшення такого доступу.

Основний принцип ефективного контролю полягає в тому, що контролюючі органи (а не служби безпеки чи виконавча влада, що є об'єктом перевірки) повинні визначати, яка інформація стосується їхньої роботи. У разі виникнення суперечок з цього приводу, повинні бути механізми з їх оперативного врегулювання.

Важливим доповненням до забезпечення доступу контролерів до всієї необхідної інформації є необхідність реалізації заходів забезпечення, щоб оброблювана контролерами інформація була захищена й використовувалася тільки з метою контролю. Якщо контролюючі органи мають процедури, що виключають зловживання делікатною інформацією, немає підстав не вірити їх членам більше, ніж співробітникам виконавчої влади або служб безпеки.

Доступ до інформації на підставі та у зв'язку з міжнародним співробітництвом розвідувальних служб заслуговує особливого розгляду. Ураховуючи широке міжнародне співробітництво служб безпеки (і можливий вплив такого співробітництва на права людини), важливо, щоб контролери могли перевіряти інформацію про таке співробітництво, включаючи інформацію, отриману від іноземних органів або надану ім. Щоб забезпечити належну перевірку цієї діяльності, важливо, щоб контролерів у силу закону або на практиці не вважали «третьою стороною» і не застосовували до них принцип контролю джерела. Демократичний контроль є досить складним, якщо іноземні органи фактично мають право вето (оскільки служби безпеки повинні запитувати дозвіл іноземних партнерів перед тим, як контролери зможуть переглянути таку інформацію) на те, що може перевіряти контролюючий орган.

Ще одним завданням є забезпечення контролерів необхідними фінансовими і людськими ресурсами, що гарантують їх ефективність. Багато служб безпеки нарощують свої можливості (завдяки технічному прогресу та зростаючим бюджетам) збирати, передавати й одержувати інформацію та використовують для цього усе складніші системи. Ресурси більшості контролерів не зросли відповідно до таких змін. Зараз загальновизнано, що використання незалежних технічних знань є невід'ємним від ефективного контролю.

Системи збору і зберігання інформації стали складнішими, і наслідки цього для прав людини важко оцінити без спеціальних знань. Тому закони мають дозволяти контролерам наймати технічних фахівців, і повинні надаватися ресурси, що дають їм змогу робити це.

5.4. Прозорість контролюючих органів

Контролюючі органи перевіряють служби безпеки від імені населення. При цьому важливими завданнями є надання громадськості гарантій (в обґрунтованих випадках), що служби безпеки здійснюють свої функції відповідно до закону, та інформування (за необхідності) про те, що зроблено неправильно. Контролюючі органи можуть робити це, тільки якщо вони своєю звітністю й іншими формами інформування показують, що служби безпеки перебувають

під суворим контролем і що всі випадки порушень прав людини (або інших порушень) розглядаються. Друге завдання в цьому зв'язку – інформувати громадськість про ролі служб безпеки в демократичній країні. Це має особливе значення для суспільств, в яких служби безпеки в минулому порушували права людини та/або не користуються довірою суспільства. Для цього важливо, щоб органи парламентського й експертного контролю максимально залучали громадськість. Вони повинні бути зобов'язані видавати публічні версії своїх регулярних або спеціальних звітів, додержуючись відповідних заходів для збереження деяких деталей в таємниці з міркувань національної безпеки та захисту приватного життя.

5.5. Оцінка систем контролю

На території Ради Європи досягнуто істотного прогресу в організації зовнішнього контролю за службами безпеки, але далеко не всі країни пішли далі, проводячи аналіз ефективності окремих контролюючих органів, не говорячи вже про системи контролю[109]. Законодавчо створивши контролюючі органи, у багатьох випадках 10-20 років тому, більшість країн не переглядало їх організацію або робило це тільки після гучних скандалів або провалів розвідки. Тому дуже важко з'ясувати, зокрема, чи займаються системи контролю найбільш актуальними аспектами діяльності служб безпеки; чи ефективно вони сприяють кращому додержанню прав людини в політиці, операціях і правилах служб безпеки; чи використовують ефективні методи та чи проводять достатньо суворі розслідування; чи користуються вони довірою суспільства; чи надають вони точні й корисні звіти.

Як показано вище, для того, щоб системи контролю ефективно попереджали й реагували на побоювання щодо прав людини в роботі або у зв'язку з роботою служб безпеки, їм необхідний відповідний юридичний мандат і повноваження, ресурси та знання. Ці вимоги зростають з розвитком характеру, масштабів і технологій, що застосовуються у роботі служб безпеки.

Тому важливо, щоб системи контролю періодично оцінювалися на предмет наявності або відсутності необхідних характеристик.

Пов'язане з цим питання – чи можна вважати, що контролюючі органи (і, більш широко, системи контролю) ефективно виконують свої функції – перебуває поза залежністю від адекватності їх правового мандату, повноважень і ресурсів. Воно включає оцінку ефективності забезпечення відповідності політики, операцій і практик служб безпеки правам людини, а також

109. Серед винятків – Бельгія і Нідерланди: Senat et Chambre des Representants de Belgique, «Evaluation du fonctionnement des Comites permanent de controle des services de police et de renseignements», Rapport fait au nom des commissions speciales chargees du suivi parlementaire des Comites permanent de controle des services de police de renseignements par MM. Foret and De Crem, 16 février 1996. 437/1 – 95/96 Chambre, 1-258/1 Senat; Fijnaut 2012.

розгляду та реагування на скарги, що сприяє відшкодуванню збитків та організаційному вдосконаленню. Оцінка таких питань вимагає глибокого аналізу функціональності методів і підходів роботи контролерів. Тому перш ніж розпочати офіційну оцінку, варто подивитися, як можна оцінити ефективність контролю і, зокрема, як можна оцінити здатність системи контролю захистити права людини[110]. Це є темами для подальшого обговорення і потенційної роботи на європейському рівні.

Парламенти і міністри можуть відігравати важливу роль щодо цього, забезпечуючи включення положень про оцінку в законодавство про служби безпеки і контроль за ними[111]. Як варіант, виконавча влада, парламент або контролюючі органи можуть формувати такі оцінки на тимчасовій основі, як це нещодавно було зроблено в Нідерландах. Альтернативна, або додаткова, модель прийнята у Великобританії, де є незалежний рецензент законодавства з питань тероризму (*Independent Reviewer of Terrorism Legislation*)[112]. Хоча його бюро займається законодавством про боротьбу з тероризмом більш широко, ця посадова особа розглядає адекватність положень закону, що стосуються контролю, і вповноважений давати відповідні рекомендації.

110. Докладніше див.: Wills 2012b: 471-499.
111. Найкращий приклад щодо цього ми маємо за межами території Ради Європи: Canada 1984: § 56; Canada 1990.
112. Див.: https://terrorismlegislationreviewer.independent.gov.uk/, accessed 28 March 2015.

Посилання

Article 29 Working Party (2014a), Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, 819/14/EN WP 215, 10 April 2014.

Article 29 Working Party (2014b), Joint Statement of the Article 29 Working Party, adopted 26 November 2014.

Balkan Insight (2015a), «Serbian ombudsman complains of threats», 21 January 2015: www.balkaninsight.com/en/article/, accessed 28 March 2015.n-aftermilitary-secret-service-revelation, accessed 28 March 2015.

Balkan Insight (2015b), «Macedonia PM accused of large-scale wire-tapping», 9 February 2015: www.balkaninsight.com/en/article/eavesdropping-bombshell-explodes-in-macedonia, accessed 28 March 2015.

BBC News (2015), «Sim card firm links GCHQ and NSA to hack attacks», 25 February 2015: www.bbc.co.uk/news/technology-31619907, accessed 28 March 2015.

Belgian Standing Intelligence Agencies Review Committee (2011), Annual report 2010-2011, Intersentia, Brussels. Available at: www.comiteri.be/images/pdf/publicaties/activity_report_2010-2011.pdf, accessed 28 March 2015.

Belgium (1991), Act governing review of the police and intelligence services and of the Coordination Unit for Threat Assessment 1991. Available at: http://comiteri.be/images/pdf/engels/w.toezicht%20-%20l.control.pdf, accessed 28 March 2015.

Belgium (1998), Law on the Intelligence and Security Services 1998.

Belgium (2010), Law on the Intelligence and Security Services 1998, (as modified by the law on collection of data by the intelligence and security services of 14 February 2010).

Bigo D. et al. (2013), «National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law», European Parliament, Brussels.

Bigo D. et al. (2014), «France's surveillance: justice, freedom and security in the EU», openDemocracy.net, 14 May 2014.

Borger J. (2013), «NSA files: why the Guardian in London destroyed hard drives of leaked files», The Guardian, 20 August 2013.

Borger J. (2014), «Ministers should assess UK surveillance warrants, says Philip Hammond», The Guardian, 23 October 2014.

Born H. and Leigh I. (2005), Making intelligence accountable, Parliament of Norway, Oslo.

Born H., Leigh I. and Wills A. (forthcoming), Making international intelligence cooperation accountable, Parliament of Norway, Oslo.

Bosnia and Herzegovina (2004), Law on the intelligence and security agency of Bosnia and Herzegovina 2004.

Cameron I. (2000), National security and the European Convention on Human Rights, Martinus Nijhof Publishers, The Hague.

Cameron I. (2008), «National Security and the European Convention on Human Rights – Trends and Patterns», speech to the Stockholm International Symposium on National Security and the European Convention on Human Rights, 4-5 December 2008.

Cameron I. (2011), «Parliamentary and specialised oversight of security and intelligence agencies in Sweden», in Wills A. and Vermeulen M. (eds) (2011), «Parliamentary oversight of security and intelligence agencies in the European Union», European Parliament, Brussels.

Cameron I. (2013), «Foreseeability and safeguards in the area of security: some comments on ECHR case law», in Regards sur le controle, Laethem W. (Van) and Vanderborght J. (eds) (2013), Intersentia, Antwerp.

Canada (1984), Canadian Security Intelligence Service Act 1984.

Canada (1990), «In fux but not in crisis», Canada Special Committee on the Review of the CSIS Act and the Security Act (NCJ 131163), Ottawa, Canada. Cobain I. (2013), Cruel Britannia: a secret history of torture, Portobello Books, London.

Commissioner for Human Rights, Council of Europe (2013a), «Human rights and the security sector: report of the round-table with human rights defenders, organised by the Office of the Council of Europe Commissioner for Human Rights, Kyiv, 30-31 May (2013)», CommDH(2013)17.

Commissioner for Human Rights, Council of Europe (2013b), «Human rights at risk when secret surveillance spreads», Human Rights Comment, 24 October 2013.

Commissioner for Human Rights, Council of Europe (2014a), The rule of law on the internet and in the wider digital world, Issue Paper, Council of Europe, Strasbourg.

Commissioner for Human Rights, Council of Europe (2014b), Statement of 12 December 2014: www.facebook.com/permalink.php?story_fbid=377981239044459&id=118705514972034, accessed 28 March 2015.

Commissioner for Human Rights, Council of Europe (2014c), «Report by Nils Muiznieks, Council of Europe Commissioner for Human Rights, following his visit to the Netherlands, from 20 to 22 May 2014», CommDH(2014)18, 14 October 2014.

Commissioner for Human Rights, Council of Europe (2015), «4th quarterly activity report 2014», CommDH(2015)3.

Connolly K. (2014), «Romanian ex-spy chief acknowledges CIA had 'black prisons' in country», The Guardian, 14 December 2014.

Council of Europe (2006a), «Secretary General's report under Article 52 ECHR on the question of secret detention and transport of detainees suspected of terror-

ist acts, notably by or at the instigation of foreign agencies», SG/Inf (2006)5, 28 February 2006.

Council of Europe (2006b), «Secretary General's supplementary report», SG/Inf (2006)13, 14 June 2006.

Croatia (2006), Act on the Security Intelligence System of the Republic of Croatia, 30 June 2006.

CTIVD (2014), «Review report on the processing of telecommunications data by GISS and DISS»? No. 38, 5 February 2014.

Cvrtila V. (2012), «Intelligence governance in Croatia», DCAF. Available at: www.dcaf.ch/content/download/104961/1617969/version/2/fle/croatia_eng1.pdf, accessed 28 March 2015.

Czech Republic (1994), Act on the Security Information Service, Act No. 154 of July 7, 1994.

European Data Protection Authorities (2014), Joint Statement of the European Data Protection Authorities Assembled in the Article 29 Working Party, adopted 26 November 2014, 14/EN WP227.

European Parliament (2001), «Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)», Temporary Committee on the ECHELON Interception System, 11 July 2001, A5-0264/2001.

European Parliament (2007), «Resolution on the alleged use of European countries by the CIA for the transportation and illegal detention of prisoners», 14 February 2007, P6_TA(2007)0032.

European Parliament (2013), «Resolution of 10 October 2013 on alleged transportation and illegal detention of prisoners in European countries by the CIA», P7_TA(2013)0418.

European Parliament (2014), «Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs», A7-0139/2014, 21 February 2014.

Farson S. (2012), «Establishing effective intelligence oversight systems» in Born H. and Wills A. (eds) (2012) Overseeing intelligence service: a toolkit, DCAF, Geneva.

Fijnaut C. (2012), «Het toezicht op de inlichtingen- en veiligheidsdiensten: de noodzaak van krachtiger samenspel, De vertrekpunten en uitkomsten van een gespreksronde», The Hague.

Foldvary G. (2011), «Parliamentary and specialised oversight of security and intelligence agencies in Hungary», Annex A in Wills A. and Vermeulen M. (2011), Parliamentary oversight of security agencies in the European Union, European Parliament, Brussels.

Follorou J. (2014), «Espionnage: comment Orange et les services secrets cooperent», Le Monde, 20 March 2014.

Follorou J. and Johannes F. (2013), «Revelations sur le Big Brother francais», Le Monde, 4 July 2013.

Forcese C. (2012), «Handling complaints about intelligence services», in Born H. and Wills A. (eds), Overseeing intelligence services: a toolkit, DCAF, Geneva.

France (2007), Loi n° 2007-1443 du 9 octobre 2007 portant création d'une délégation parlementaire au renseignement.

Gallagher R. and Greenwald G. (2014), «How the NSA plans to infect 'millions' of computers with malware», The Intercept, 3 December 2014: https://frstlook.org/theintercept/2014/03/12/nsa-plans-infect-millions-computers-malware/, accessed 28 March 2015.

Germany (2001a), Act restricting the Privacy of Correspondence, Posts and Telecommunications (G10 Act), Federal Law Gazette I, p. 1254, revised 2298, last amended by Article 2 of the Act of June 6 2013, Federal Law Gazette I, p. 1482.

Germany (1990b), Act on the Protection of the Constitution (BVerfSch), Federal Law Gazette I, p. 2954, last amended by Article 6 of the Act of June 6, 2013, Federal Law Gazette I, p. 1602.

Germany (1978), Parliamentary Control Panel Act (PKGr), Federal Law Gazette I, p. 453, last amended by the Act of July 29, 2009, Federal Law Gazette I, p. 2346.

Goumaz M. (2014), «Statut special voulu par les espions», Le Temps, 1 July 2014.

Hernes H. (2008), «Effective Remedy with Regard to Secret Surveillance and Security Files», speech to the Stockholm International Symposium on National Security and the European Convention Human Rights, 4-5 December 2008.

Higgins A. (2013), «Luxembourg's prime minister resigns», New York Times, 12 July 2013.

Human Rights Watch (2009), Cruel Britannia, British complicity in the torture and ill-treatment of terror suspects in Pakistan, November 2009.

Human Rights Watch (2014a), Rights in retreat: abuses in Crimea, Human Rights Watch, New York.

Human Rights Watch (2014b), «Turkey: spy agency law opens door to abuse», April 2014: www.hrw.org/news/2014/04/29/turkey-spy-agency-law-opens-door-abuse, accessed 28 March 2014.

Hungary (1995), Act CXXV of 1995 on the National Security Services, section 16(2).

International Commission of Jurists (2009), Assessing damage, urging action: report of the Eminent Jurists Panel on terrorism, counter-terrorism and human rights, ICJ, Geneva.

Italy (2007), Law 127/2007 (as amended 1 August 2012).

Jacobsen A. (2012), «Regional consultation on national security and the right to information», www.right2info.org/resources/publications/national-security-page/european-questionnaires/slovenia-rosana-lemut-strle, accessed 28 March 2015.

Jacobsen A. (2013), «National security and the right to information in Europe», April 2013: www.right2info.org/resources/publications/national-security-expert-papers/jacobsen_nat-sec-and-rti-in-europe, accessed 28 March 2015.

JUSTICE (2011), Freedom from suspicion: surveillance reform for a digital age, Justice, London.

Laethem W. (Van) (2011), «Parliamentary and specialised oversight of security and intelligence agencies in Belgium», in Wills A. and Vermeulen M. (2011), «Parliamentary oversight of security and intelligence agencies in the European Union», European Parliament, Brussels.

LAHRC (2015), Draft Resolution adopted by LAHRC on 26 January 2015.

Le Monde (2013), «La DCRI accusee d'avoir illegalement force la suppression d'un article de Wikipedia», 6 April 2013.

Leigh I. (2012), «A view from across the Channel: intelligence oversight in the UK», in Laethem W. (Van) and Vanderborght J. (2012) (eds), Regards sur le controle, Intersertia, Antwerp.

Lithuania (2002), Law on Operational Activities 2002 (as amended).

Marty D. (2011), «Abuse of state secrecy and national security: obstacles to parliamentary and judicial scrutiny of human rights violations», Report for the Committee on Legal Affairs and Human Rights, Doc. 12714, 16 September 2011.

Nemtsova A. (2012), «Putin's secret war,» Foreign Policy, June 2012.

Netherlands (2002), Intelligence and Security Services Act 2002. Available at: www.ctivd.nl/?download=WIV%202002%20Engels.pdf, accessed 28 March 2015.

Norton-Taylor R. (2015), «Britain needs independent scrutiny of intelligence, says former head of MI6», The Guardian, 17 March 2015.

Norway (1981), Criminal Procedure Act, Act of 22 May 1981 No. 25 (as amended).

Norway (1995), Act relating to the Oversight of Intelligence, Surveillance and Security Services Act No. 7 of 3 February 1995. Available at: http://eos-utvalget.no/english_1/legal_framework/content_3/text_ 1401199215164/1401199215664/lovengelsk.pdf, accessed 28 March 2015.

Norway (2012), EOS-Utvalget Committee, Annual Report 2011.

Norway (2013), EOS-Utvalget Committee, Annual Report 2012.

Norway (2014), EOS-Utvalget Committee, Annual Report 2013.

Omtzigt, P. (2015), «Mass surveillance», PACE Committee on Legal Affairs and Human Rights, 26 January 2015, [AS/Jur (2015) 01].

Open Society Foundations (2013), Global Principles on National Security and the Right to Information (Tshwane Principles), adopted on 12 June 2013 in Tshwane, South Africa: www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf, accessed 28 March 2015.

Open Society Justice Initiative (2013), Globalizing torture: CIA secret detention and extraordinary rendition, OSF, New York.

Osborne L. (2013), «Germany denies phone data sent to NSA used in drone attacks», The Guardian, 12 August 2013.

Ottawa Principles on Anti-terrorism and Human Rights, adopted in 2006 in Ottawa, Canada: http://aix1.uottawa.ca/~cforcese/hrat/principles.pdf, accessed 28 March 2015.

Petrovic P. (2012), «Serbia», Strengthening intelligence oversight in the Western Balkans series, DCAF, Geneva. Available at: www.dcaf.ch/content/download/104944/1617879/version/2/fle/serbia_eng1.pdf, accessed 28 March 2015.

Poland (2002), Act of 24 May 2002. Internal Security Agency and Foreign Intelligence Agency.

Pond E. (2013), «What the NSA can learn from Sweden», World Policy Blog, 9 August 2013, www.worldpolicy.org/blog/2013/08/09/what-nsa-can-learn-sweden, accessed 28 March 2015.

Portugal (2004), Intelligence Systems of the Portuguese Republic, Framework Law 4/2004.

Priest D. (2005), «CIA holds suspects in secret prisons», Washington Post, 2 November 2005.

Privacy International (2014), Statement of Grounds submitted to the Investigatory Powers Tribunal, 8 May 2014: www.privacyinternational.org/sites/default/files/PI%20Hacking%20Case%20Grounds.pdf, accessed 28 March 2015.

Protector of Citizens of the Republic of Serbia (2010), «Report on a preventive control visit by the Protector of Citizens to the Security-Information Agency», (Belgrade, 2010). Available at: www.ombudsman.org.rs/ attachments/088_Report%20on%20the%20Preventive%20Control%20Visit.pdf, accessed 28 March 2015.

Protector of Citizens of the Republic of Serbia (2014), Annual Report for 2013. Available at: www. ombudsman.rs/attachments/2013%20Annual%20Report%20of%20the%20Protector%20of%20Citizens.pdf, accessed 28 March 2015.

Review Group on Intelligence and Communications Technologies (2013), «Liberty and security in a changing world», 13 December 2013: www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_fnal_report.pdf, accessed 28 March 2015.

Romania (1991), Law on the National Security of Romania, No. 51/July 29 1991.

Sanchez Ferro S. (2011), «Parliamentary and specialised oversight of security and intelligence agencies in spain», Annex A in Wills A. and Vermeulen M. (2011), «Parliamentary oversight of security agencies in the European Union», European Parliament, Brussels.

Serbia (2014), The Law on Security Information Agency Official Gazette of the Republic of Serbia (as amended in 2014), Official Gazette Nos. 42/2002, 111/2009,65/2014 – US, 66/2014.

Singh A. and Scholes J. (2014), «Denmark, the CIA, and the killing of Anwar al-Awlaki», 30 April 2014: www.opensocietyfoundations.org/voices/denmark-cia-and-killinganwar-al-awlaki, accessed 28 March 2015.

Stark H. (2011), «Germany limits information exchange with US intelligence», Der Spiegel, 17 May 2011.

Stoll M. (2014), «Des documents du SRC peuvent aussi etre publics», Oefentlichkeitsgesetz.ch, 15 December 2014: www.oefentlichkeitsgesetz.ch/francais/2014/12/des-documents-du-src-peuvent-aussi-etre-publics/#more-3569, accessed 28 March 2015.

Townsend M. (2014), «UK rights groups reject official inquiry into post-September 11 rendition», The Observer, 8 November 2014.

Travis A. and Bowcott O. (2015), «UK admits unlawfully monitoring legally privileged communications», The Guardian, 18 February 2015.

Turkey (2014), Law Amending the Law on State Intelligence Services and the National Intelligence Agency, No. 6532, April 2014.

UK (2000), Regulation of Investigatory Powers Act (RIPA) 2000.

UK (2010), «Consolidated guidance to intelligence officers and service personnel on the detention and interviewing of detainees overseas, and on the passing and receipt of intelligence relating to detainees», Cabinet Office, London, July 2010.

Venice Commission (1998), «Internal security services in Europe», 7 March 1998, CDL-INF (98) 6.

Venice Commission (2007), «Report on the democratic oversight of the security services», 11 June 2007, CDL-AD(2007)016.

Venice Commission (2012), «Revised draft opinion on the federal law on the Federal Security Service (FSB) of the Russian Federation», Opinion no. 661/2011.

Venice Commission (2015), «Update of the 2007 Report on the democratic oversight of the security services and report on the democratic oversight of signals intelligence agencies», adopted at the 102nd plenary session (Venice, 20-21 March 2015, CDL-AD(2015)006.

Verhoeven N. (2011), «Parliamentary and specialised oversight of security and intelligence agencies in Germany», in Wills A. and Vermeulen M. (2011), «Parliamentary oversight of security agencies in the European Union», European Parliament, Brussels.

Wills A. (2012a), «Financial oversight of intelligence services,» in Born H. and Wills A. (eds) (2012), Overseeing intelligence services: a toolkit, DCAF, Geneva.

Wills A. (2012b), «Who's watching the overseers? Ad hoc evaluations of intelligence oversight and control bodies», in Laethem W. (Van) and Vanderborght J. (eds), Regards sur le controle, Intersertia, Antwerp.

Wills A. and Vermeulen M. (2011), «Parliamentary oversight of security and intelligence agencies in the European Union», European Parliament, Brussels.

With H. (De) and Kathmann E. (2011), «Parliamentary and specialised oversight of security and intelligence agencies in Germany», in Wills A. and Vermeulen M. (2011), «Parliamentary oversight of security agencies in the European Union», European Parliament, Brussels.

Генеральна Асамблея ООН (2013), Резолюція 68/167, 18 грудня 2013 р., A/RES/68/167.

Генеральна Асамблея ООН (2014), Резолюція 69/166, A/RES/69/166, 18 грудня 2014 р.

Комітет ООН з прав людини (2004), Зауваження загального порядку № 31, UN Doc.CCPR/C/21/Rev.1/Add.13 (2004).

ООН (1987), Конвенція ООН проти катувань та інших жорстоких, нелюдських або таких, що принижують гідність, видів поводження і покарання, 10 грудня 1984 р. (введена в дію 26 червня 1987 р.).

ООН (2010a), «Добірка оптимальних практичних методів, що застосовуються щодо законодавчої та інституціональної основи та заходів, які забезпечують дотримання прав людини спеціальними службами в умовах боротьби з тероризмом, у тому числі стосовно контролю за їх діяльністю», Спеціальний доповідач з питання заохочення і захисту прав людини та основних свобод в умовах боротьби з тероризмом, 17 травня 2010 р., A/HRC/14/46.

ООН (2010b), «Спільне дослідження про глобальну практику у зв'язку з таємним утриманням під вартою в умовах боротьби з тероризмом», Спеціальний доповідач з питання заохочення і захисту прав людини та основних свобод в умовах боротьби з тероризмом, A/HRC/13/42, 19 лютого 2010 р.

ООН (2013), «Доповідь Спеціального доповідача з питань сприяння та захисту права на свободу думок та їх вільного вираження Франка Ла Рю», 17 квітня 2013 р., A/HRC/23/40.

ООН (2014), «Доповідь Спеціального доповідача з питання заохочення і захисту прав людини та основних свобод в умовах боротьби з тероризмом», 23 вересня 2014 р., A/69/397.

ПАРЄ (2005), Парламентська асамблея Ради Європи, Рекомендація 1713 (2005), 23 червня 2005 р.

ПАРЄ (2011), Парламентська асамблея Ради Європи, Резолюція 1838 (2011), 6 жовтня 2011 р.

ПАРЄ (2013), Парламентська асамблея Ради Європи, Резолюція 1954 (2013), 2 жовтня 2013 р.

Рада ООН з прав людини (2009), Резолюція 10/15, 10-а сесія, 26 березня 2009 р.

Управління Верховного комісара ООН з прав людини (2014), «Право на недоторканність особистого життя в цифрове століття», 30 червня 2014 р., A/HRC/27/37, UN High Commissioner for Human Rights. Available at: www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/ A.HRC.27.37_en.pdf, accessed 28 March 2015.

Судові прецеденти

Європейський суд з прав людини

Abu Zubaydah v. Lithuania, Application No. 46454/11, communicated on 14 December 2012.

Al Nashiri v. Poland, Application No. 28761/11, 24 July 2014.

Al Nashiri v. Romania, Application No. 33234/12, communicated on 18 September 2012.

Assenov and Others v. Bulgaria, Application No. 90/1997/874/1086, 28 October 1998.

Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, Application No. 62540/00, 28 June 2007.

Big Brother Watch and Others v. the United Kingdom, Application No. 58170/13, lodged on 4 September 2013 (challenging PRISM and TEMPORA).

Dumitru Popescu v. Romania, Application No. 71525/01, 26 April 2007.

El Masri v. «the former Yugoslav Republic of Macedonia», Application No. 39630/09, 13 December 2012.

Husayn (Abu Zubaydah) v. Poland, Application No. 7511/13, 24 July 2014.

Iordachi and Others v. Moldova, Application No. 25198/02, 10 February 2009.

Kennedy v. the United Kingdom, Application No. 26839/05, 18 May 2010.

Klass and Others v. Germany, Application No. 5029/71, 6 September 1978.

Leander v. Sweden, Application No. 9248/81, 26 March 1987.

Liberty and Others v. the United Kingdom, Application No. 58243/00, 1 July 2008.

Malone v. the United Kingdom, Application No. 8691/79, 2 August 1984.

Nasr and Ghali v. Italy, Application No. 44883/09, communicated on 22 November 2011.

Segerstedt-Wiberg and Others v. Sweden, Application No. 62332/00, 6 June 2006.

Sunday Times v. the United Kingdom (No. 2), Application No. 13166/87, 26 November 1991.

Vetter v. France, Application No. 59842/00, 31 May 2005.

Weber and Saravia v. Germany, Application No. 54934/00, decision on admissibility of 29 June 2006.

Національні суди

Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others, Joined Cases C-293/12 and C-594/12, 14 April 2014.

Liberty & Others vs. the Security Service, SIS, GCHQ, IPT/13/77/H, 6 February 2015.

Ефективний демократичний контроль за діяльністю національних служб безпеки

Координатори проекту:
Іден Коул (Женевський Центр демократичного
контролю над збройними силами),
Валентин Бадрак (Центр досліджень армії, конверсії та роззброєння)

надруковано: Адеф Україна

Тираж: 1000 екз.

Викриття масового стеження за електронними лініями зв'язку вільнонайманим співробітником американської розвідки Едвардом Сноуденом викликали серйозні побоювання щодо порушення права на приватне і сімейне життя, свободи слова і свободи об'єднання. Нинішнім викриттям передували інші, пов'язані з причетністю деяких служб безпеки до серйозних порушень прав людини протягом попередніх десяти років. Все це порушує питання про адекватність правового регулювання і контролю над діяльністю служб безпеки на території Ради Європи.

Ця доповідь насамперед розглядає роль національних інститутів, відповідальних за санкціонування, моніторинг, перевірку та розгляд діяльності служб безпеки і, меншою мірою, органів виконавчої влади, відповідальних за служби безпеки. Зокрема, були розглянуті приклади таких інститутів контролю різних європейських держав: парламентські комітети, судові і квазісудові органи, органи експертного контролю над розвідкою та безпекою, уповноважені з питань даних та інформації, інститути омбудсменів і виконавчої влади та механізми внутрішнього контролю служб безпеки.

Поряд з аналізом національних практик контролю, у цій доповіді також розглянуто зростаючий масив міжнародних принципів «твердого» і «м'якого» права щодо контролю над службами безпеки. Особливу увагу приділено актуальності Європейської конвенції з прав людини та її прецедентному праву в цій галузі. У публікації цілеспрямовано розглянуто контроль над діяльністю, що викликає в цей час побоювання щодо прав людини, включаючи співробітництво зі службами безпеки і розвідки інших держав, невибіркове масове стеження за електронними лініями зв'язку та проникнення в комп'ютерні мережі (хакерство).

У доповіді міститься ряд рекомендацій щодо того, як можна підсилити контроль над службами безпеки для забезпечення кращого захисту прав людини в цій сфері діяльності держави. Визнаючи, що єдиної «ідеальної» моделі або системи контролю не існує, рекомендації пропонують принципи, що можуть бути реалізовані у будь-якій політичній або конституційній системі.

www.commissioner.coe.int

UKR

www.coe.int

Рада Європи є провідною організацією із захисту прав людини континенту. Вона включає в себе 47 держав-членів, 28 з яких є членами Європейського союзу. Усі держави-члени Ради Європи підписалися під Європейською конвенцією з прав людини – договір, спрямований на захист прав людини, демократії та верховенства закону. Європейський суд з прав людини контролює здійснення Конвенції у державах-членах.

COMMISSIONER FOR HUMAN RIGHTS
COMMISSAIRE AUX DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE