Рамкова програма співробітництва
для Вірменії, Азербайджану, Грузії, Республіки Молдова, України й Білорусі
Programmatic Cooperation Framework for
Armenia, Azerbaijan, Georgia, Republic of Moldova, Ukraine and Belarus
Funded by the European Union and the Council of Europe
Implemented by the Council of Europe
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Спільний проект Європейського Союзу та Ради Європи
«Посилення імплементації європейських стандартів прав людини в Україні»

Подальша підтримка реформи кримінальної юстиції в Україні
MINISTRY OF FOREIGN AFFAIRS OF DENMARK
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

DGI(2016) 19
(номер англ. оригіналу)
3 листопада 2016 р.
Переклад з англійської

ВИСНОВОК ГЕНЕРАЛЬНОГО ДИРЕКТОРАТУ З ПРАВ ЛЮДИНИ ТА ВЕРХОВЕНСТВА ПРАВА РАДИ ЄВРОПИ

НА ПРОЕКТ ЗАКОНУ УКРАЇНИ № 4778 «ПРО ОПЕРАТИВНО-РОЗШУКОВУ ДІЯЛЬНІСТЬ»

Підготовлено на основі експертного аналізу Брайана Чепела, Ральфа Роша, Сари Ширазян та Еріка Сванідзе

Зміст

1. Резюме……………………………………….……….……………..……...3

2. Вступ ……..…………..…………..……………..…………..……………4

3. Європейські стандарти ……………………………………...………………6

4. Загальні зауваження……………………………………………….…….… .14

5. Постатейні коментарі ……………………………………………….……. . 22

6. Перелік рекомендацій………………………………………….…………. .. 36

1. Резюме

1.1 Цей висновок стосується проекту Закону України «Про оперативно-розшукову діяльність», що, за намірами, повинен підвищити ефективність відповідних органів у здійсненні оперативно-розшукової діяльності та забезпечити відповідність європейським стандартам

1.2 Існує ціла низка європейських стандартів, яких стосується проект Закону, зокрема, щодо негласного спостереження та захисту даних. Негласне спостереження підіймає істотні питання відповідності стандартам, зі значним акцентом на процесуальних гарантіях. Технологічний прогрес останніх часів ставить нові задачі у забезпеченні права на повагу до приватного життя та в забезпеченні того, щоб будь-яку обробку персональних даних здійснювали належним чином і з чітко визначеною метою. Цей висновок розглядає в деталях найрелевантніші з цих стандартів.

1.3 Законопроект комплексно вирішує завдання розробки законодавчої бази діяльності органів, що відповідають за захист національної (державної) безпеки, розслідування тяжких злочинів і організованої злочинності та інших злочинів, визначених українською державою. Він передбачає широкий набір гласних і негласних слідчих тактик, регулює питання отримання дозволів на використання заходів та питання відповідальності.

1.4 Проте у цій законодавчій базі наявна низка недоліків та прогалин, що потрібно виправити для забезпечення відповідності європейським стандартам та вимогам Кримінального процесуального кодексу України (КПК). Ряд рекомендацій, наданих у цьому висновку, спрямовані насамперед на підвищення рівня процесуальних гарантій у Законопроекті (зокрема, тих, що стосуються судового контролю й нагляду) та розробку орієнтирів для використання конкретних повноважень, включно з, за можливістю, загальнодоступною інформацією.

1.5 Приклади рекомендацій включають чітке встановлення підстави для початку оперативно-розшукової діяльності та визначення видів злочинів, щодо яких її може бути розпочато, забезпечення повідомлення осіб, до яких застосовували приховане спостереження, після його завершення, узгодження Законопроекту з вимогами КПК щодо прокурорського та судового нагляду, мінімальні умови для затримання, введення інформації до Єдиного реєстру досудових розслідувань тощо. Крім того, визначення, наведені у Законопроекті, мають відповідати тим, що закріплені КПК, щоб забезпечити узгодженість та запобігти зловживанням передбаченими ним повноваженнями. У Законопроекті також є низка питань, які варто було б прояснити, наприклад, обставини, за яких можна використовувати таємних інформаторів (Covert Human Intelligence Sources).

1.6 Ще один комплекс рекомендацій стосується відповідності Європейським стандартам захисту даних та захисту прав дітей.

1.7 Як було пояснено вище, Законопроект є містким та має потенціал для надання правоохоронним органам та органам безпеки комплексною законодавчою базою для підтримки їхньої діяльності, однак, є аспекти, у яких його варто було б допрацювати та питання, які варто більш ретельно врегулювати, спираючись на аналогічне законодавство.

1.8 Успішне виконання рекомендацій, що містяться в цьому висновку, забезпечать більш повне досягнення мети впровадження європейських стандартів та ще більше вдосконалить Законопроект, надаючи міцне підґрунтя законному й ефективному використання оперативно-розшукової діяльності відповідними українськими органами.

2. Вступ

2.1 У цьому висновку проаналізовано проект Закону України №4778 «Про оперативно-розшукову діяльність» («Законопроект»), що внесений до Верховної Ради України.

2.2. У Законопроекті зазначено, що він спрямований на зменшення бюрократії та підвищення ефективності роботи підрозділів з розслідування злочинів, а також забезпечення дотримання стандартів у галузі прав людини[1]. Як зазначено у пояснювальній записці до Законопроекту, його метою є «удосконалення правових засад здійснення оперативно-розшукової діяльності, приведення її у відповідність із європейськими стандартами, які висуваються до діяльності, пов'язаної з тимчасовим обмеженням прав і свобод людини, синхронізації оперативно-розшукової діяльності та процесуальної діяльності, яка здійснюється відповідно до приписів Кримінального процесуального кодексу України («КПК»)». Згідно з пояснювальною запискою, це необхідно з огляду на низку причин:

- Чинний Закон України «Про оперативно-розшукову діяльність» був прийнятий у 1992 році, коли Україна ще не була членом Ради Європи і стороною Європейської конвенції з прав людини («Конвенції»);

- Новий КПК України, прийнятий у 2013 році, викликав ряд практичних проблем щодо здійснення оперативно-розшукових заходів. Наприклад, положення статті 214 КПК, за яким усі повідомлення про дійсні чи можливі кримінальні правопорушення вносяться до Єдиного реєстру досудових розслідувань протягом 24 годин з моменту отримання таких повідомлень.

- Започаткування нових правоохоронних органів (Національного антикорупційного бюро України та Державного бюро розслідувань) викликало потребу у створенні послідовного підходу до отримання дозволу та проведення оперативно-розшукової діяльності різними органами.

2.3 У цьому висновку Законопроект проаналізовано на предмет його відповідності європейським стандартам, зокрема, вимогам Конвенції та протоколів до неї у світлі практики Європейського суду з прав людини («ЄСПЛ»). У висновку розглянуто концептуальний підхід Законопроекту та його потенційний вплив на систему кримінального судочинства. Крім того, у висновку проаналізовано, наскільки Законопроект узгоджується з останніми змінами до КПК.

2.4 Висновок підготовлено в рамках проекту Ради Європи «Подальша підтримка реформи кримінальної юстиції в Україні», що фінансується урядом Данії, та спільного проекту Ради Європи і Європейського Союзу «Посилення імплементації європейських стандартів прав людини в Україні». Коментар базується на перекладі українського тексту Законопроекту на англійську мову[2].

2.5 Законопроект був проаналізований групою консультантів Ради Європи:

Браян Чепел, незалежний консультант з кримінальної юстиції, старший викладач-сумісник Інституту кримінальної юстиції Університету Портсмута, де читає лекції для бакалаврів та аспірантів. Спеціалізується на питаннях розслідування кримінальних справ, оперативної інформації, організованої злочинності, а також етики, лідерства та управління в сферах

[1] Пояснювальна записка до Законопроекту (серпень 2016 р.).

2 Переклад підготовлено в рамках проекту Ради Європи «Продовження підтримки реформи кримінальної юстиції в Україні», що фінансується коштом Уряду Данії, та спільного проекту Ради Європи і Європейського Союзу «Посилення імплементації європейських стандартів прав людини в Україні».

оперативної інформації та розслідування злочинів. Має 30-річний досвід роботи у міській поліції Лондона (Новий Скотланд Ярд), де працював старшим детективом та головою оперативної служби експертного управління. Має практичний та управлінський досвід в усіх аспектах активного розслідування злочинів, розробки та аналізу оперативної інформації, а також підготовки експертів для місцевої та закордонної поліції та зовнішніх органів, у тому числі національний та міжнародний стратегічний досвід у забезпеченні кращих практик та дотримання прав людини у контексті таємних поліцейських операцій. Очолював низку проектів з розбудови спроможності міжнародних правоохоронних органів. Має ступінь доктора кримінальної юстиції (DCrimJ) Портсмутського університету і ступінь магістра з питань досліджень інформації та безпеки Університету Брунеля.

Ральф Рош навчався у Трініті Коледж в Дубліні, Університетському коледжі в Дубліні та Королівському університеті Белфасту. Адвокат, допущений до практики у Північній Ірландії, Англії та Вельсі. Має багатий досвід роботи у галузі прав людини, зокрема, працював старшим міжнародним юристом у Палаті з питань прав людини для Боснії та Герцеговини, а також у Незалежній судовій комісії Боснії та Герцеговини, що відповідала за комплексне впровадження судової реформи. Має низку публікацій, у тому числі посібник «Європейська конвенція з прав людини та діяльність поліції», написаний у співавторстві з професором Джимом Мердоком і опублікований Радою Європи у 2013 році. Розробив і викладав навчальні курси для слідчих МВС України, у т.ч. курс «Гарантії прав людини на етапі досудового розслідування», що проходив у Києві у 2014 році.

Сара Ширазян -- юрист-міжнародник, спеціалізується на питаннях громадянських свобод, захисту даних і національної безпеки. Працює консультантом Ради Європи, відповідає за розробку навчальних програм з європейських стандартів у галузі конфіденційності та захисту даних в рамках проекту «Освіта у галузі прав людини для професійних юристів у 28 країнах-членах Європейського Союзу» (’HELP in the 28’). Раніше працювала юристом в Європейському суді з прав людини; займалася питаннями ядерної безпеки; розслідувала міжнародну торгівлю наркотиками в секретаріаті Інтерполу. Наразі отримує ступінь доктора юридичних наук (J.S.D.) в Університеті Стенфорда. У Стенфорді викладає курс американської зовнішньої політики та демократії і соціального підприємництва. До Стенфордського університету викладала у Державному університету Єревану (Вірменія), де розробила і читала магістерські курси з міжнародного права прав людини та міжнародного публічного права. Працювала у проекті Американської асоціації юристів «Ініціатива з верховенства права», впроваджувала реформи кримінальної юстиції у Вірменії.

Ерік Сванідзе, юрист та експерт-міжнародник, консультант Ради Європи, раніше – прокурор у Грузії, заступник Міністра юстиції, член та експерт Європейського комітету з питань запобігання катуванням, член групи консультантів Ради Європи, що здійснили експертну оцінку нового КПК України, Закону України «Про прокуратуру» (у т.ч. відповідний висновок Венеціанської комісії), Закону України «Про Державного бюро розслідувань» та інших нормативно-правових актів. Отримав ступінь магістра права з питань прав людини Університету Лунда, Швеція. Зараз очолює проект ЄС з моніторингу юстиції у Вірменії.

3. Європейські стандарти

Вступ

3.1 Метою цього розділу є надати короткий опис головних європейських стандартів у галузі захисту даних і негласного спостереження за особами[3].

3.2 Європейським країнам доводиться боротися із різноманітними чинниками, що загрожують безпеці їхніх громадян. Щоби захистити тих, хто знаходиться під їхньою юрисдикцією, держави повинні дати правоохоронним та розвідувальним органам необхідні повноваження, що забезпечать їх можливість працювати ефективно. За певних обставин правоохоронні органи повинні вживати слідчі чи захисні заходи, а невжиття цих заходів може призвести до порушення позитивних або процесуальних зобов'язань держави за статтею 2 Конвенції[4].

3.3 «Негласне спостереження» передбачає право перехоплювати повідомлення, проводити негласні обшуки та інші повноваження, передбачені Законопроектом. Згідно практики ЄСПЛ, цей термін включає спостереження і фіксацію переміщень людини, використання таємних пристроїв прослуховування та перехоплення повідомлень[5].

3.4 Останніми роками відбувається стрімкий безперервний процес розвитку новітніх технологій для таємного спостереження, включаючи технології для розпізнавання обличь та збору й аналізу великих обсягів даних. ЄСПЛ відзначає «масштаби втручання у приватне життя, що стає можливим завдяки появі нових, все більш складних технологій»[6]. Парламентська Асамблея Ради Європи зі стурбованістю відзначає масовий розвиток «спостережно-промислового комплексу"[7], що створює небезпеку для прав громадян європейських країн.

3.5 Негласне спостереження за своєю природою несе у собі загрозу свавілля та зловживань, і ЄСПЛ відзначив «ризик того, що система негласного спостереження, створена з метою захисту національної безпеки, може підірвати й навіть знищити демократію під прикриттям її захисту»[8]. Європейська історія пам'ятає чимало випадків, коли авторитарні режими використовували негласне спостереження для втручання у права осіб, що перебувають під їхньою юрисдикцією. Це вплинуло на практику ЄСПЛ, який дуже прискіпливо оцінює практичне застосування державами заходів негласного спостереження[9]. Комітет міністрів Ради Європи попереджає, що «можливості та практика [масового спостереження] можуть мати згубний вплив на здатність громадян брати участь у соціальному, культурному та політичному житті, а у довгостроковій перспективі можуть мати негативні наслідки для демократії»[10].

---

[3]Термін «негласне спостереження» використовується Європейським судом з прав людини і, відповідно, у тексті цього висновку.

[4]Див, наприклад, посібник «Європейська конвенція з прав людини та діяльність правоохоронних органів» за авторством Дж. Мердока і Ральфа Роша, Рада Європи (2013), стор. 64.

[5]Гаріс, О'Бойль і Ворбрік, Право Європейської конвенції прав людини, видання 3-тє (2014), стор. 555.

[6]*Кьопке проти Німеччини (Köpke v. Germany),* рішення від 5 жовтня 2010 року, заява № 420/07.

[7]Резолюція 2045 (2015) «Масове спостереження», доступне за посиланням: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21692&lang=en

[8] *Роман Захаров проти Росії (Roman Zakharov v. Russia*), рішення (Велика Палата) від 4 грудня 2015 р, заява № 47143/06, пункт 232.

[9] Див., наприклад, *Коп проти Швейцарії (Kopp v. Switzerland),* рішення від 25 березня 1998 року, заява № 23224/94.

[10]Декларація Комітету міністрів про ризики для основоположних прав людини, що виникають із цифрового спостереження та інших спостережних технологій (прийнято 11 червня 2013 року на 1173-й зустрічі міністрів).

3.6 Наразі відбувається стрімкий розвиток галузі права, що регулює утримування, зберігання та обмін даними, здобутими під час негласного спостереження. Про неї і піде мова у тих розділах цього висновку, де Законопроект проаналізовано на предмет його відповідності стандартам у сфері захисту інформації.

Повага до права на особисте життя

3.7 Негласне спостереження за особою чи групою осіб неодмінно призводить до втручання у їхнє право на повагу до особистого життя, гарантованого статтею 8 Конвенції. У ситуаціях, що охоплюються Законопроектом, особи, щодо яких проводиться розслідування, дуже часто не повинні знати про те, що їхня кореспонденція та інші аспекти приватного життя підлягають моніторингу. Як наслідок, як зазначив ЄСПЛ, «особливо коли повноваження представників виконавчої влади здійснюються таємним чином, ризики свавілля очевидні»[11]. Це ще раз говорить про необхідність запровадження чітких і доступних правил, що визначають обставини, за яких правоохоронним органам дозволяється перехоплювати особисті повідомлення та використовувати інші заходи негласного спостереження[12].

3.8 Утримування та зберігання інформації на постійній основі є порушенням права на повагу до особистого життя, а отже, потребує обґрунтування[13].

3.9 Парламентська Асамблея Ради Європи зазначила, що «необхідно створити нормативно-правову базу національного та міжнародного рівня, що забезпечить захист прав людини, особливо права на повагу до особистого життя»[14].

«Згідно із законом»

3.10 ЄСПЛ зазначав, що втручання у право на повагу до особистого життя може бути виправданим лише тоді, коли воно відбувається «згідно із законом». Це «передбачає, щоби відповідний захід базувався на положеннях національного законодавства і відповідав принципу верховенства права, що прямо зазначений у Преамбулі до Конвенції і є невід'ємною складовою об'єкта й цілей статті 8. Таким чином, закон повинен задовольняти критерії якості: він має бути доступним для відповідної особи та передбачуваним щодо своїх наслідків»[15]. Немає потреби забезпечувати особі можливість «точно знати, коли її можуть прослуховувати», адже «це зводить нанівець саму суть негласного спостереження»[16]. Проте «національне законодавство має бути достатньо чітким, щоби забезпечити громадянам достатнє розуміння вказівки щодо обставин, за яких, та умов, на яких органи влади мають право вдаватися до таких заходів»[17].

3.11 У низці країн закони, що регулюють негласне спостереження, доповнюється підзаконними актами, наприклад внутрішніми інструкціями відповідних міністерств чи

[11] Там само, пункт 229.
[12] *Малоун проти Сполученого Королівства (Malone v. United Kingdom),* рішення від 2 серпня 1984 р., заява № 8691/79.
[13] *Ротару проти Румунії (Rotaru v. Romania),* рішення від 4 травня 2000 року (Велика палата), заява № 28341/95.
[14] Резолюція 2045 (2015) «Масове спостереження», доступне за посиланням: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21692&lang=en
[15] *Роман Захаров проти Росії (Roman Zakharov v. Russia)*, рішення (Велика палата) від 4 грудня 2015 р., заява № 47143/06, пункт 228.
[16] Джейкобс, Вайті та Оуві, Європейська конвенція прав людини, видання 6-те, видавництво Оксфордського університету (2014), стор. 371.
[17] *Сантаре та Лабазніковс проти Латвії (Šantare and Labaznikovs v. Latvia),* рішення від 31 березня 2016, заява № 34148/07, пункт 53.

кодексами поведінки. У Великобританії низка таких кодексів є публічними; вони регулюють такі питання, як рівні та порядок отримання дозволів на застосування різних видів негласного спостереження, і досить докладно описують ситуації, коли можна отримати цей дозвіл. ЄСПЛ визнав, що це забезпечує достатню доступність закону[18]. Конституційний, Верховний чи інший суд може тлумачити і застосовувати положення первинного законодавства, але він не повинен розмивати чи знищувати передбачені ними гарантії правового захисту. Так, ЄСПЛ вирішив, що рішення хорватських судів, які по суті скасовували вимогу отримання попереднього дозволу на здійснення негласного спостереження, суперечать статті 8 Конвенції.[19]

3.12 Наступним важливим аспектом вимоги «відповідності [заходів негласного спостереження] закону» є наявність адекватних гарантій захисту від зловживань[20]. Ця вимога виконується, якщо положення закону достатньо чіткі і дають людям належні орієнтири, щоби визначити, за яких умов і обставин може використовуватися негласне спостереження. Яскравим прикладом ситуації, коли закону бракує достатніх гарантій захисту від зловживань, є справа *Малоун проти Сполученого Королівства (Malone v. United Kingdom)*[21]. Справа стосувалася перехоплення кореспонденції. Суд вирішив, що «неясність та невизначеність щодо статусу закону»[22], зокрема, надані міністерствам дискреційні повноваження, означають, що відповідні положення не можуть вважатися «згідними з законом» у розумінні Конвенції.

3.13 Обсяг необхідних гарантій певною мірою залежить від того, наскільки серйозним є втручання в особисте життя особи в результаті використання оперативно-розшукового заходу. Наприклад, використання пристрою для відстежування транспортних засобів, який фіксує їхнє переміщення, становить менше втручання, ніж запис розмов усередині цих транспортних засобів, тому що у першому випадку не відбувається розкривання поглядів, поведінки чи почуттів особи[23]. Натомість, направлення перевдягненого агента із звукозаписувальними пристроями до приватного помешкання особи було визнано «по суті ідентичним» перехопленню телефонних розмов з огляду на характер його втручання в особисте життя[24].

Законна мета

3.14 Якщо використання заходів таємного спостереження передбачено законом, що відповідає вимогам законності та необхідності, на них є відповідний дозвіл і вони проводяться у відповідності із законом, виникає наступне запитання: чи переслідують вони законну мету? Приклади законної мети: запобігання злочину, охорона громадської безпеки, охорона прав та свобод інших осіб тощо. Водночас, слідчі заходи, що призводять до втручання у права людини, можуть використовуватися лише для розслідування серйозних злочинів. Так, ЄСПЛ розкритикував уряд-відповідача за перехоплення телефонних розмов для розслідування дрібної кишенькової крадіжки[25]. Крім того, свобода розсуду, надана правоохоронним органам, не повинна бути надмірно широкою. Так, російський закон «Про

[18] *Р.Е. проти Сполученого Королівства (R.E. v. United Kingdom),* рішення від 27 жовтня 2015 р., заява № 62498/11, пункти 121.
[19] *Драгожевіч проти Хорватії (Dragojević v. Croatia)*, рішення від 15 січня 2015 р., заява № 68955/11, пункти 94-102.
[20] *Клас проти Німеччини (Класс v.Germany),* рішення від 6 вересня 1978 р., заява № 5029/71, пункт 50.
[21] Там само.
[22] Там само, пункт 79.
[23] *Узун проти Німеччини (Uzun v. Germany),* рішення від 2 вересня 2010 р., заява № 35623/05, пункт 52.
[24] *Биков проти Росії (Bykov v. Russia),* рішення від 10 березня 2009 р., заява № 4378/02, пункт 79.
[25] *Роман Захаров проти Росії (Roman Zakharov v.Russia)*, рішення від 4 грудня 2015 р., заява № 47143/06, пункт 244.

оперативно-розшукові заходи» від 12 серпня 2005 року надавав «правоохоронцям необмежені повноваження визначати, за яким умов він застосовується»[26]; Суд вирішив, що в цьому випадку ефективний судовий нагляд за процедурами відсутній. У справі щодо Франції Суд визнав, що оскільки закон не визначає види злочинів, для розслідування яких дозволяється прослуховувати телефонні розмови, це становить порушення статті 8 Конвенції[27].

Нагляд за використанням права на здійснення негласного спостереження

3.15 Основоположним елементом процесуальних гарантій захисту прав людини є наявність незалежного контролю за використанням заходів негласного спостереження. Це потрібно, щоби забезпечити «достатні та ефективні гарантії проти зловживань»[28] з боку органів влади. При цьому ЄСПЛ не зазначив, як саме це відбувається. Так, контроль може знадобитися, «коли спостереження лише починається, проводиться або вже завершилося»[29].

3.16 ЄСПЛ опікується насамперед якістю системи контролю. У більшості країн континентальної системи права, зокрема в Україні, дозвіл на використання заходів спостереження, що приводять до особливо сильного втручання у права особи, надається незалежним судовим або квазі-судовим органом. Це може бути слідчий суддя або прокурор. У країнах системи загального права, зокрема, у Великобританії та на Кіпрі, практикується використання внутрішніх дозволів та застосування зовнішнього незалежного контролю. У справі *Кеннеді проти Сполученого Королівства (Kennedy v. United Kingdom)* ЄСПЛ проаналізував функції комісара з перехоплення кореспонденції. Комісар призначається у відповідності до національного законодавства і перевіряє відповідність дозволів на перехоплення повідомлень положенням відповідних законодавчих актів[30]. Хоча дозволи на використання заходів негласного спостереження надає міністр, ЄСПЛ зазначив, що «роль комісара у забезпеченні правильного застосування (національного законодавства) є надзвичайно важливою: кожні два роки він вибірково переглядає справи, у яких використовувалося негласне спостереження, здійснюючи тим самим необхідний контроль за діяльністю правоохоронних органів»[31].

3.17 Одним з головних способів забезпечення контролю над використанням негласного спостереження є подальше повідомлення особи, до якої воно застосовувалося. У свіжій справі щодо Угорщини Суд зазначив, що «оскільки повідомлення може надаватися після завершення спостереження без шкоди для мети обмеження, то особам слід надавати відповідну інформацію»[32]. Отже, хоча і не існує суворого правила про подальше повідомлення особи, відсутність такого повідомлення вимагає серйозного обґрунтування, наприклад, ризик розкриття особи інформатора. Це пояснюється тим, що в разі неповідомлення особа, за якою стежили, дуже обмежується у можливості оскаржити цей захід в суді.

---

[26] Там само, пункт 266.
[27] *Хувіг проти Франції (Huvig v. France),* рішення від 24 квітня 1990 р., заява № 11105/84.
[28] *Роман Захаров проти Росії (Roman Zakharov v.Russia)*, рішення від 4 грудня 2015 р., заява № 47143/06, пункт 232.
[29] Там само, пункт 233.
[30] Закон про регулювання слідчих повноважень (2000). Робота над законом про слідчі повноваження, що буде прийнятий на заміну старому закону, зараз перебуває на кінцевому етапі підготовки.
[31] *Кеннеді проти Сполученого Королівства (Kennedy v. United Kingdom),* рішення від 18 травня 2010 року, заява № 26839/05, пункт 166.
[32] *Шабо та Віссі проти Угорщини (Szabó and Vissy v. Hungary),* рішення від 12 січня 2016 р., заява № 37138/14, пункт 86.

3.18 ЄСПЛ звертає увагу не лише на законодавчу основу існування контрольних механізмів, а й на їхню ефективність. Важливо, щоби ці механізми мали необхідні ресурси і були інституційно спроможні виконувати свої функції і повноваження. Необхідно передбачити законодавчі положення, на підставі яких ці органи повинні мати доступ до усіх документів, необхідних для перевірки підстав застосування заходів негласного спостереження[33]. ЄСПЛ вирішив, що російський закон «Про оперативно-розшукові заходи» від 12 серпня 2005 року та Кримінально-процесуальний кодекс від 18 грудня 2001 року порушують цю вимогу, оскільки не зобов'язують правоохоронні органи надавати суддям інформацію щодо використання таємних агентів та подробиці оперативно-розшукових заходів[34]. Крім того, ЄСПЛ розкритикував відсутність законодавчої вимоги про розумні підстави підозрювати у вчиненні злочину осіб, до яких ці заходи застосовуються[35]. Інформація про діяльність контрольних механізмів підлягає оприлюдненню[36]; при цьому необхідно забезпечити захист конфіденційної інформації.

Захист даних

3.19 Цей висновок базується на ключових європейських правових інструментах з питань захисту персональних даних: Конвенції, включаючи відповідну практику Європейського суду, Конвенції Ради Європи про захист осіб стосовно автоматизованої обробки персональних даних та додаткового Протоколу до неї; рекомендації Комітету міністрів державам-членам Ради Європи № R.(87) 15 стосовно використання персональних даних у правоохоронному секторі. У необхідних випадках наводяться посилання на відповідні стандарти Європейського Союзу, такі як Директива ЄС 95/46/ЕС про захист осіб щодо обробки персональних даних та про вільний рух таких даних; Рамкове рішення Ради 2008/977/ЈНА[37], Директива 2002/58/ЕС про електронну приватність, Директива 2006/24/ЕС,[38] про збереження даних, Висновок Генерального адвоката Суду справедливості Європейського Союзу, пана Круза Віялона, щодо Директиви 2006/24/ЕС про збереження даних, рішення Суду справедливості у справах «Діджітал райтс Ірландія та ін.» (*Digital Rights Ireland and Others*) та «Шремс» (*Schrems*)[39].

---

[33] *Там само*.

[34] *Роман Захаров проти Росії (Roman Zakharov v.Russia)*, рішення від 4 грудня 2015 р., заява № 47143/06, пункти 257-267.

[35] *Там само*.

[36] *Кеннеді проти Сполученого Королівства (Kennedy v. United Kingdom),* рішення від 18 травня 2010 року, заява № 26839/05, пункт 166; *Роман Захаров проти Росії (Roman Zakharov v.Russia),* рішення від 4 грудня 2015 р., заява № 47143/06, пункт 283.

[37] Рамкове рішення 2008/977/ЈНА гарантує низку принципів захисту даних. Ці принципи застосовні лише щодо захисту даних, які обробляють у рамках співпраці поліції та судових органів у кримінальних справах. Натомість Рекомендація R(87)15 має ширший предмет регулювання та закріплює конкретний та повніший набір правил.

[38] Директиву про збереження даних зараз скасовано. Див. Марін, Луїза «Доля Директиви про збереження даних: про масове спостереження та основоположні права у правовому порядку ЄС» (Marin, Luisa. "The fate of the Data Retention Directive: about mass surveillance and fundamental rights in the EU legal order." Research Handbook on EU Criminal Law, Forthcoming (2015)).

[39] На момент підготовки цього висновку було підготовлено Пакет реформ з захисту даних Європейського Союзу. В результаті було прийнято Загальне положення про захист даних 2016/679, Директиву 2016/680, що регулює поводження з даними у ситуаціях, пов'язаних із правоохоронною діяльністю, та Директиву про фіксування імен пасажирів (Директива 2016/68). Хоча Україна і не є членом ЄС, цілком імовірно, що ці законодавчі зміни потягнуть за собою наслідки й поза зобов'язаннями держав-членів Союзу. Основним підзаконним актом ЄС щодо захисту даних досі залишається Директива про захист даних 95/46ЕС, зазначене Загальне положення скоро замінить її. Цей документ вступить у силу з травня 2018 р. та матиме пряму дію в усіх державах-членах ЄС, не потребуючи додаткової імплементації на рівні держав. Пакет реформ з захисту даних також включив Директиву ЄС 2016/680 про захист фізичних осіб в контексті обробки персональних даних уповноваженими органами для цілей запобігання кримінальним правопорушенням, їх розслідування, виявлення, та обвинувачення за них, або виконання кримінальних покарань, а також про вільне переміщення

3.20 Практика ЄСПЛ і відповідні документи Ради Європи у сфері захисту даних визначають широке коло чітких, доступних і практичних стандартів, яким має відповідати цей Законопроект. ЄСПЛ визнав, що збір, зберігання, доступ, використання та поширення персональних даних з метою, наприклад, розвідки чи захисту національної безпеки, якщо вона відрізняється від первинної мети, з якою їх було зібрано, дозволяється, лише якщо це є «вкрай необхідним у демократичному суспільстві». ЄСПЛ визначив набір «мінімальних гарантій від зловживань» щодо цих основоположних прав людини. «Мінімальними гарантіями захисту від зловживань, які, на думку Суду, повинні бути визначені в національному законодавстві, щоби не допустити зловживань повноваженнями», є:[40]

- Характер правопорушень, для розслідування яких може дозволятися використання заходів таємного спостереження;
- Визначення категорій осіб, до яких можуть застосовуватися ці заходи;
- Максимальна тривалість застосування заходів;
- Порядок отримання дозволу на застосування заходів та порядок використання і зберігання отриманих даних; він має бути визначений «у формі, що відкрита для громадського контролю та обізнаності»;
- Заходи безпеки під час передачі даних іншим сторонам;
- Умови, за яких перехоплені дані можна чи необхідно стерти чи знищити[41].

3.21 Щоб оцінити обсяг і межі використання персональних даних під час правоохоронних заходів, необхідно проаналізувати загальні положення українського законодавства у сфері захисту інформації, особливо Закон про захист персональних даних. Надзвичайно важливо забезпечити, щоби загальне українське законодавство у сфері захисту інформації відображало ключові європейські принципи у цій галузі, зокрема, щоби дані (a) отримувалися і оброблялися чесно і законно; (b) зберігалися для визначених законних цілей і не використовувалися у спосіб, що їм суперечить; (c) були достатніми, необхідними та ненадмірними по відношенню до мети, з якою вони зберігаються; (d) були точними, а де це необхідно також актуальними; (e) зберігалися у формі, що дозволяє ідентифікувати суб'єктів

таких даних (більш відома під назвою "Поліцейська директива"). Поліцейська директива замінить Рамкове рішення Ради 2008/977/JHA.

[40] *Вебер і Саравія проти Німеччини (Weber and Saravia v.Germany),* рішення від 29 червня 2006 р., заява № 54934/00. В інших справах ЄСПЛ наголошував на необхідності брати до уваги усі суттєві обставини, включаючи характер, обсяг і тривалість потенційних заходів; підстави, необхідні для отримання дозволу на їхнє застосування; органи, уповноважені давати такі дозволи, застосовувати заходи та контролювати їхнє застосування; засоби правового захисту, передбачені національним законодавством *(Кеннеді проти Сполученого Королівства (Kennedy v. United Kingdom),* рішення від 18 травня 2010 року, заява № 26839/05, пункт 166; див. також рішення у справі *Шимоволос проти Росії (Shimovolos v. Russia),* рішення від 21 червня 2011 року, заява № 30194/09), Суд справедливості ЄС, Шермс, пункт 91. Див. також статтю «Утримування телекомунікаційних даних і права людини: відповідність бланкетного утримування даних трафіку до вимог Конвенції», Патрік Бейєр, Європейський журналі права, випуск 11, № 3, травень 2015 р., стор. 365-375. Інтернет: практика Європейського суду з прав людини, червень 2015 р., доступно за посиланням: http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf.

[41] Корф, Дуве. Експертний висновок для слідчого комітету Бундестагу з питань глобальних систем спостереження, викритих Едвардом Сноуденом, Бундестаг, 1. Парламентське розслідування 18-ти (2014).

даних не довше, ніж це необхідно для мети, з якою ці дані зберігаються[42]. Це важливо, тому що названі принципи становлять основу обробки персональних даних і так само застосовуються у контексті правоохоронних операцій[43].

3.22 Короткий опис ключових європейських стандартів щодо поводження з персональними даними у контексті правоохоронних операцій наведений нижче.

Гарантії захисту	**Характеристики:**
1. Гарантії, що стосуються збору даних під час здійснення правоохоронної діяльності	- Законність обробки, включаючи чітку мету/ обмеження у використанні зібраних даних/мінімізація обсягу даних[44], а також обмеження щодо подальшої обробки; - Чесність в обробці; - Інформування суб'єкта даних; - Обробка окремих категорій даних (конфіденційні/не конфіденційні персональні дані); розподіл суб'єктів даних по категоріях (наприклад, обробка даних стосовно осіб, які не підозрюються у вчиненні злочину, а також дітей).
2. Гарантії, що стосуються контролю та інформування: обов'язки володільців і розпорядників персональних даних.	- Роль і повноваження контрольних органів (контрольні органи повинні мати незалежний статус і бути підзвітними та обиратися парламентом, а не виконавчою гілкою влади); - Попередня консультація з контрольним органом; - Повідомлення контрольного органу, включаючи повідомлення про файли на паперових носіях та тимчасові (ad hoc) файли; - Оцінка впливу на реалізацію права на повагу до приватного життя; ведення журналу доступу до персональних даних та інші розумні заходи; - Безпека обробки даних, повідомлення про порушення права на захист персональних даних.
3. Гарантії, пов'язані з правами суб'єктів персональних даних.	- Інформування суб'єкта даних; - Право суб'єкта даних на доступ до цих даних і

[42] Туркочоріті, Іоанна. «Трансатлантичні потоки даних і виняток "національної безпеки" в європейських правилах у сфері захисту персональних даних: у пошуках законодавчих гарантій захисту від спостереження». Журнал міжнародного права Університету Пенсильванії, випуск 36 (2014), стор. 459-524.

[43] Суд справедливості ЄС у відомій справі за Директивою про збереження даних підкреслив, що обробка даних, яка супроводжується обмеженням основоположних прав індивіда, має відбуватися у повній відповідності із принципами захисту особистих даних, а будь-які обмеження дозволяються лише як виняток і повинні використовуватися дуже вузько. Див. рішення у справі «Діджітал райтс Ірландія та інші» (*Digital Rights Ireland and Others*), номер справи C-293/12 та C-594/12, пункт 52.

[44] Як нещодавно нагадав Суд ЄС у своїх рішеннях у справі *Шремс* (Schrems) та справі *Діджитал Райтс Ірландія та інші (Digital Rights Ireland and Others),* втручання у реалізацію особами права на повагу до приватного життя і права на захист персональних даних має бути обмежене тим, що є вкрай необхідним і співмірним з поставленими цілями, які представляють загальний інтерес, наприклад, попередження, розслідування, виявлення або переслідування за кримінальні правопорушення чи виконання кримінальних покарань.

	обмеження права на доступ; - Право на внесення змін до даних та їх видалення; - Право на заперечення; - Право на подання скарги; звернення до контрольного органу.
4. Гарантії, пов'язані з повідомленням і передачею персональних даних іншим державним органам і приватним установам, третім країнам і міжнародним організаціям.	- Жорстке обмеження щодо мети передачі: лише для попередження, розслідування, виявлення і переслідування за конкретні злочини або для виконання покарань в рамках конкретного провадження/процедури; - Заборона масової, неодноразової і структурованої передачі персональних даних третім країнам; - Обмежувальне тлумачення виключень; - Документування процесу передачі даних; - Вимоги щодо належного рівня захисту під час передачі персональних даних третім країнам (рішення у справі «Шремс проти Комісара із захисту прав даних» (*Shrems v. Data Protection Commissioner*).
5. Гарантії збереження даних і термін зберігання.	- Принцип якості даних; - Точність та надійність (розмежування між даними, які базуються на фактах, і даними, що базуються на суб'єктивних поглядах); - Адміністративні дані (не підпадають під дію правил, які застосовуються до поліції); - Жорсткі правила/процедури знищення/видалення перехоплених даних.

4. Загальні зауваження

4.1 Законопроект комплексно вирішує завдання розробки законодавчої бази діяльності органів, що відповідають за захист національної (державної) безпеки, розслідування тяжких злочинів і організованої злочинності та інших злочинів, визначених українською державою. Він передбачає повний набір гласних і негласних слідчих тактик, що можуть застосовуватися для проведення операцій, як активних так і тих, що базуються на оперативних даних; Законопроект також містить процедури отримання дозволів на використання заходів та регулює питання відповідальності. Нижче наведено кілька зауважень щодо прогалин у цих процедурах, які можна заповнити шляхом поширення еквівалентних положень КПК на оперативно-розшукові заходи за цим Законопроектом. Це приведе українське законодавство у відповідність до законодавства інших європейських країн і полегшить дотримання стандартів у галузі прав людини, що визначені у Конвенції і розтлумачені у рішеннях ЄСПЛ.

4.2 Хоча Законопроект досить лаконічний і може вважатися послідовною законодавчою основою діяльності правоохоронних та безпекових органів з причин, що наведені вище, пропонується допрацювати і вдосконалити низку його положень, спираючись на аналогічне законодавство. Прикладом позитивного підходу до публічності інформації можна вважати Великобританію, де кодекси поведінки правоохоронних органів викладені у публічний доступ, і громадяни можуть ознайомитися з усіма видами негласних заходів, які можуть використовувати правоохоронні, розвідувальні та безпекові органи[45]. Ці кодекси містять детальну інформацію щодо окремих заходів, і ЄСПЛ схвально відгукувався про них у низці рішень[46].

4.3 Перш ніж приступати до детального аналізу Законопроекту, варто згадати, що новоприйнятий КПК - це крок вперед у порівнянні із кримінальним процесом радянської доби, що був надто обтяжливим, містив повтори і передбачав три стадії. Зокрема, новий Кодекс не містить поняття «дізнання», яке передувало формальній стадії кримінального (досудового) розслідування. Третя стадія складалася з судового розгляду та наступних оскаржень. На практиці дізнання являло собою низку оперативних перевірок, що проводилися різноманітними правоохоронними органами та посадовими особами. Існування великої кількості органів, що по суті мали слідчі повноваження, здійснювала негативний вплив на незалежність та законність досудового процесу, права на справедливий суд, інших гарантій та системи кримінальної юстиції загалом.

4.4 Таке розпорошення повноважень між оперативними підрозділами та посадовими особами у минулому призводило до широкомасштабного зловживання цими повноваженнями і створювало сприятливі умови для корупції. Крім того, це призвело до чисельних порушень прав людини, що підтверджується, серед іншого, низкою рішень ЄСПЛ щодо України. Це і таємне утримування осіб та посилання на належні підстави позбавлення свободи і продовження тримання особи під вартою[47]; це і катування і жорстоке поводження,

---

[45] Регулювання британського закону про слідчі повноваження, у тому числі розділу 3 закону про поліцію 1997 року, доступно за посиланням: https://www.gov.uk/government/collections/ripa-codes

[46] Див., наприклад, справу *Кеннеді проти Сполученого Королівства (Kennedy v. United Kingdom),* рішення від 18 травня 2010 р., заява № 26839/05.

[47] Див., наприклад, рішення ЄСПЛ у справах *Осипенко проти України (Osypenko v. Ukraine)*, рішення від 9 листопада 2011 р., заява № 4634/04; *Доронін проти України (Doronin v. Ukraine),* рішення від 19 лютого 2009 р., заява № 16505/02; *Гаркавий проти України (Garkavyy v. Ukraine),* рішення від 18 лютого 2010 р., заява № 25978/07; *Ічін та інші проти України (Ichin and Others v. Ukraine),* рішення від 21 грудня 2010 р., заява № 28189/04 та 28192/04; *Корнєв та Карпенко проти України (Kornev and Karpenko v. Ukraine)* та *Нечіпорук і Йонкало проти України (Nechiporuk and Yonkalo v. Ukraine),* рішення від 21 квітня 2011 р., заява № 42310/04.

часто у поєднанні із забороненими методами отримання доказів[48]; відсутність належної правової бази та процедур, що регулюють негласне спостереження[49]; інші випадки порушень прав людини.

4.5 Отже, відсутність у новому КПК вимоги про необхідність приймати формальне рішення щодо того, чи потрібно починати розслідування кримінальної справи, є розумною. Натомість, новий КПК вимагає реєструвати ці провадження у Єдиному реєстрі досудових розслідувань. Крім того, КПК вимагає, щоб розслідування злочинів і ті, хто їх проводить, дотримувалися комплексної та послідовної системи правил, що включає належні процесуальні гарантії, у тому числі судовий нагляд та залучення підозрюваних та інших осіб, яких це стосується. Новий КПК більше відповідає вимогам Конвенції, ніж попередній, тому що він запровадив елементи змагальності на усіх стадіях кримінального процесу. Наприклад, невикористання у суді доказів, добутих із порушенням вимог КПК, а також заборона залучати до кримінального процесу членів «оперативних підрозділів» без відповідного дозволу.

4.6 Варто зазначити, що як національні, так і міжнародні моніторингові механізми свідчать, що новий КПК призвів до позитивних змін, включаючи зменшення жорстокого поводження та інших серйозних порушень прав людини[50].

4.7 Будь-які реформи такого масштабу завжди створюють складнощі на етапі впровадження, і ця реформа не є винятком. Новий КПК передбачає зміну парадигми у відносинах між основними учасниками процесу, зокрема, правоохоронними органами і прокуратурою.

4.8 Окрім цього КПК передбачає відносно нежорсткі умови для початку кримінального розслідування («обставини, що ймовірно вказують на вчинення кримінального правопорушення»)[51] і встановлює рамки повноважень та завдань різних оперативних підрозділів[52]. У такий спосіб КПК поєднує принцип обов'язку розслідування злочинів та необхідність мати належний рівень функцій та повноважень цих підрозділів. Це перегукується із кращими практиками в інших юрисдикціях, де оперативно-розшукові заходи проводяться з метою збору доказів для підтримки кримінальних звинувачень під керівництвом прокурора. У випадках, коли негласне спостереження було спрямовано насамперед на збір оперативної інформації, це часто призводило до ігнорування принципу верховенства права під час застосування кримінального закону для притягнення до відповідальності винних осіб[53].

---

[48] Див., наприклад, *Афанасьєв проти України (Afanasev v. Ukraine),* рішення від 5 квітня 2005 р., заява № 38722/02; *Вергельський проти України (Vergelskyy v. Ukraine*), рішення від 12 березня 2009 р., заява № 19312/06; Хайло проти України *(Khaylo v. Ukraine),* рішення від 12 листопада 2008 р., заява № 39964/02; *Міхалкова проти України (Mikhalkova v. Ukraine),* рішення від 13 січня 2011 р., заява № 10919/05; *Нечіпорук і Йонкало проти України (Nechiporuk and Yonkalo v. Ukraine)*, рішення від 21 квітня 2011 р., заява № 42310/04.

[49] Див., наприклад, рішення про справі *Михайлюк і Петров проти України (Mikhalyuk and Petrov v. Ukraine),* рішення від 10 грудня 2009 р., заява № 11932/02; *Владімір Поліщук та Світлана Поліщук проти України (Vladimir Polischuk and Svetlana Polischuk v. Ukraine),* рішення від 30 вересня 2010 р., заява № 12451/04.

[50] Див., зокрема, звіт для уряду України щодо візиту Європейського комітету запобігання катуванням та нелюдському і такому, що принижує гідність, поводженню чи покаранню (КЗК) до України, що тривав з 9 до 21 жовтня 2013 р. (CPT/Inf (2014) 15. Звіт про оцінку впровадження Кримінального процесуального кодексу України, лютий 2015 р., підготовлений в рамках проекту «Підтримка реформи кримінальної юстиції в Україні».

[51] Стаття 214 КПК.

[52] Стаття 41 КПК.

[53] Див., наприклад, Організація безпеки та співробітництва в Європі, Права людини і антитерористичні розслідування: практичні настанови для співробітників правоохоронних органів, Варшава (2013), стор. 46-49.

4.9 Отже, концептуально неправильно говорити про параліч кримінального процесу через те, «що оперативно-розшукові органи були без розумних причини позбавлені незалежності у прийнятті рішень щодо заходів у кримінальному процесі». Співробітники оперативно-розшукових підрозділів мають унікальні фахові навички, які варто використовувати на забезпечення слідчих та інших потреб на допомогу слідчим та прокурорам. Такий розподіл повноважень був справедливо посилений Законом про прокуратуру та останніми змінами до статті 131-1 Конституції.

4.10 Судячи з останніх конституційних та законодавчих змін, Україна запровадила систему, за якої негласні/оперативно-розшукові операції правоохоронних органів підлягають контролю з боку прокуратури. Хоча оперативно-розшукові операції можуть проводитися з метою збору оперативної інформації (зокрема, у сфері національної безпеки), чітким пріоритетом має бути ініціювання розслідування кримінальної справи у відповідності до статті 214 КПК.

4.11 Хоча ця вимога деякою мірою відображена у Законопроекті, вона не прописана достатньо чітко, і тому залишає детективам/співробітникам оперативно-розшукових органів можливості її порушення. Так, пункт 2 статті 12 Законопроекту називає обов'язок оперативно-розшукових підрозділів виконувати «запити повноважних державних органів, установ та організацій про проведення оперативно-розшукових заходів». Пункти 3 та 4 статті 39 дозволяють у певних випадках використовувати надзвичайні повноваження («у випадках отримання інформації про вчинення злочинів»). Ці винятки сформульовані надто широко і можуть використовуватися державними органами тощо для прийняття рішень про застосування оперативно-розшукових заходів для дуже широкого кола випадків, потенційно в обхід статті 214 КПК. Крім того, ці положення не містять обмежень щодо використання цих заходів у часі, що є дуже значним упущенням, зважаючи на можливу тривалість складних оперативно-розшукових заходів. Для запобігання зловживанням на ці заходи необхідно прямо поширити дію статті 214 КПК.

Рекомендація 1: Рекомендується безпосередньо вказати, що пункт 3 статті 12 та пункти 3 і 4 статті 39 підпорядковуються вимогам статті 214 КПК в частині внесення до реєстру інформації щодо дійсного чи можливого вчинення злочину протягом 24 годин з моменту отримання такої інформації. Крім того, слід заборонити проведення оперативно-розшукових операцій поза межами цього строку без спеціального дозволу, що отримується в порядку, передбаченому Законопроектом. Нарешті, слід прямо заборонити детективам проводити будь-які заходи без дозволу, а також встановити вимогу про обов'язок звертатися за інструкціями на проведення конкретних заходів до слідчого органу чи прокурора у відповідності до статті 41 КПК[54].

4.12 У тексті Законопроекту використовуються різноманітні терміни, зокрема, «підозра» та інші терміни, що визначені у КПК, але не визначені у самому Законопроекті. Це може призвести до плутанини у використанні цих термінів у контексті Законопроекту та КПК.

Рекомендація 2: Для уникнення непорозумінь щодо значення цілого ряду термінів у Законопроекті та КПК рекомендується надати їм однакове визначення в обох текстах.

4.13 Визначну роль у Законопроекті посідають оперативно-розшукові функції, якими наділені різні правоохоронні та інші органи. У порівнянні із нинішнім Законом про оперативно-розшукову діяльність від 1992 р, роль цих органів суттєво зросла. Зокрема, вони стали відігравати ключову роль у виконанні розвідувальних, превентивних та інших

[54]Що стосується затримання злочинців, детективи мають право робити це в рамках механізмів, передбачених статтями 207-213 КПК. Див. також пункт 31 цього висновку.

функцій. Вони мають ряд повноважень, зокрема, можуть пропонувати заходи на стратегічному рівні, визначати наявність достатніх підстав для використання певних дій щодо конкретних осіб, а також вживати на практиці оперативно-розшукові заходи у конкретних випадках. Цей підхід відповідає концепції Європейського Союзу щодо активного підходу до забезпечення внутрішньої безпеки ЄС на основі оперативних даних[55].

4.14 Численні положення Законопроекту перегукуються із положеннями КПК, що регулюють відкриті й таємні слідчі дії, зокрема щодо повноважень правоохоронних органів та їхніх слідчих підрозділів.

4.15 Проте Законопроект містить прогалини в частині процесуальних гарантій. КПК передбачає низку ретельно підібраних процесуальних гарантій, що здатні забезпечити відповідність процесу конвенційним стандартам[56]. Натомість, Законопроект жодним чином не розрізняє використання різних видів негласного спостереження в публічних і приватних місцях (останнє становить набагато більше втручання), не містить визначення «житла» та інших спеціальних умов, які мають задовольняти гласні й негласні оперативно-розшукові заходи, щоби забезпечити дотримання прав людини. Це надзвичайно важливо з огляду на передбачений Законопроектом широкий перелік оперативно-розшукових заходів, за відсутності чіткої вказівки на те, що вони можуть здійснюватися лише за умови дотримання положень про дозволи і контролі, передбачені КПК. Статтею 31 Законопроекту передбачено: «Судовий контроль за оперативно-розшуковою діяльністю здійснюється у порядку, передбаченому чинним Кримінальним процесуальним кодексом України щодо здійснення негласних слідчих (розшукових) дій». Проте вважаємо, що для забезпечення повної відповідності Законопроекту КПК цю вимогу слід прописати більш детально, із чітким посиланням на відповідні норми КПК.

4.16 Ця прогалина створює значний ризик того, що оперативно-розшукові заходи, передбачені Законопроектом, будуть здійснюватися із порушенням прав людини осіб, щодо яких вони проводитимуться.

Рекомендація 3: Законопроект повинен містити чіткі й конкретні вимоги про поширення на нього процесуальних гарантій того ж рівня, що й гарантії за КПК, зокрема, в частині прокурорського й судового контролю.

4.17 Законопроект не містить вимоги про те, що особи, до яких застосовувалися негласні заходи, повинні бути за можливості про це повідомлені. Як зазначалося у пункті 3.17 цього висновку, це ключова процесуальна гарантія забезпечення судового контролю над таємними заходами, на важливості якої наголошував ЄСПЛ.

Рекомендація 4: Законопроект повинен передбачати, що після завершення оперативно-розшукових заходів особи, до яких вони застосовувалися, повинні в міру можливості про це повідомлятися. Це слід зробити у спосіб, аналогічний до того, як це зроблено у статтях 253 та 254 КПК.

4.18 Мінімальні умови для затримання осіб за пунктом 2 частини 6 статті 10 та частиною 3 статті 39 суперечать положенням статті 207 КПК або є недостатньо високими, щоби задовольнити вимоги статті 5 Конвенції: вони не вимагають існування розумних підстав вважати, що особа скоїла чи намагається скоїти злочин. Хоча затримання осіб під час

[55] Див. Стокгольмська програма -- відкрита й безпечна Європа на службі й захисті своїх громадян, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52010XG0504(01) та пов'язане законодавство ЄС. Див. також «Стратегія внутрішньої безпеки ЄС стосовно європейської безпекової моделі», ЄС (2010), стор. 22.
[56] Це питання детально розглядається у розділі 3 цього висновку.

оперативно-розшукових заходів в разі нагальної потреби не забороняється, мінімальні умови для такого затримання мають бути ідентичними до умов затримання осіб за інших обставин.

Рекомендація 5: Мінімальні умови для затримання, передбачені пунктом 2 частини 6 статті 10 та частиною 3 статті 39, необхідно привести у відповідність із положеннями статті 207 КПК.

4.19 Одним із заходів, передбачених Законопроектом, є «перевірка фінансово-господарської діяльності підприємств» (пункт 19 частини 2 статті 10). У первинному тексті Законопроекту передбачено, що ці повноваження включають «організацію перевірки», що певною мірою передбачає право проводити загальний аудит, інспекцію та нагляд. Хоча в рамках конкретного розслідування чи операції органам може дійсно знадобитися переглянути фінансові документи, треба чітко зазначити, що Законопроект не дає їм загального права перевіряти ці документи в рамках функції загального контролю чи нагляду. Надання цих повноважень широкому колу оперативно-розшукових органів без врахування їхньої основної функції та непослідовність щодо вимоги отримання попереднього судового дозволу[57] може вважатися еквівалентом певної форми загального нагляду[58].

4.20 Поле для зловживання цими повноваженнями є широким. Законний інтерес щодо забезпечення фінансової дисципліни можна реалізувати за допомогою відкритих заходів, зокрема, шляхом опублікування бухгалтерських даних і використання аудиторських та інспекційних повноважень компетентних органів. У необхідних випадках ці повноваження може бути покладено на інші органи, зокрема, Державну контрольно-ревізійну службу та Національну комісію з цінних паперів та фондового ринку.

Рекомендація 6: У Законопроекті слід використовувати такий самий підхід[59], що й у КПК, тобто визначити, що перевірки юридичних осіб за пунктом 19 частини 2 статті 10 можуть проводитися лише в рамках конкретних гласних чи негласних оперативно-розшукових заходів.

4.21 Для забезпечення правової чіткості, уникнення конфлікту повноважень різних органів та оперативно-розшукових і слідчих операцій та зменшення поля для зловживань під час здійснення оперативно-розшукових операцій необхідно дуже чітко визначити підстави для проведення таких операцій. Стаття 9 Законопроекту сформульована досить широко, зокрема в частині оперативно-розшукових заходів, спрямованих на осіб, що готують злочин. Рекомендується зазначити у Законопроекті, що в разі скоєння злочину *(corpus delicti),* як у випадку завершеного, так і незавершеного[60], подальші заходи повинні носити характер розслідування і проходити із дотриманням відповідних положень КПК.

4.22 Частиною 1 статті 9 Законопроекту передбачено, що інформація, достатня для проведення оперативно-розшукової діяльності, включає інформацію про «осіб, які переховуються від органів досудового розслідування, слідчого судді, суду, або ухиляються від відбування кримінального покарання» Варто роз'яснити процесуальний статус цих осіб, оскільки до них можуть застосовуватися запобіжні заходи згідно з КПК. Невиконання

[57] Відповідно до частини 4 статті 10 це не вимагає судового дозволу, а пунктом 3 частини 1 статті 13 передбачено, що вимагання, ознайомлення, вивчення та вилучення документів та даних, що характеризують діяльність підприємств, установ і організацій, потребує дозволу слідчого судді.

[58] Див. пункти 7, 25 та 26 спільного висновку Венеціанської комісії та Генерального директорату прав людини (2013 р.) щодо проекту Закону України «Про прокуратуру» та попередню оцінку проектів законодавчих актів з питань діяльності прокуратури, CDL (2013)039.

[59] Статті 36,40 та 93 КПК.

[60] Визначення наведене у статті 13 Кримінального кодексу України.

обов'язку дотримуватися запобіжних заходів становить конкретну юридичну підставу для проведення слідчих дій.

Рекомендація 7: Було б доцільно, щоб стаття 9 Законопроекту передбачала, що, якщо злочин було скоєно (є склад злочину – *corpus delicti*), незалежно від того, був він закінченим чи ні[61], або там, де вимоги конкретних запобіжних заходів не були виконані, будь-які подальші дії повинні бути слідчими, що здійснюються на підставі відповідних положень КПК.

4.23 Невиправдано широким є формулювання підстав для проведення оперативно-розшукових заходів, передбачених пунктами 3 та 4 частини 1 статті 9 Законопроекту, а саме «потреба в отриманні розвідувальної інформації в інтересах безпеки суспільства і держави» та «наявність узагальнених матеріалів центрального органу виконавчої влади».

4.24 Підстава, передбачена пунктом 3, повинна містити вимогу про наявність законного інтересу та необхідності отримання такої інформації. Конвенція та практика ЄСПЛ визнають першочергову важливість захисту державної (національної) безпеки[62] та боротьби з тяжкими злочинами і тероризмом[63]. Проте це не можна використовувати як загально застосовну підставу для негласного спостереження: для цього необхідно мати конкретні підстави в кожному індивідуальному випадку.

4.25 Що стосується пункту 4, то хоча для використання оперативно-розшукових заходів у контексті національної безпеки і не вимагається підозрювати осіб у вчиненні конкретного злочину, необхідно тим не менш мати достатні підстави говорити про наявність конкретних дій, що пов'язані чи потенційно пов'язані з кримінально караними діями індивідуального чи системного характеру: відмивання брудних коштів, фінансування тероризму тощо.

Рекомендація 8: Пунктом 3 частини 1 статті 9 необхідно перебачити вимогу про існування підстав для проведення конкретного оперативно-розшукового заходу. Пунктом 4 необхідно передбачити вимогу про наявність достатніх підстав підозрювати особу у вчиненні конкретних дій, що пов'язані чи потенційно пов'язані з кримінально караними діяннями індивідуального чи системного характеру: відмивання брудних коштів, фінансування тероризму тощо.

4.26 У пунктах 20, 21 та 22 частини 2 статті 10 згадуються «профілактично-пошуковий захід», «оперативна установка» та «радіотехнічна розвідка» відповідно. Слід дати кращі визначення цим термінам, оскільки наявні визначення надто широкі і позначають категорії оперативно-розшукових заходів, а не конкретні заходи.

Рекомендація 9: Термінам, що містяться в пунктах 20, 21 та 22 частини 2 статті 10, необхідно дати більш точне визначення.

4.27 Законопроект передбачає надто широкі умови й підстави проведення оперативно-розшукових заходів до отримання необхідного дозволу. У цьому контексті Законопроект відрізняється він чинного закону, який включає відповідні вимоги глави 21 КПК. Як наслідок, замість забезпечення відповідності вже наявній законодавчій базі (що містить вимоги терміновості, залучення прокуратури, негайного судового контролю та інших важливих процесуальних гарантій), у частинах 5 та 6 статті 10 Законопроекту просто

[61] Як це визначено у статті 13 Кримінального кодексу України.
[62] Див., наприклад, справу *Нолан та К. проти Росії (Nolan and K. v. Russia),* рішення від 12 лютого 2009 року, заява № 2512/04.
[63] Див., наприклад, У*зун проти Німеччини (Uzun v. Germany),* рішення від 2 вересня 2010 р., заява № 35623/05.

міститься посилання на «інші закони». Законопроект не включає процесуальних гарантій, передбачених у чинному законодавстві. І це попри той факт, що оперативно-розшукові заходи потенційно можуть супроводжуватися ще більшою кількістю зловживань, ніж заходи в рамках досудового розслідування. Як наслідок, використання цих положень Законопроекту із дуже високою імовірністю може призвести до порушення вимог Конвенції.

4.28 Таким чином, Законопроект повинен безпосередньо включати положення статті 250 КПК, прямо або шляхом посилання на вимоги цієї статті. Це належним чином обмежить проведення оперативно-розшукових заходів, що пов'язані із втручанням у права людини, до отримання судового дозволу.

Рекомендація 10: До Законопроекту слід безпосередньо включити положення статті 250 КПК або конкретне посилання на вимоги цієї статті.

4.29 Аналогічні зауваження стосуються відсутності чітко визначеного порядку реєстрації документів, що містять інформацію, отриману під час проведення оперативно-розшукових заходів. Оперативно-розшукові заходи можуть проводитися без реєстрації. Це випливає зі статті 16 Законопроекту, яка не містить вимоги про реєстрацію інформації, отриманої, наприклад, у процесі застосування заходів, передбачених пунктом 19 частини 2 статті 10 («перевірка фінансово-господарської діяльності підприємств») та інших пунктів частини 2 цієї статті. Відсутність вимоги щодо реєстрації оперативно-розшукових заходів є суттєвим недоліком з точки зору забезпечення підзвітності та полегшення контролю.

Рекомендація 11: Законопроект повинен включати вимогу про те, що усі оперативно-розшукові заходи, включаючи будь-яку пов'язану з ними інформацію, у т.ч. отриману інформацію, повинні належним чином реєструватися.

4.30 Законопроект, як у випадку прийняття його у поточній редакції, так і у випадку внесення рекомендацій, наведених у цьому висновку, вимагатиме внесення змін до низки інших законодавчих актів, у тому числі КПК. Отже, він повинен містити таблицю змін до інших законодавчих актів.

Рекомендація 12: Законопроект повинен містити таблицю, де описані зміни до інших законодавчих актів, що вносяться відповідно до Законопроекту.

4.31 Практична порада з юридичної техніки: низка статей складаються лише з однієї частини, а отже, немає потреби нумерувати ці частини. В англомовній версії Законопроекту це статті 4, 17, 25, 27, 28 та 35.

4.32 З точки зору захисту даних Законопроект містить позитивні моменти, що відповідають європейським стандартам, і посилається на певні гарантії, що застосовуються при проведенні оперативно-розшукових заходів, зокрема, на судовий контроль негласних операцій. Наприклад:

i. Стаття 8 визначає перелік підрозділів, що здійснюють оперативно-розшукову діяльність; стаття 10 перелічує конкретні оперативно-розшукові заходи і детально визначає процедуру подання клопотання для отримання дозволу на проведення таких заходів (у клопотанні необхідно продемонструвати, що всі інші способи отримання інформації про можливе вчинення кримінально караного діяння було вичерпано). Стаття 11 називає органи та злочини, для розслідування яких можуть проводитися оперативно-розшукові заходи. Стаття 42 регулює порядок засекречування та розсекречування матеріалів, отриманих під час оперативно-розшукової

діяльності. Розділ 6 Законопроекту визначає багаторівневий механізм здійснення контролю за оперативно-розшуковою діяльністю.

ii. Водночас, Законопроект викликає запитання стосовно дотримання стандартів у сфері захисту інформації. Нижче наводиться постатейний аналіз цих питань.

4.33 При аналізі Закону України «Про захист персональних даних» та проекту Закону України «Про оперативно-розшукові заходи» схоже на те, що Закон України «Про захист персональних даних» не поширюється на діяльність правоохоронних органів (чи використання персональних даних у контексті правоохоронної діяльності у більш широкому розумінні). В Україні немає окремого закону, що регулює використання персональних даних правоохоронними органами, якщо тільки це питання не врегульоване іншими законодавчими актами. Законопроект не забезпечує комплексного регулювання питань захисту персональних даних у контексті запобігання та розслідування злочинів.

Рекомендація 13: Законопроект повинен врегулювати аспекти захисту персональних даних у контексті правоохоронної діяльності більш системно (наприклад, шляхом включення відповідного розділу з детально виписаними положеннями або прийняття спеціального закону з захисту даних, що покривав би правоохоронні органи).

5. Постатейні коментарі

Глосарій термінів і визначень

5.1 Розділ Законопроекту під назвою “Визначення термінів” є важливим нововведенням у порівнянні із діючим Законом.

5.2 Слід вжити заходів для забезпечення послідовного використання визначень в усьому тексті проекту Закону. Наприклад, у визначенні терміну "аудіоконтроль особи" не вказано, чи мається на увазі перехоплення телефонних розмов ("прослуховування телефонних розмов"), а також застосування звукозаписувальних пристроїв, які полегшують прослуховування (радіомікрофони). Існують також терміни «контроль за телефонними розмовами» і «контроль кореспонденції», які, вочевидь, стосуються перехоплення телефонних розмов і поштових відправлень. У загальних рисах, перехоплення телефонних розмов вважається тактикою, що передбачає особливе втручання у реалізацію особами права на повагу до приватного життя, у той час як прослуховування вважається трохи менш жорстким заходом (в залежності від того, де воно відбувається). Наприклад, таємний запис розмови людини в громадському місці, будучи посяганням на її право на повагу до приватного життя, є набагато менш жорстким (інтрузивним) заходом, ніж таємний запис телефонної розмови людини або запис її розмови у власному помешканні. Потрібно точно визначити природу того, що охоплюється терміном "аудіоконтроль особи". Якщо цього немає, важко забезпечити дотримання принципу пропорційності (співмірності). ЄСПЛ зазначив, що у національних законах має бути детально викладено, що передбачають різні правові норми, при цьому невиправдано великі за обсягом визначення є неприйнятними.

Рекомендація 14: У визначенні терміну "аудіоконтроль особи" в Законопроекті має бути проведена різниця між різними формами аудіоконтролю, які дозволяється здійснювати, зокрема, між використанням пристроїв для прослуховування та перехопленням телефонних розмов, а також між заходами з аудіоконтролю особи залежно від місця, в якому вони проводяться.

5.3 З'являється термін «конфіденційне співробітництво», хоча трохи нечіткий, для визначення використання послуг таємних інформаторів/агентів або *осіб, які таємно здобувають інформацію за допомогою безпосередніх контактів з її носіями (англ. Covert Human Intelligence Sources*, далі по тексту використовується англійська абревіатура *CHIS)*. CHIS – термін, прийнятий у правоохоронних органах, який частіше застосовується в англійській мові в рамках Європейського співтовариства правоохоронних органів. Може варто розглянути питання належного перекладу цього терміну для використання в проекті даного Закону і в більш загальному контексті. Крім того, термін «конфіденційне співробітництво» не передбачає застосування даного заходу із залученням неповнолітніх. Натомість є обставини, за яких може бути дозволено залучати неповнолітню особу в якості CHIS. Проте, подібні ситуації повинні виникати дуже рідко і вимагати надзвичайно ретельного вивчення і контролю. Найкращі інтереси неповнолітнього мають бути головною турботою при наданні такого дозволу відповідно до вимог статті 3 Конвенції Організації Об'єднаних Націй про права дитини. Більш доцільно було б передбачити в проекті Закону спеціальну норму, що стосувалася б ролі неповнолітніх в оперативно-розшуковій діяльності в цілому, а не конкретно питання їх залучення в якості CHIS.

Рекомендація 15: Законопроект має містити чітке положення про те, що будь-які дії, пов'язані із залученням неповнолітніх до оперативно-розшукової діяльності, повинні мати за основну мету захист найкращих інтересів дитини.

5.4 «Поліграфне опитування» з точки зору його необхідності і пропорційності; незрозуміло, якими є підстави для застосування цього заходу, не беручи до уваги аргументи, що стосуються довіри до нього. Крім того, відсутнє будь-яке пояснення того, коли виникає необхідність у застосуванні даного заходу, а також технічних аспектів його застосування на практиці. Пропонується, щоб проект Закону містив більш детальні пояснення з приводу цих питань.

Рекомендація 16: В проект Закону потрібно включити додаткові положення, що врегулюють застосування методу поліграфного опитування, або конкретну відсилку до відповідних законодавчих норм.

5.5 Проект закону вводить поняття оперативного експерименту. Це може бути результатом механічного перенесення і технічного підлаштування під положення КПК, який містить термін «слідчий експеримент». Суть останнього полягає в тому, що він має чисто доказове значення і стосується відтворення дій та обставин певної події. Незрозуміло, за яких обставин виникне необхідність і можливість у застосуванні цього методу в оперативно-розшукової діяльності. Якщо поняття «оперативного експерименту» передбачає поетапну дію, яка може виступати в якості пускового механізму в ході оперативно-розшукових операцій і буде частиною загальної стратегії збору інформації, тоді незрозуміло, як це поняття відрізняється від інших видів діяльності (наприклад, "оперативної закупки" і т.д.), які вже містяться в проекті закону і прописані доволі докладно. Цей момент потрібно уточнити.

5.6 Визначення терміну "Негласне проникнення та обстеження публічно недоступних місць, житла чи іншого володіння особи" у законопроекті наводиться двічі. Цю проблему слід розв'язати для уникнення можливої плутанини.

5.7 Потрібно розглянути питання використання в тексті проекту Закону термінів «необхідність» і «пропорційність» («співмірність») там, де це є доцільним, наприклад, використовувати слово «необхідно» замість «важливо». Концепція «необхідності» має принципове значення з точки зору демонстрації нагальної потреби у вчиненні певної дії і, таким чином, слугує для забезпечення правової основи згідно з критеріями Конвенції, оскільки остання містить вимогу про те, що держава має вчинити певні дії для захисту інтересів постраждалих осіб (зокрема жертв). Використання терміну «необхідно» забезпечить узгодженість з термінологією, яка застосовується в аналогічному законодавстві країн Європи. Крім того, ці терміни часто використовуються у прецедентних рішеннях ЄСПЛ. Отже, їх застосування у законопроекті значною мірою допомогло б у забезпеченні і поясненні підстав та обґрунтування для проведення оперативно-розшукових дій.

Стаття 2

5.8 Загалом негласне спостереження слід використовувати тільки щодо злочинів з достатнім ступенем тяжкості.[64] Хоча частина 4 статті 10 проекту Закону обмежує застосування заходів, передбачених пунктами 1 – 11 частини 2 статті 10, випадками, коли йдеться про тяжкі або особливо тяжкі злочини, інші заходи, передбачені у частині 2, не

[64] Наприклад, у Сполученому Королівстві деякі заходи, які обмежують права людини, можуть бути застосовані виключно у випадку розслідування тяжких злочинів, що передбачено у статті 93 частина 4 Закону про поліцію 1997 року:

«Поведінка, яка:

(a) передбачає застосування насильства, має наслідком заволодіння майном (коштами) у великих розмірах чи вчиняється великою кількістю осіб з метою досягнення спільної мети; або

(b) становить правопорушення або одне з правопорушень, за яке особа, що досягла 21-річного віку та не має судимостей у минулому, може бути засуджена до позбавлення волі строком на 3 роки і більше.»

підпадають під дію цих обмежень. Надання дозволу на їх застосування у випадках розслідування злочинів, які не мають необхідного рівня тяжкості, може створити проблеми з дотриманням вимог Конвенції.[65]

5.9 Крім того, мета, викладена в пункті 2 статті 2, щодо отримання інформації про будь-які правопорушення, що не є злочинами, виявлення яких сприятиме вирішенню завдань протидії злочинності, не узгоджується зі статтею 9 і розширює підстави для проведення оперативно-розшукової діяльності, які визначені у цій статті.

Рекомендація 17: Необхідно розглянути питання щодо виключення пункту 2 статті 2.

5.10 Сфера застосування пункту 3 статті 2 не є достатньо чіткою, що може привести до її широкого тлумачення з боку влади. Визначення «отримання інформації про факти та обставини, що не мають ознак кримінального правопорушення, проте, відповідно до законодавства України, потребують перевірки», вочевидь, не пов'язане з поняттям злочину, є нечітким і може привести до обробки персональних даних в найширшому контексті правоохоронного діяльності.

5.11 Крім того, згідно з повною версією положень проекту Закону "*випадки отримання інформації про будь-які факти та обставини, що не мають ознак кримінального правопорушення, відповідно до чинного законодавства України, яке підлягає застосуванню, потребують перевірки*" (згадані у пункті 3) обмежуються лише а) встановленням місцезнаходження безвісно зниклих осіб, що вже згадувалося у статті, яка обговорюється, б) перевірки осіб у зв'язку з їх допуском до державної таємниці і до роботи з ядерними матеріалами та на ядерних установках (передбачені пунктом 2 частини 1 статті 9). Для недопущення будь-якого розширеного тлумачення і несанкціонованого застосування оперативно-розшукових заходів необхідно було б внести зміни до цієї норми (пункт 3), щоб вона передбачала вичерпний перелік таких випадків.

Рекомендація 18: Сферу застосування пункту 3 статті 2 слід переглянути з тим, щоб не допустити будь-якого розширеного тлумачення і несанкціонованого застосування оперативно-розшукових заходів, а також забезпечити, щоб цей пункт унеможливлював обробку персональних даних за надмірно широкого переліку обставин.

Стаття 4

5.12 Побудова цієї норми з включенням принципу пропорційності, який сформульований як "відповідність та адекватність використання оперативно-розшукових заходів ступеню суспільної небезпечності протиправної діяльності", можна було б поліпшити і привести у відповідність до формулювання, запропонованого частиною 2 статті 8 Конвенції.

Рекомендація 19: З метою забезпечення узгодженості з положеннями Конвенції та практикою ЄСПЛ стаття 4 проекту Закону має включати в себе в якості принципу оперативно-розшукової діяльності *необхідність у демократичному суспільстві в інтересах національної та громадської безпеки, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод людини*. Цей принцип потрібно також включити до частини 2 статті 6 законопроекту.

Стаття 5

[65] Рішення у справі «*Роман Захаров проти Росії*» (*Roman Zakharov v. Russia*) від 4 грудня 2015 року, заява № 47143/06, пункт 244.

5.13 Частину 2 статті 5 можна тлумачити як обмежувальну норму загального призначення, що дозволяє проводити обробку персональних даних лише в тих випадках, коли це прямо передбачено в проекті закону. Цю норму варто привітати. Обмеження щодо мети використання є одним з основних принципів захисту даних, спрямованих на встановлення вимог, за яких персональні дані, зібрані з певною метою, можуть додатково оброблятися в інших цілях. У Принципі 4 Рекомендації № (87) 15 Комітету Міністрів Ради Європи[66] також заявлено про це такими словами: "[...] персональні дані, зібрані та збережені поліцією в цілях реалізації своїх повноважень, мають використовуватися винятково в цих цілях". Хоча посилання на обмеження щодо мети використання є позитивним моментом, проект Закону, схоже, не враховує вимоги щодо розмежування різних категорій даних (конкретних даних або конкретних категорій суб'єктів даних).

5.14 В контексті обмеження щодо мети використання повинні існувати суворі правила стосовно того, коли дані можуть бути розкриті і у подальшому передані різним правоохоронним органам (наприклад, стаття 37, а також частини 2 і 3 статті 12). У той час як важливо забезпечити міжвідомчу координацію та співпрацю в цілях якнайшвидшого розслідування злочину, повинні діяти належні гарантії від порушень права на захист персональних даних. Дані, зібрані для розкриття конкретного злочину, можуть бути також використані уповноваженими органами в рамках розслідування іншого злочину за умови, що дотримання згаданих гарантій оцінюється на індивідуальній основі у кожному конкретному випадку та врегульовується конкретними законодавчими нормами. Принцип 5 Рекомендації № (87) 15 пропонує керівні принципи передачі перехоплених даних.

Стаття 6

5.15 Одним з важливих аспектів оперативно-розшукових заходів є забезпечення управління усіма прогнозованими ризиками. Наприклад, CHIS або інші особи, які допомагають поліції, можуть наражатися на серйозний ризик у частині завдання їм шкоди. Для того, щоб впоратися з цим ризиком, повинні вживатися відповідні заходи з точки зору планування і контролю за проведенням оперативно-розшукової діяльності.

5.16 Цілком ймовірно, що будь-які слідчі (розшукові) дії передбачатимуть збір інформації. У багатьох випадках може бути зібрана інформація, яка не має безпосереднього відношення до завдань цих слідчих дій. Це може розглядатися як супутнє (побічне) втручання з боку правоохоронних органів, наприклад збір інформації про осіб, з якими контактує об'єкт (ти) оперативно-розшукових заходів, але які самі не підозрюються у причетності до будь-якої неправомірної діяльності. Законопроект повинен містити положення щодо поводження з такою інформацією.

Рекомендація 20: Законопроект повинен містити норми, які регулюють питання управління інформацією, зібраною в ході оперативно-розшукової діяльності, що стосується осіб, які не підозрюються у вчиненні будь-яких незаконних дій.

5.17 Крім того, пропонується більше уваги приділяти веденню обліку цих оперативно-розшукових заходів і відповідних органів, які їх здійснюють, включаючи будь-які контрольні механізми, з метою забезпечення повного виконання положень щодо відповідальності. Ведення журналів обліку оперативно-розшукових дій з всебічною інформацією про них є ключовим методом забезпечення відповідальності в рамках судового нагляду.

[66] «що регулює використання персональних даних у діяльності поліції»

5.18 Частина 2 статті 6 включає в себе норму про подальше застосування принципу пропорційності. Визначення, яке рекомендується включити у статтю 4, про що йшлося вище (див. рекомендацію 19), слід також використати у цій статті.

5.19 Вітається положення про відшкодування заподіяної шкоди, яке міститься в частині 2 статті 6. Проте, можуть виникнути обставини, за яких виникне потреба у судовому захисті прав, наприклад, для того, щоб забезпечити належний судовий нагляд, або якщо постраждала особа не вважає, що будь-яка запропонована їй компенсація є достатньою за відповідних обставин. Засіб судового захисту має бути додатковим по відношенню до відшкодування шкоди, передбаченої в частині 4, яка стосується випадків, коли прокурору або судді стає відомо про порушення прав людини.

Рекомендація 21: Частина 2 статті 6 повинна містити положення про судовий захист права на відшкодування шкоди у відповідних випадках.

5.20 Частина 3 статті 6, здається, піднімає питання з точки зору прав людини і захисту даних, особливо в частині права суб'єкта даних бути поінформованим (наприклад, особи, за якою здійснюється спостереження). Принцип 2.2 Рекомендації № (87) 15[67] визнає право суб'єкта даних бути поінформованим, особливо коли збір даних відбувався без його/її відома. Хоча згідно з частиною 3 статті 6 фізичним особам дозволяється вимагати від відповідних органів надання письмових пояснень з приводу обмеження їх прав і свобод, здається, що відповідне зобов'язання або обов'язок державних органів щодо інформування людей про проведення оперативно-розшукових заходів стосовно них цією правовою нормою не передбачені. Хоча важливо не створювати загрозу для національної безпеки і розслідування злочинів, право на отримання інформації має безпосередній вплив на реалізацію права на ефективний засіб правового захисту. Таким чином має існувати механізм для повідомлення користувача, навіть після того, як заходи вже не проводяться, для того, щоб суб'єкт персональних даних міг реалізувати своє право на ефективний засіб правового захисту, принаймні постфактум (*ex post facto*).[68]

5.21 Частини 5 і 6 статті 11 і частина 6 стаття 15 стосуються охорони державної таємниці в частині здійснення оперативно-розшукових заходів. Хоча це законний інтерес, необхідно узгодити його з правами суб'єкта даних, який повинен мати можливість реалізувати своє право на юридичний захист.

5.22 Недавня справа *Романа Захарова* є актуальною в цьому контексті, підкреслюючи зв'язок між правом бути поінформованим і правом на ефективний засіб правового захисту. Суд постановив, що «[...] в принципі існує мало можливостей для звернення до суду зацікавленої особи, якщо тільки остання не була повідомлена про заходи, вжиті без її відома, і таким чином, може оскаржити їх законність; або, як альтернатива, якщо тільки будь-яка особа, яка підозрює, що її розмови/листування перехоплюються в даний час або перехоплювалися раніше, не звернеться до суду, і, отже, судовий розгляд не залежатиме від інформування цієї особи про те, що її розмови/листування перехоплюються»[69]. Більш детально це питання висвітлене вище в пункті 3.17.

---

[67] Принцип 2.2 Якщо дані, що стосуються індивіда, були зібрані і зберігалися без його відома, і, якщо ці дані не були знищені, він повинен бути проінформований, коли це практично можливо, про те, що інформація про нього зберігається, якщо тільки об'єкту діяльності поліції цим більше не може бути завдано шкоди.

[68] Відступ від цього принципу допускається лише у випадках, коли така інформація суперечитиме інтересам слідства, поставить під загрозу здоров'я, безпеку або свободу особи або негативно вплине на реалізацію прав та інтересів інших.

[69] Рішення у справі «*Роман Захаров проти Росії*» (*Roman Zakharov v. Russia*) від 4 грудня 2015 року, заява № 47143/06, пункт 234. Дивись також рішення у справі «*Вебер і Саравія проти Німеччини*» (*Weber and Saravia v. Germany*) від 29 червня 2006 року, заява № 54934/00, в якому Суд підкреслив, що, коли перехоплені дані

Рекомендація 22: У частині 3 статті 6 слід прописати чіткий механізм реалізації на практиці права бути поінформованим про перебування у статусі об'єкта оперативно-розшукових заходів. Будь-які обмеження цього права, викликані необхідністю зберегти таємницю організації і тактики слідчих дій, повинні бути мінімально необхідними для захисту цієї таємниці і не повинні надмірно перешкоджати реалізації права на інформацію.

Стаття 7

5.23 Положення частини 2 статті 7 можуть потребувати більш детальних пояснень, щоб забезпечити гарантії конфіденційності особи. У деяких випадках відомості (персональні дані) про CHIS та інших осіб можуть потребувати розголошення відповідним державним органам з метою надання їм допомоги (наприклад, у тому випадку, коли вони змінюють ім'я та інші персональні дані або беруть участь у програмі захисту свідків). Можливо частина 2 цієї статті стосується лише розголошення персональних даних цих осіб, але тоді це потрібно зазначити.

Рекомендація 23: Частина 2 статті 7 повинна передбачати розголошення персональних даних CHIS у випадках, коли це необхідно для захисту їх життєво важливих інтересів.

Стаття 9

5.24 Дивись зауваження та рекомендації щодо цієї статті у Розділі «Загальні зауваження», пункти 4.21 – 4.25, а також рекомендації 7 та 8, наведені вище.

Стаття 10

5.25 Перелік, наведений у частині 2 цієї статті, схоже, не містить положень щодо постановлення завдань для/залучення CHIS, чиїми послугами користуються правоохоронні або інші органи для негласного одержання інформації. Незрозуміло, чи йдеться про недоопрацювання цієї правової норми, або таке залучення CHIS вважається складовою інших заходів, наприклад, оперативного експерименту?

Рекомендація 24: Якщо залучення CHIS не розглядаються в якості оперативно-розшукового заходу, передбаченого частиною 2 статті 10, потрібно включити до проекту Закону окрему норму про залучення CHIS.

5.26 Стаття 10 містить перелік конкретних оперативно-розшукових заходів і пропонує два окремі нормативно-правові режими їх застосування в залежності від характеру відповідного заходу. З точки зору характеру цих заходів, який передбачає обмеження прав та свобод людини, і, таким чином, вимагає більш суворих процесуальних гарантій, рекомендується оперативно-розшукові заходи, наведені в пунктах 15 ("спостереження за річчю або місцем") і 22 ("радіотехнічна розвідка") частини 2 статті 10, додати до першої групи (яка в даний час включає в себе оперативно-розшукові заходи, перелічені у пунктах 1-11).

Рекомендація 25: Оперативно-розшукові заходи, передбачені пунктами 15 ("спостереження за річчю або місцем") і 22 ("радіотехнічна розвідка") частини 2 статті

знищені та відповідні особи не були поінформовані про те, що за ними здійснювалося спостереження, "це може слугувати підставою для приховування заходів контролю, які здійснювалися державними органами". **Отже таке спостереження (здійснюване також [органами, відповідальними за національну безпеку]) має відбуватися "відповідно до закону", переслідувати "законну мету у демократичному суспільстві", і бути "необхідним" та "співмірним" з поставленою метою.**

10, повинні бути додані до групи оперативно-розшукових заходів, перелічених у пунктах 1-11, які вимагають застосування додаткових процесуальних гарантій.

5.27 Дивись також зауваження та рекомендації, що стосуються цієї статті, у Розділі «Загальні зауваження», пункти 4.19, 4.20 і 4.26 – 4.28, і рекомендації 5, 9 і 10, наведені вище.

5.28 Має місце технічна помилка в частині 7, де помилково міститься посилання на частину 5 цієї ж статті.

Стаття 11

5.29 Зазначення конкретних оперативно-розшукових заходів, які має право проводити кожний орган, з їх конкретною прив'язкою до компетенції та повноважень цього органу, є дуже позитивною ініціативою, що сприятиме забезпеченню того, щоб будь-які оперативно-розшукові заходи були пропорційними і необхідними. Це також сприятиме зменшенню масштабів і ймовірності зловживань або надмірного застосування оперативно-розшукових заходів.

Стаття 12

5.30 Дивись зауваження та рекомендації, що стосуються цієї статті, у Розділі «Загальні зауваження», пункт 4.11, і рекомендацію 1, наведені вище.

5.31 Конкретний перелік обов'язків підрозділів, що проводять оперативно-розшукові заходи, є позитивною ініціативою, оскільки це забезпечує чіткий орієнтир для цих підрозділів. Це також має сприяти зменшенню масштабів і ймовірності зловживань або надмірного застосування оперативно-розшукових заходів.

Стаття 13

5.32 Не зовсім зрозуміло, чи стосується пункт 2 статті 13 CHIS, агента або негласного інформатора. CHIS, як правило, отримує плату за свою допомогу, хоча це не є обов'язковою вимогою. Необхідний контекст для того, щоб продемонструвати, чи йдеться про патріотично-налаштованого громадянина, який надає інформацію на «безоплатній основі», або ж існує система оплати чи винагороди за виконання конкретних завдань для осіб, які можуть співпрацювали на платній основі або вмотивовані взаємодіяти задля отримання певної винагороди. Статус особи має важливе значення для розуміння її мотивації, але також з точки зору того, щоб правоохоронні та інші органи мали змогу впоратися з існуючими ризиками.

5.33 Пункт 8 дозволяє одержання широкого спектру інформації, включаючи відомості, що становлять "комерційну і банківську таємницю". Слід розглянути питання відповідності цього положення вимогам статті 269 КПК і, у разі необхідності, внести зміни в цей пункт.

5.34 Пункт 14 виграв би, якби містив недвозначне твердження про те, що будь-яке застосування засобів фізичного впливу повинно бути мінімально необхідним для досягнення законної мети, що переслідується. Запропонована редакція цього пункту, здається, є стандартним формулюванням, що передбачає застосування сили для підтримки проведення оперативно-розшукових заходів. Хоча, якщо коротко, більше уваги слід приділити посиленню принципів необхідності та пропорційності.

Рекомендація 26: Пункт 14 статті 13 повинен містити чітку вимогу про те, що будь-яке застосування засобів фізичного впливу має бути мінімально необхідним для досягнення законної мети, що переслідується.

Рекомендація 27: Потрібно ретельно вивчити питання відповідності пункту 8 статті 13 Законопроекту вимогам статті 269 КПК.

5.35 Дивись також зауваження та рекомендації, що стосуються цієї статті, у Розділі «Загальні зауваження», пункт 4.19, і рекомендацію 6, наведені вище.

5.36 Згідно зі статтею 13 проекту Закону підрозділам, що здійснюють оперативно-розшукову діяльність, дозволяється отримувати доступ до даних, що зберігаються приватними юридичними особами, включаючи постачальників послуг у мережі Інтернет або мережах зв'язку загального користування. Оцінка українського національного законодавства у сфері зберігання інформації виходить за межі цього Висновку. Водночас для проведення повного аналізу відповідності запропонованого проекту Закону європейським стандартам у сфері захисту персональних даних, необхідно було б дослідити, чи відповідно до законодавства України мережі зв'язку загального користування зобов'язані зберігати дані, що стосуються життя особи та її контактів, а також чи обов'язок щодо зберігання таких даних відповідає вимозі «крайньої необхідності» (зокрема, якою є тривалість такого зберігання та порядок передачі такої інформації державним органам)[70].

Рекомендація 28: Потрібно вивчити питання про те, чи покладається за законодавством України обов'язок на мережі зв'язку загального користування щодо зберігання даних, які стосуються життя особи та її контактів, а також чи відповідає цей обов'язок принципу "крайньої необхідності".

Стаття 14

5.37 Пункт 4 містить заборону підбурювати або провокувати будь-яких осіб до вчинення правопорушень. Це є важливою гарантією. Проте слід розглянути питання щодо використання терміну «агент – провокатор» в якості універсального терміну і однозначного посилання на заборону підбурювання до вчинення злочину, яка закріплена у практиці ЄСПЛ за статтею 6 Конвенції. Існує відповідна практика Суду: рішення у справах «*Тейшейра де Кастро проти Португалії*»[71] і «*Раманаускас проти Литви*».[72]

5.38 Це може бути виключно питання тлумачення, але заборона на застосування сили, закріплена в пункті 5 статті 14, не повинна бути категоричною забороною. Виникають ситуації, коли підрозділи, які здійснюють оперативно-розшукові заходи, матимуть потребу у застосуванні сили для того, щоб захистити себе чи інших. Це чітко передбачено у пункті 14 статті 13.

[70] Внаслідок рішення у справі «Діджитал Райтс Ірландія та інші» (*Digital Rights Iriland and others*), яким було скасовано Директиву ЄС про зберігання даних, низка європейських країн реформувала своє національне законодавство у цій сфері. На сьогодні європейські країни розділилися з цього питання. Деякі з них жорстко дотримуються зобов'язання не запроваджувати зберігання даних, тоді як інші, зокрема Франція та Сполучене Королівство, жорстко зобов'язалися продовжувати практику зберігання даних. Для формування своєї позиції Україна має уважно слідкувати за наслідками обговорення цих питань. Дивись висновок Генерального адвоката Saugmandsgaard Øe від 19 липня 2016 року. Згідно з цим висновком загальний обов'язок зберігати дані, покладений державою-членом на постачальників послуг електронного зв'язку, може відповідати законодавству ЄС. Водночас цей обов'язок, за будь-яких умов, має бути обумовлений суворими гарантіями, http://curia.europa.eu/jcms/upload/docs/application/pdf/2016-07/cp160079en.pdf.

[71] *Teixeira de Castro v Portugal*, Рішення від 9 червня 1998 року, заява № 25829/94.

[72] *Ramanauskas v. Lithuania,* Рішення від 5 лютого 2008 року, заява № 74420/01.

Стаття 15

5.39 Безпека має першорядне значення для забезпечення того, щоб інформація, одержана в ході оперативно-розшукових заходів, не використовувалася всупереч вимогам законодавства. Належні заходи безпеки можуть забезпечити дотримання порядку передачі і зберігання інформації та прозорості даних про те, хто мав доступ до цієї інформації.

Рекомендація 29: Слід розглянути питання щодо доцільності включення слова "надійно" в частину 2, щоб текст звучав таким чином: "Інформація про об'єкти обліку фіксується і надійно зберігається у формі справ, картотек, а також шляхом переносу даних, що обліковуються, на цифрові носії".

5.40 Згідно з частиною 5 статті 15 строк збереження інформації, що стосується терористичних актів, обмежується п'ятьма роками. Цей строк є відносно коротким і в багатьох країнах така інформація буде зберігатися протягом значно довшого періоду часу. Якщо є законні підстави для збереження інформації, що стосується тероризму (або інших тяжких злочинів), протягом більш тривалих періодів, доцільно це зробити.[73]

5.41 Положення частини 4 статті 15 щодо «знищення» відомостей, одержаних внаслідок оперативно-розшукової діяльності (в тому числі персональних даних), сформульоване занадто загально і не містить жодних додаткових деталей/процедур, строків для знищення даних. Незрозуміло, що автори законопроекту мали на увазі у зазначеному формулюванні: «якщо вони не містять інформації про вчинення дій, заборонених законодавством України». Цю фразу можна тлумачити в широкому сенсі й незрозуміло, чи буде вона охоплювати конкретні кримінальні правопорушення або будь-які інші неправомірні дії.

5.42 Європейські стандарти, в тому числі Принцип 6 Рекомендації № (87) 15, вимагають встановлення суворих правил щодо знищення/видалення даних, здобутих в результаті спостереження, щоб запобігти залишенню спостереження прихованим після того, як цей факт відбувся. У внутрішньому законодавстві повинні бути передбачені достатньо чіткі процедури безпечної обробки, зберігання і знищення матеріалів, одержаних в результаті негласного спостереження.[74] Частина 3 статті 20 також є важливою у цьому контексті, оскільки стосується термінів зберігання закритих оперативно-розшукових справ.

Рекомендація 30: Запропонований Законопроект повинен передбачати процеси і процедури видалення даних. Якщо існує національне законодавство або інші обов'язкові правові норми, що врегульовують питання обробки перехоплених даних, запропонований проект Закону повинен містити чітке посилання на це законодавство.

5.43 Для української влади також важливо вивчити шляхи впровадження технічних засобів для забезпечення належного знищення даних, оскільки більша частина відомостей, одержаних в результаті таємного спостереження, буде в цифровій формі (дані електронного зв'язку, як зміст, так і метадані), аудіо- і відеозаписи, дані, перехоплені за допомогою мобільних телефонів, і т.д. В світлі існуючих та інноваційних технологій, а також «хмарних» рішень (cloud solutions) такі дані можуть залишатися доступними на серверах, в «хмарі» (cloud) або їх може бути легко скопіювати.

---

[73] Дивись, наприклад, рішення у справі «*Сегерштедт-Вайберг проти Швеції» (Segerstedt-Wiberg v. Sweden) від* 6 червня 2006 року, заява №62332/00.

[74] Дивись відповідну практику Суду: рішення у справі «*Р.Е. проти Сполученого Королівства»* (*R.E. v. United Kingdom*) від 27 жовтня 2015 року, заява № 62498/11, рішення у справі «*Ротару проти Румунії» (Rotaru v. Romania) від* 4 травня 2000 року (Велика Палата), заява № 28341/95, рішення у справі «*Кеннеді проти Сполученого Королівства*» (*Kennedy v. the United Kingdom*) від 18 травня 2010 року, заява № 26839/05.

Рекомендація 31: Законопроект повинен містити вимогу щодо проведення технічних заходів, спрямованих на забезпечення належного знищення даних.

5.44 Проект закону не містить положень щодо обробки і використання конфіденційних даних у контексті правоохоронної/розшукової діяльності. Наприклад, стаття 15 не містить жодної вказівки на те, як здійснюється обробка конфіденційних даних. Застосування частини 6 статті 22 також може мати наслідки для обробки конфіденційних персональних даних. Якщо інше не передбачено українським законодавством, рекомендується включити положення, яке дзеркально відображує формулювання, наведене у Принципі 2.4 Рекомендації № (87) 15, що регулює використання персональних даних у сфері правоохоронної діяльності.[75]

Рекомендація 32: Якщо інше не передбачено українським законодавством, рекомендується включити до Законопроекту положення, яке відображатиме зміст Принципу 2.4 Рекомендації № (87) 15 щодо збору і обробки конфіденційних даних у сфері правоохоронної діяльності.

5.45 Якщо це питання не врегульоване іншим чином, рекомендується запровадити у запропонований законопроект підхід, прийнятий у новій директиві ЄС 2016/680 про захист фізичних осіб в контексті обробки персональних даних уповноваженими органами для цілей запобігання кримінальним правопорушенням, їх розслідування, виявлення, та обвинувачення за них, або виконання кримінальних покарань, а також про вільне переміщення таких даних (більш відома під назвою "Поліцейська директива"). Відповідно до Поліцейської директиви "заходи, що вживаються розпорядником даних, повинні, крім іншого, включати розробку і реалізацію конкретних гарантій щодо поводження з персональними даними дітей, якщо це необхідно".

Рекомендація 33: Обробка даних, які стосуються дітей, потребує особливої уваги і повинна бути забезпечена посиленими гарантіями, такими як процедура регулярного перегляду ефективності обробки таких даних і більш жорсткі терміни зберігання.

5.46 Відповідно до європейських стандартів захисту даних, включаючи нову Поліцейську директиву ЄС, потрібно провести розмежування між різними категоріями суб'єктів даних (наприклад, обробка даних осіб, які не підозрюються у вчиненні злочину). Обробка даних осіб, які не підозрюються у вчиненні будь-якого злочину (крім потерпілих, свідків, інформаторів, осіб, з якими контактували підозрювані особи, партнерів/колег останніх), повинна строго відрізнятися від обробки даних осіб, що мають відношення до конкретного злочину, і «може бути дозволеною тільки за певних умов і лише коли це вкрай необхідно для досягнення законної, чітко визначеної та конкретної мети».[76] Запропонований проект не визначає, яким чином буде забезпечене таке розмежування між різними категоріями даних. Якщо інше не врегульоване законами України, рекомендується, щоб таке положення було включене в запропонований проект Закону. Таке розмежування також має важливі наслідки для належної реалізації принципів захисту даних (наприклад, обмеження щодо мети використання, законність обробки).

[75] "Збір даних про осіб лише на тій підставі, що вони мають особливе расове походження, особливі релігійні переконання, сексуальну поведінку чи політичні погляди або належать до особливих рухів чи організацій, які не оголошені поза законом, повинен бути заборонений. Збір даних, що торкаються цих характеристик, може здійснюватися у разі виняткової потреби для цілей конкретного розслідування."

[76] На думку європейських органів із захисту даних, така обробка повинна «бути обмежена чітко визначеним періодом часу і подальше використання цих даних для інших цілей має бути заборонене.» Спеціальний захист "осіб, які не підозрюються у вчиненні злочину", особливо необхідний у тих випадках, коли обробка не здійснюється в рамках розслідування конкретного злочину або переслідування за злочин.

Рекомендація 34: Для того, щоб забезпечити наближення до європейських стандартів захисту даних, слід провести розмежування між різними категоріями суб'єктів даних (наприклад, обробка даних осіб, які не підозрюються у вчиненні злочину).

Стаття 16

5.47 У пункті 5 статті 16 йдеться про стандарти накопичення даних. Наприклад, чи існує визначений стандарт для ведення матеріалів кримінальних справ і складання заяв/дозволів щодо проведення негласних слідчих (розшукових) дій, який був би прийнятним для прокурора і полегшував би заходи судового нагляду? Предметом розгляду може стати доцільність включення цього питання у законодавство або будь-які внутрішні принципи діяльності або процедури, що забезпечить узгодженість стандартів і сприятиме проведенню будь-яких перевірок.

5.48 Як було зазначено вище стосовно частини 2 статті 15, слід вивчити питання щодо включення слова "надійно" в запропоновану редакцію частини 5 статті 16, з тим, щоб це положення було сформульоване таким чином: «Матеріали про результати проведення оперативно-розшукових заходів надійно накопичуються в оперативно-розшукових справах».

5.49 Дивись також зауваження та рекомендації, що стосуються цієї статті, у Розділі «Загальні зауваження», пункт 4.31, наведений вище.

Стаття 18

5.50 Стаття 18 стосується заведення оперативно-розшукових справ за визначених обставин. Важливо звести до мінімуму ймовірність здійснення різними органами оперативно-розшукових проваджень стосовно тих самих осіб або груп осіб. Подібна ситуація може виникнути, якщо аналогічна інформація отримується більш ніж одним підрозділом або установою і така інформація фактично або, на думку цих органів, входить до їх компетенції.

5.51 Якщо має бути заведена лише одна оперативно-розшукова справа, необхідно забезпечити функціонування механізму, який би унеможливлював заведення різними підрозділами або установами оперативно-розшукової справи на підставі тієї ж інформації. Необхідна координація для того, щоб уникати конфліктів, потенційних ризиків, а також для забезпечення максимально ефективного використання ресурсів. Це може бути темою для міркування для посадових осіб, що визначають політику в межах кожної конкретної установи, або для вирішення за допомогою координаційного форуму.

Стаття 24

5.52 У частині 3 статті 24 допускається надання показів у суді керівником відповідного підрозділу, що здійснює оперативно-розшукову діяльність, в тих випадках, коли особа, залучена до оперативно-розшукової діяльності, в результаті надання таких показів опиниться у небезпеці. Важливо забезпечити, щоб це не призводило до порушення права на справедливий суд (гарантія "рівності сторін"). За певних умов можна захистити персональні дані свідків. Проте, якщо докази мають вирішальне значення для встановлення вини чи невинуватості підсудного, свідку може бути висунута вимога щодо особистої дачі показів.[77] Побоювання свідка щодо існування небезпеки для нього мають бути об’єктивно обґрунтовані; для керівника відповідного підрозділу, що здійснює оперативно-розшукову

[77] Рішення у справі «*Аль-Хаваджа і Тахері проти Сполученого Королівства*» (*Al-Khawaja and Tahery v. United Kingdom*)(Велика Палата) від 20 січня 2009 року, заяви №№ 26766/05 і 22228/06, пункт 147.

діяльність, недостатньо заявити про існування небезпеки.[78] Крім цього, слід дотримуватися вимог статті 97 КПК (зокрема частини 5).

Рекомендація 35: Використання положень частини третьої статті 24, що дозволяє давати показання в суді керівнику відповідного підрозділу, має базуватися на об'єктивно обґрунтованих побоюваннях та відповідати статті 97 (зокрема частині п'ятій) КПК.

Стаття 31

5.53 На додаток до концептуальних зауважень і рекомендацій стосовно того ж набору запобіжних заходів і гарантій, що підлягають застосуванню по відношенню до заходів, які передбачають обмеження прав і свобод людини, і відповідних процесуальних норм,[79] варто ще раз підкреслити, що в статті не вистачає достатньо детальних, чітких посилань на конкретні статті КПК.

5.54 Крім того, пропонований проект зобов'язує державу повідомляти лише ту інформацію про оперативно-розшукові заходи, яка вважається статистичною. Існує потреба у більшій прозорості, підзвітності та демократичному контролі для підвищення довіри громадян. Звіти мають містити більш детальну інформацію (наприклад, обсяг і розміри приватних електронних повідомлень, що зберігаються у державних органах, кількість і типи запитів, що були задоволені, види оперативно-розшукових заходів, які на цій підставі були проведені (наприклад, перехоплення повідомлень і розмов, відеоспостереження, метадані або контент перехоплених даних). Існуючий формат громадського та парламентського контролю не передбачає процедури, за якої громадськість могла б отримати достатньо докладну інформацію про характер спостереження (контролю). Більш того, у цій сфері парламентський контроль повинен бути більш активним з ширшими повноваженнями щодо нагляду за законністю заходів зі спостереження, які проводяться відповідними органами. Якщо обробка персональних даних в контексті діяльності правоохоронних органів підпадає під юрисдикцію Уповноваженого Верховної Ради України з прав людини (Омбудсмена), у запропонованому проекті Закону або у Законі «Про захист персональних даних» необхідно чітко це зазначити (в даному випадку Омбудсмен виступає в якості загального незалежного контрольного органу).

Рекомендація 36: Якщо Омбудсмену не вистачає повноважень щодо здійснення контролю за дотриманням прав і свобод людини під час таємного спостереження, має бути створений незалежний контрольний орган, не підвідомчий органам поліції, який повинен відповідати за забезпечення дотримання принципів захисту персональних даних в контексті правоохоронної діяльності (Принцип 2.4 Рекомендації № (87) 15).[80] Контроль з боку цього органу повинен бути додатковим поряд з прокурорським та судовим наглядом, якщо інше не передбачено законодавством, і міг би зосередитися на системних питаннях, а не на окремих випадках.

Розділ 7

[78] *Дивись той самий документ, пункт* 124.
[79] Дивись, наприклад, пункти 4.1 та 4.13, наведені вище.
[80] ЄСПЛ стверджує, що для судді бажано здійснювати функції нагляду. Це не виключає, що інший орган також може відповідати за здійснення нагляду, «якщо тільки цей орган є достатньо незалежним від виконавчої гілки влади» та «від органів, які здійснюють спостереження, а також наділений достатніми повноваженнями і компетенцією для здійснення ефективного і безперервного контролю». ЄСПЛ також "відзначає, що вкрай необхідним є надання контрольному органу доступу до відповідних документів, включаючи засекречені матеріали». Нарешті, ЄСПЛ бере до уваги, «чи діяльність контрольного органу є відкритою для громадського контролю»."

5.55 Назва цього розділу звужує роль, якою наділена прокуратура відповідно до Конституції (стаття 131), а також функцій, передбачених в усьому тексті проекту Закону, зокрема статтях 34 і 35. Цей контроль не обмежується дотриманням законності під час проведення оперативно-розшукової діяльності та поширюється на організаційні питання, а також здійснення керівництва ними. Відповідно, термін «дотримання законності» не відображає дійсної ролі, яку відіграє прокуратура, і повинен бути вилучений.

Рекомендація 37: Фраза "дотримання законності" має бути вилучена з назви Розділу.

Стаття 34

5.56 Частина 1 статті 34 має бути змінена у відповідності до зауважень і рекомендацій щодо обсягу прокурорського нагляду.[81]

Стаття 35

5.57 Дивись також зауваження та рекомендації, що стосуються цієї статті, у Розділі «Загальні зауваження», пункт 4.33, наведений вище.

5.58 Для забезпечення чіткості слід розглянути питання щодо викладення ролі прокурора у виняткових невідкладних випадках. Включення таких положень мало б позитивний вплив на цю статтю та відповідало б вимогам статті 250 КПК.

Стаття 38

5.59 Відрадно відзначити, що існує законодавча норма, спрямована на забезпечення міжвідомчої взаємодії, яка може сприяти подоланню потенційних перешкод на шляху розвитку культури міжвідомчої співпраці, коли різні установи працюють ізольовано одна від одної, а також просуванню і розвитку професійної практики.

Стаття 39

5.60 Ця стаття передбачає загальний огляд повноважень, наданих слідчим щодо проведення слідчих (розшукових) дій в рамках вирішення завдань будь-якого кримінального провадження. Проте, існує можливість покращити чіткість формулювання термінів, які наразі є неоднозначними, наприклад, пунктів 1 і 2 частини 1 «аудіоконтроль особи» і «відеоконтроль особи». Не зовсім зрозуміло, чи стосуються ці терміни «аудіоспостереження за особою» і «відеоспостереження за особою», передбачених у Розділі «Визначення термінів» на початку проекту Закону. Важливо, щоб термінологія, яка використовується у проекті Закону, узгоджувалася в усьому його.

5.61 Дивись також зауваження та рекомендації, що стосуються цієї статті, у Розділі «Загальні зауваження», пункти 4.13 і 4.20, і рекомендації 1 та 5, наведені вище.

Стаття 40

Рекомендація 38: Частина 1 статті 40 має бути приведена у відповідність до статті 41 КПК шляхом уточнення того, що слідчі (розшукові) дії здійснюються за письмовим дорученням.

[81] Дивись пункт 4.12 і рекомендацію 3, наведені вище.

Стаття 41

5.62 Ця стаття стосується повноважень щодо залучення (найму) і постановки завдань інформатору/агенту або CHIS для негласного збору інформації в цілях кримінального провадження. У частині 1 йдеться про співпрацю з цими особами на «постійній основі». Цей термін є потенційно неоднозначним, оскільки він може стосуватися агента, який здійснює тривале проникнення у злочинне середовище, або фізичної особи, яка завербована для виконання завдань протягом конкретної операції. Пропонується уточнити цей термін.

5.63 Частини 2 і 3 видаються спрощеними з урахуванням складності і ризиків, пов′язаних із залученням CHIS до проведення оперативно-розшукових дій. Стаття 275 КПК містить рамкові положення щодо використання конфіденційного співробітництва, в тому числі обмеження щодо залучення до такої співпраці конкретних категорій осіб. Отже потрібно відповідним чином послатися на цю статтю КПК і процитувати її положення.

5.64 Існує також потреба у розробці та застосуванні відповідної інструкції для забезпечення захисту прав CHIS. Зокрема, якщо існує завчасно передбачувана вірогідність того, що роль CHIS або інформація, отримана за його/її допомогою, стане актуальною в рамках будь-якого подальшого досудового слідства, необхідним є ретельне вивчення цього питання й управління ризиками. Це може бути темою для подальших міркувань, а також розробки відповідних положень, які дозволять ефективно здійснювати вербування і постановлення завдань для CHIS. Можна зробити це шляхом розробки інструкції або іншого відповідного організаційно-розпорядчого документа.

Рекомендація 39: Термін “на постійній основі” потребує роз’яснення.

Рекомендація 40: Потрібно включити посилання на статтю 275 КПК і положення з неї. Необхідно розглянути питання розробки практичних рекомендацій щодо процедури, яка підлягатиме застосуванню у випадках, коли роль таємного інформатора (CHIS) вірогідно буде розкрита під час будь-якого наступного досудового розслідування.

Стаття 42

5.65 Стаття 254 КПК передбачає заходи щодо захисту і використання інформації, одержаної в результаті проведення негласних слідчих (розшукових) дій, тому потрібно відповідним чином включити посилання на цю статтю і положення з неї.

Рекомендація 41: Потрібно включити посилання на статтю 254 КПК та її положення.

Перелік рекомендацій

Рекомендація 1: Рекомендується безпосередньо вказати, що пункт 3 статті 12 та пункти 3 і 4 статті 39 підпорядковуються вимогам статті 214 КПК в частині внесення до реєстру інформації щодо дійсного чи можливого вчинення злочину протягом 24 годин з моменту отримання такої інформації. Крім того, слід заборонити проведення оперативно-розшукових операцій поза межами цього строку без спеціального дозволу, що отримується в порядку, передбаченому Законопроектом. Нарешті, слід прямо заборонити детективам проводити будь-які заходи без дозволу, а також встановити вимогу про обов'язок звертатися за інструкціями на проведення конкретних заходів до слідчого органу чи прокурора у відповідності до статті 41 КПК.

Рекомендація 2: Для уникнення непорозумінь щодо значення цілого ряду термінів у Законопроекті та КПК рекомендується надати їм однакове визначення в обох текстах.

Рекомендація 3: Законопроект повинен містити чіткі й конкретні вимоги про поширення на нього процесуальних гарантій того ж рівня, що й гарантії за КПК, зокрема, в частині прокурорського й судового контролю.

Рекомендація 4: Законопроект повинен передбачати, що після завершення оперативно-розшукових заходів особи, до яких вони застосовувалися, повинні в міру можливості про це повідомлятися. Це слід зробити у спосіб, аналогічний до того, як це зроблено у статтях 253 та 254 КПК.

Рекомендація 5: Мінімальні умови для затримання, передбачені пунктом 2 частини 6 статті 10 та частиною 3 статті 39, необхідно привести у відповідність із положеннями статті 207 КПК.

Рекомендація 6: У Законопроекті слід використовувати такий самий підхід, що й у КПК, тобто визначити, що перевірки юридичних осіб за пунктом 19 частини 2 статті 10 можуть проводитися лише в рамках конкретних гласних чи негласних оперативно-розшукових заходів.

Рекомендація 7: Було б доцільно, щоб стаття 9 Законопроекту передбачала, що, якщо злочин було скоєно (є склад злочину – *corpus delicti*), незалежно від того, був він закінченим чи ні[82], або там, де вимоги конкретних запобіжних заходів не були виконані, будь-які подальші дії повинні бути слідчими, що здійснюються на підставі відповідних положень КПК.

Рекомендація 8: Пунктом 3 частини 1 статті 9 необхідно перебачити вимогу про існування підстав для проведення конкретного оперативно-розшукового заходу. Пунктом 4 необхідно передбачити вимогу про наявність достатніх підстав підозрювати особу у вчиненні конкретних дій, що пов'язані чи потенційно пов'язані з кримінально караними діяннями індивідуального чи системного характеру: відмивання брудних коштів, фінансування тероризму тощо.

Рекомендація 9: Термінам, що містяться в пунктах 20, 21 та 22 частини 2 статті 10, необхідно дати більш точне визначення.

[82] Як це визначено у статті 13 Кримінального кодексу України.

Рекомендація 10: До Законопроекту слід безпосередньо включити положення статті 250 КПК або конкретне посилання на вимоги цієї статті.

Рекомендація 11: Законопроект повинен включати вимогу про те, що усі оперативно-розшукові заходи, включаючи будь-яку пов'язану з ними інформацію, у т.ч. отриману інформацію, повинні належним чином реєструватися.

Рекомендація 12: Законопроект повинен містити таблицю, де описані зміни до інших законодавчих актів, що вносяться відповідно до Законопроекту.

Рекомендація 13: Законопроект повинен врегулювати аспекти захисту персональних даних у контексті правоохоронної діяльності більш системно (наприклад, шляхом включення відповідного розділу з детально виписаними положеннями або прийняття спеціального закону з захисту даних, що покривав би правоохоронні органи).

Рекомендація 14: У визначенні терміну "аудіоконтроль особи" в Законопроекті має бути проведена різниця між різними формами аудіоконтролю, які дозволяється здійснювати, зокрема, між використанням пристроїв прослуховування та перехопленням телефонних розмов, а також між заходами з аудіоконтролю особи залежно від місця, в якому вони проводяться.

Рекомендація 15: Законопроект має містити чітке положення про те, що будь-які дії, пов'язані із залученням неповнолітніх до оперативно-розшукової діяльності, повинні мати за основну мету захист найкращих інтересів дитини.

Рекомендація 16: До Законопроекту потрібно включити додаткові положення, що врегулюють застосування методу поліграфного опитування, або конкретну відсилку до відповідних законодавчих норм.

Рекомендація 17: Необхідно розглянути питання щодо виключення пункту 2 статті 2.

Рекомендація 18: Сферу застосування пункту 3 статті 2 слід переглянути з тим, щоб не допустити будь-якого розширеного тлумачення і несанкціонованого застосування оперативно-розшукових заходів, а також забезпечити, щоб цей пункт унеможливлював обробку персональних даних за надмірно широкого переліку обставин.

Рекомендація 19: З метою забезпечення узгодженості з положеннями Конвенції та практикою ЄСПЛ стаття 4 проекту Закону має включати в себе в якості принципу оперативно-розшукової діяльності *необхідність у демократичному суспільстві в інтересах національної та громадської безпеки, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод людини*. Цей принцип потрібно також включити до частини 2 статті 6 законопроекту.

Рекомендація 20: Законопроект повинен містити норми, які регулюють питання управління інформацією, зібраною в ході оперативно-розшукової діяльності, що стосується осіб, які не підозрюються у вчиненні будь-яких незаконних дій.

Рекомендація 21: Частина 2 статті 6 повинна містити положення про судовий захист права на відшкодування шкоди у відповідних випадках.

Рекомендація 22: У частині 3 статті 6 слід прописати чіткий механізм реалізації на практиці права бути поінформованим про перебування у статусі об'єкта оперативно-

розшукових заходів. Будь-які обмеження цього права, викликані необхідністю зберігти таємницю організації і тактики слідчих дій, повинні бути мінімально необхідними для захисту цієї таємниці і не повинні надмірно перешкоджати реалізації права на інформацію.

Рекомендація 23: Частина 2 статті 7 повинна передбачати розголошення персональних даних CHIS у випадках, коли це необхідно для захисту їх життєво важливих інтересів.

Рекомендація 24: Якщо залучення CHIS не розглядаються в якості оперативно-розшукового заходу, передбаченого частиною 2 статті 10, потрібно включити до проекту Закону окрему норму про залучення CHIS.

Рекомендація 25: Оперативно-розшукові заходи, передбачені пунктами 15 ("спостереження за річчю або місцем") і 22 ("радіотехнічна розвідка") частини 2 статті 10, повинні бути додані до групи оперативно-розшукових заходів, перелічених у пунктах 1-11, які вимагають застосування додаткових процесуальних гарантій.

Рекомендація 26: Пункт 14 статті 13 повинен містити чітку вимогу про те, що будь-яке застосування засобів фізичного впливу має бути мінімально необхідним для досягнення законної мети, що переслідується.

Рекомендація 27: Потрібно ретельно вивчити питання відповідності пункту 8 статті 13 Законопроекту вимогам статті 269 КПК.

Рекомендація 28: Потрібно вивчити питання про те, чи покладається за законодавством України обов'язок на мережі зв'язку загального користування щодо зберігання даних, які стосуються життя особи та її контактів, а також чи відповідає цей обов'язок принципу "крайньої необхідності".

Рекомендація 29: Слід розглянути питання щодо доцільності включення слова "надійно" в частину 2, щоб текст звучав таким чином: "Інформація про об'єкти обліку фіксується і надійно зберігається у формі справ, картотек, а також шляхом переносу даних, що обліковуються, на цифрові носії".

Рекомендація 30: Запропонований Законопроект повинен передбачати процеси і процедури видалення даних. Якщо існує національне законодавство або інші обов'язкові правові норми, що врегульовують питання обробки перехоплених даних, запропонований проект Закону повинен містити чітке посилання на це законодавство.

Рекомендація 31: Законопроект повинен містити вимогу щодо проведення технічних заходів, спрямованих на забезпечення належного знищення даних.

Рекомендація 32: Якщо інше не передбачено українським законодавством, рекомендується включити до Законопроекту положення, яке відображатиме зміст Принципу 2.4 Рекомендації № (87) 15 щодо збору і обробки конфіденційних даних у сфері правоохоронної діяльності.

Рекомендація 33: Обробка даних, які стосуються дітей, потребує особливої уваги і повинна бути забезпечена посиленими гарантіями, такими як процедура регулярного перегляду ефективності обробки таких даних і більш жорсткі терміни зберігання.

Рекомендація 34: Для того, щоб забезпечити наближення до європейських стандартів захисту даних, слід провести розмежування між різними категоріями суб'єктів даних (наприклад, обробка даних осіб, які не підозрюються у вчиненні злочину).

Рекомендація 35: Використання положень частини третьої статті 24, що дозволяє давати показання в суді керівнику відповідного підрозділу, має базуватися на об'єктивно обґрунтованих побоюваннях та відповідати статті 97 (зокрема частині п'ятій) КПК.

Рекомендація 36: Якщо Омбудсмену не вистачає повноважень щодо здійснення контролю за дотриманням прав і свобод людини під час таємного спостереження, має бути створений незалежний контрольний орган, не підвідомчий органам поліції, який повинен відповідати за забезпечення дотримання принципів захисту персональних даних в контексті правоохоронної діяльності (Принцип 2.4 Рекомендації № (87) 15). Контроль з боку цього органу повинен бути додатковим поряд з прокурорським та судовим наглядом, якщо інше не передбачено законодавством, і міг би зосередитися на системних питаннях, а не на окремих випадках.

Рекомендація 37: Фраза "дотримання законності" має бути вилучена з назви Розділу.

Рекомендація 38: Частина 1 статті 40 має бути приведена у відповідність до статті 41 КПК шляхом уточнення того, що слідчі (розшукові) дії здійснюються за письмовим дорученням.

Рекомендація 39: Термін "на постійній основі" потребує роз'яснення.

Рекомендація 40: Потрібно включити посилання на статтю 275 КПК і положення з неї. Необхідно розглянути питання розробки практичних рекомендацій щодо процедури, яка підлягатиме застосуванню у випадках, коли роль таємного інформатора (CHIS) вірогідно буде розкрита під час будь-якого наступного досудового розслідування.

Рекомендація 41: Потрібно включити посилання на статтю 254 КПК та її положення.