GUIDES TO GOOD GOVERN-ANCE

No. 06

Балансування відкритості та конфіденційності в оборонному секторі: уроки успішної міжнародної практики

Centre for Integrity in the Defence Sector

Міністерство оборони України

Norwegian Ministry of Defence

ЦЕНТР З РОЗБУДОВИ ДОБРОЧЕСНОСТІ В ОБОРОННОМУ СЕКТОРІ

Центр з розбудови доброчесності в оборонному секторі (ЦДОС) здійснює сприяння доброчесності, боротьбі з корупцією та належному врядуванню в оборонному секторі. Центр співпрацює з норвезькими та міжнародними партнерами з метою підвищення рівня компетентності, інформування і надання практичних засобів для зменшення ризику корупції. ЦДОС було створено Міністерством оборони Норвегії у 2012 році.

ПРО АВТОРА

Франсіско Кардона (Francisco Cardona) – асоційований міжнародний експерт ЦДОС. Кардона є відомим фахівцем з розроблення та оцінювання реформ державної служби і державного управління, адміністративного права і правосуддя, антикорупційної політики та інституційного розвитку. Його професійний досвід включає роботу як на батьківщині – в Іспанії, де він зробив кар'єру у державній службі, так і у міжнародних організаціях, таких як ОЕСР та програма SIGMA, де він протягом 15 років працював старшим політичним аналітиком у сфері державного врядування. Працюючи у SIGMA, він консультував близько 25 країн з перехідною економікою та країн, що розвиваються, у Східній Європі, Африці, Латинській Америці та Карибському регіоні. Він отримав юридичну освіту (Університет Валенсії, 1976 рік) і має декілька ступенів магістра у сфері державного управління.

ПЕРЕДМОВА

Першочерговим завданням Посібників з належного врядування, розроблених ЦДОС, є ознайомлення з ключовими питаннями, що мають відношення до сфери «належного врядування». Посібники мають стислу форму, але в той же час викладені в них питання занадто не спрощуються.

У шостому Посібнику з належного врядування автор має на меті переглянути концепцію конфіденційності в оборонному секторі. Розглядаючи цю тему, автор ставить питання: «(...) де повинен бути баланс між вільним доступом до інформації та обмеженням цього доступу в певній мірі» в демократичному суспільстві з (...) «відкритим урядом»? Крім того, коли виникає необхідність обмежувати інформацію з міркувань національної безпеки? Розглядається право громадян на державний захист.

Цей Посібник написаний Франциско Кардона, старшим міжнародним експертом ЦДОС. Я хотів би подякувати йому за внесок у таку важливу тему в галузі належного врядування. Ця тема має високу актуальність у публічних дискусіях протягом останніх років і, ймовірно, продовжить бути актуальною в наступні роки.

Я також хотів би подякувати редактору центру Бьорду Бредруп Кнуцену та нашому координатору публікацій Асе Марі Фоссум за їхній внесок у Посібник.

Центр сподівається, що цей Посібник з належного врядування буде використаний широкою аудиторією як в державному секторі, включаючи оборонну сферу, так і поза його межами. Збалансованість відкритості та конфіденційності є життєво важливою для добре функціонуючого демократичного суспільства.

ЦДОС буде вдячний за отримані відгуки щодо Посібника.

Осло, 24 квітня 2018 року.

Пер Крістенсен
Директор

ЗМІСТ

Вступ

У цьому Посібнику з належного врядування представлено короткий огляд передових практик країн ЄС та ОЕСР, спрямованих на збереження конфіденційності публічної інформації в секторі оборони та національної безпеки, а також сприяння загальному праву громадськості на доступ до інформації, що зберігається державними установами. Метою цього посібника є надання політик, які сприяють відкритому урядуванню, доступу до інформації та спроможності громадян приймати обґрунтовані рішення щодо діяльності урядів. У той же час, окреслюються межі для надійного захисту державної таємниці у тих питаннях, які є чутливими для національної безпеки, оборони та розвідки, а також у сфері боротьби з корупцією та злочинністю.

Прозорість та публічність є чудовими профілактичними засобами проти корупції, неналежного адміністрування та слабкого управління. Демократії не можуть діяти належним чином в умовах секретності, оскільки, якщо секретність переважає, то політичний режим просто стає недемократичним, адже громадяни виключаються з цього процесу. Це означає, що здійснення владних повноважень може вийти з-під контролю, а демократична підзвітність не може бути реалізована. Однак, доступ громадськості до інформації також може бути обмежений для збереження правильного функціонування демократії в ефективно керованій державі. Тому, як розкриття публічної інформації, так і певні обмеження у цьому питанні повинні однаковою мірою служити інтересам суспільства.

.

Концептуальна база: національна безпека як виправдання конфіденційності

Основне концептуальне припущення полягає в тому, що відкритий уряд і вільний доступ до інформації, з одного боку, та обмеження доступу в певній мірі, з іншого боку, мають користь для суспільних інтересів. Загальноприйнятий на міжнародному рівні принцип зводиться до того, що уряди повинні пропагувати «право знати», при цьому встановлюючи розумні межі для захисту конфіденційності певної публічної інформації. Останнє є необхідним для ефективної реалізації державної діяльності у певних сферах, зокрема в питаннях національної безпеки та оборони.

Основна проблема, що стосується такої секретності, полягає у визначенні того, коли і як обмеження доступу громадськості до інформації є легітимним. Амбітною метою здорових демократій є забезпечення належного доступу громадськості до інформації, одночасно визначаючи певні законні межі для обмеження цього доступу. Встановлення правильного балансу між цими двома поняттями значною мірою залежить від історії країни, суспільних цінностей та інших культурних факторів. Саме через це важко визначити, чи існують міжнародні стандарти, щоб допомогти досягти правильного балансу у цьому питанні (Трансперенсі Інтернешнл Великобританія, 2014 р.). На практиці точних міжнародних стандартів не існує, хоча інтелектуальні дискусії та спроби створення деяких загальних принципів останнім часом є досить численними.[1]

Якщо залишити без нагляду практику забезпечення таємності та конфіденційності, вона легко набуває значних розмірів і поширення. Деякі державні служби, які займаються питаннями національної безпеки, оборони, кримінальних розслідувань, розвідки або протидії тероризму, мають тенденцію застосовувати секретність до всього, що вони роблять, навіть якщо це перешкоджає праву громадян знати, що робить уряд. Крім високих витрат на підтримку роботи «механізму секретності», істотне та широке використання конфіденційності, як правило, підриває довіру громадськості до державних установ та, зрештою, послаблює демократичну легітимність. Занадто велика секретність також призводить до більшої кількості помилок і порушень, ніж за умов прозорості та громадського контролю, оскільки відсутність прозорості ускладнює громадський контроль та виправлення неналежних практик. Як результат, у довго-

1 Див. Принципи Цване (2013 р.). Доступно за посиланням https://www.opensocietyfoundations.org/fact-sheets/tshwane-principles-national-security-and-right-information-overview-15-points

строковій перспективі надмірна секретність може загрожувати національній безпеці більше, ніж відкритість.

Як стверджують деякі державні чиновники – наприклад, у США – занадто велика секретність «стала необґрунтованою перешкодою для обміну інформацією всередині і поза урядом, що завдає шкоди державній політиці» (Афтергуд, 2008 р., стор. 400). Це вказує на проблему надмірної таємності, тобто служби зберігання такого виду інформації прагнуть засекретити дані в тій мірі, яка значно перевищує насправді необхідну.

Мета будь-якої системи секретності – не допустити розкриття інформації, що може загрожувати національній безпеці, але розмитість таких понять як «національна безпека» та «загрози безпеці» легко призводить до надмірного використання секретності. Труднощі розмежування фактичної та суб'єктивної інформації ускладнюють встановлення чітко визначених критеріїв для коректного засекречення інформації.

Правильна секретність інформації сама по собі є дуже складним поняттям, але концептуально ми можемо погодитись, що «правильна» секретність – це та, яка є обґрунтованою та якомога більше наближеною до демократичних цінностей відкритості, прозорості та вільного доступу до інформації. Інакше кажучи, ми можемо погодитися, що розумне обмеження прозорості стосується того, що а) є винятковим, і б) захищає важливі інтереси національної безпеки. Цей висновок підтверджує, що в галузі оборони та національної безпеки є інформація, приховування якої *не є* критичним для національної безпеки, і тому може бути безпечно розкрита – повністю або частково.

У деяких демократичних країнах досі превалює традиційний підхід, згідно якого прозорість представляє лише потребу громадянина, а секретність заради національної безпеки представляє суспільний інтерес. Наприклад, пан Жан Марк Сове, заступник президента Державної Ради Франції, сказав у своєму зверненні до Національної асамблеї Франції, нижньої палати французького парламенту, 5 липня 2011 року: «Напрямком для подальших дій є створення лінії розмежування між легітимними державними інтересами, які вимагають секретності, та прозорістю, якої потребують громадяни» (Сове, 2011 р., стор. 6). Ця заява ґрунтується на припущенні, що збереження таємності захищає суспільний інтерес, тоді як прозорість є не суспільним інтересом, а лише запитом, викликаним цікавістю громадян та журналістів. Це припущення є дуже сумнівним. Як показує досвід, сприяння прозорості є одним із найкращих способів захисту суспільних інтересів, оскільки це сприяє тому, що державні органи залишаються підзвітними громадянам та забезпечує роботу інших механізмів демократичного контролю. Отже, прозорість, а не секретність, може розглядатися як засіб для *скорочення* «розриву, який природним чином виникає між державою та громадськістю» (Фенстер, 2010 р, стор. 619).

Існує широкий міжнародний консенсус, що прозорість у політиці та діяльності органів державної влади має бути загальним правилом, тоді як секретність повинна бути винятком. Більше того, такі винятки повинні бути виправданими: їх можна відстоювати лише, якщо вони є легітимними. А вони вважаються легітимними тільки тоді, коли можна довести, що ці винятки необхідні задля захисту істинних інтересів національної безпеки.

Необхідність розмежування між легітимною та нелегітимною секретністю обумовлює потребу у контролі з боку органів влади, незалежних від установи, яка засекречує інформацію. Такі незалежні механізми контролю можуть здійснюватися судами або більш спеціалізованими державними органами, і їхня роль полягає у встановленні того, чи дійсно інтереси національної безпеки, на які посилаються під час засекречення інформації, є справжніми та достатньо важливими. Без механізмів зовнішнього контролю рішення щодо засекречення інформації стають виключно дискреційними та, швидше за все, довільними. Однак, як ми побачимо нижче, історично суди відігравали роль, і все ще схильні її виконувати, яка демонструє надмірно прихильне ставлення до приховування інформації органами безпеки або службами розвідки.

Концептуально, повна прозорість не є бажаною і, мабуть, не є можливою, як зазначалося раніше. Крім того, держава завжди має діяльність у певних сферах, які є неясними або неоднозначними. Як зазначає Фенстер (2010 р., стор. 623), часто є зона між секретністю та прозорістю, що означає, що секретність не обов'язково є повною протилежністю прозорості. На практиці секретність та прозорість не є чітко протилежними реаліями, оскільки і секретність, і прозорість потребують окремих інституційних баз, які структурно відрізняються (Різ, 2014 р., стор. 14).

Більша прозорість не обов'язково має означати меншу секретність, але її краща якість може захистити конфіденційність. Більша прозорість означає, що будуть захищені лише істотні потреби в конфіденційності. Інституціоналізація політик прозорості є відносно новим процесом у більшості країн, тоді як інституціоналізація секретності походить з давно сформованих традицій. Цінності та інтереси, що стоять за кожною з цих традицій, все ще є неоднорідними та дещо непослідовними. Основний виклик полягає у поступовій гармонізації інституціоналізованого права на обізнаність та захист справжніх потреб у конфіденційності в організаційних структурах, які мають справу з ними, та в державних практиках. Пошук більшої узгодженості між цими двома політиками в ідеалі повинен сприяти формуванню єдиної, інтегрованої політики та більш узгодженій інституціоналізації доступу до інформації в рамках національних урядів, у відповідності до потреб національної безпеки.

Однак, поняття «національної безпеки» є надзвичайно розмитим, оскільки воно може означати різні речі в різних національних контекстах, що ще більше ускладнює проблему. У більшості європейських країн, які досліджувала Якобсен (2013 р.), національна безпека в тій чи іншій мірі охоплює міжнародні відносини і внутрішні загрози безпеці. Інакше кажучи, в цьому питанні не обов'язково існує очевидна межа.

Для того щоб встановити, чи є правомірною застосована урядом секретність, Афтергуд (2009 р., стор. 402-403) пропонує три практичні категорії секретності, і визнає, що тривалий час проблема державної політики у цій сфері полягає у відокремленні легітимної секретності від нелегітимної, та у збереженні першої і розкритті другої:

1. **Істинна секретність національної безпеки:** захист інформації, яка може створювати визначену загрозу національній безпеці через компрометацію її оборони або зовнішньої діяльності. Утримування такої інформації не є спірним, оскільки це є логічним обґрунтуванням всіх систем

секретності, і коли такий тип інформації залишається таємним, це найкращим чином служить державним інтересам.

2. **Бюрократична секретність:** схильність бюрократів до захисту інформації, виходячи зі зручності або через підозри, що оприлюднення даних може бути більш ризикованим, ніж утримування їх у таємниці. Ця бюрократична тенденція зазвичай призводить до надмірної секретності інформації і в результаті – до великого обсягу непотрібної таємної інформації. Це також збільшує бюджетні витрати на забезпечення секретності і часто грає на бюрократичних почуттях власної важливості та небажанні певних установ розкривати інформацію про те, як вони виконують свою роботу.

3. **Політична секретність:** схильність використовувати секретність для досягнення політичної вигоди. Ця форма секретності є найбільш спірною і небажаною, оскільки вона використовує визнану легітимність справжніх інтересів національної безпеки для просування програм, які використовуються задля власної вигоди, для уникнення політичних суперечок або підриву державної підзвітності. У крайніх випадках політична таємниця приховує порушення закону, порушення прав людини, корупцію чи неналежне управління та загрожує цілісності політичного процесу.

СЛАБКА ЗАГАЛЬНА РОЛЬ СУДОВИХ ОРГАНІВ У ПРОЦЕСІ КОНТРОЛЮ СИСТЕМ СЕКРЕТНОСТІ

Як зазначалося вище, суди традиційно проявляли, і досі це демонструють, вельми шанобливе ставлення у своїх реакціях на дії органів, які використовують секретність, і їх так званий *"виконавчий привілей у питаннях державної таємниці"*. Таке шанобливе ставлення представників судової влади допомогло закріпити ідею про те, що питання національної безпеки є надто чутливими, щоб їх можна було розкривати навіть в судах (Сетті, 2012 р.). Гарним прикладом із історії США є знакова справа періоду холодної війни *США проти Рейнольдса*.[2]

Демократичне ставлення судів до виконавчої влади посилилося після терористичних атак 11 вересня в США, ці події часто називають 9/11 – «11 вересня». Претензії уряду щодо захисту національної безпеки у судах постійно переважали над такими принципами як підзвітність, прозорість та відкритість уряду. Багато справ у США, Великобританії, Франції та інших країнах демократичного світу, не кажучи вже про країни з нижчим рівнем демократії, демонструють вузькість поглядів на роль судових органів у перегляді виконавчих рішень, пов'язаних із безпекою. На жаль, це може зашкодити захисту фундаментальних прав, верховенству закону та забезпеченню істотних безпекових інтересів.

«*Виконавчий привілей у питаннях державної таємниці*» у США, або «*свідоцтво про недоторканність державних інтересів*» у Великобританії, або «*оборонна таємниця*» у Франції – на них дуже часто посилаються органи виконавчої влади, які засекречують інформацію, з метою уникнення попереднього судового розгляду, або щоб зробити його менш ефективним. Винятки у питаннях відкритості, засновані на твердженнях подібних до трьох вищезазначених термінів, регулярно приймаються судами, навіть якщо іноді суди нечітко заявляють, що цей привілей має реалізуватися виключно у випадках, в яких мова йде про істотні аспекти націо-

2 Доступно за посиланням: https://supreme.justia.com/cases/federal/us/345/1/case.html

нальної безпеки. Ця досить поширена судова позиція, як правило, демонструє «судову зневагу до поняття стримувань і противаг, відмову від судової відповідальності та нехтування структурною потребою у збереженні можливості позивачів у висуненні претензій проти перевищення урядом своїх повноважень» (Сетті, 2012 р., стор. 1573).

Фукс (2006 р., стор. 168) у своєму видатному дослідженні про роль судів встановила, що «зважаючи на вагомі цінності, сформовані правом на доступ до урядової інформації, це право може бути принесено у жертву лише тоді, коли існує легітимна потреба в секретності ... Ні парламенти, ні громадськість самі по собі не в змозі оскаржувати надмірну секретність. Незалежний аналіз є частиною відповідальності судової влади за забезпечення належної санкціонованої діяльності уряду». Тільки суди є досить незалежними, щоб взяти на себе роль оскаржувача надмірної секретності, але як відзначає Фукс, схоже, що вони відмовилися від цієї ролі.

Майже у всіх європейських країнах, які досліджувала Якобсен (2013 р.), суди мають повноваження перевіряти таємну інформацію, яку уряд прагне залишити секретною з міркувань національної безпеки. Однак, в деяких країнах лише окремі суди чи судді, які мають спеціальний дозвіл, можуть вивчати секретну інформацію. У Німеччині лише Федеральний адміністративний суд може перевіряти засекречену інформацію. В Іспанії, хоча й Закон про офіційну таємницю не передбачає такого доступу суддів, як це визначено для Конгресу та Сенату, Верховний суд Іспанії встановив, що він, і тільки він, має право вивчати секретну інформацію, отриману від уряду. Єдина країна, в якій суди не мають жодних повноважень безпосередньо перевіряти таємну інформацію – це Франція (Сартр і Ферле, 2010 р.). Для французького судді, здається, неможливо мати прямий доступ для опрацювання секретної інформації. Щоб обмежити дію цієї заборони, відповідно до закону 1998 року, було створено французьку *Комісію з питань секретності національної оборони*, незалежну комісію, яка може отримати доступ до таємної інформації за запитом судді, щоб оцінити доречність розсекречення такої інформації.[3] Що стосується ЄС, то більшість суддів європейських країн зазвичай покладаються на оцінку отриману від органів державної влади про те, що розкриття інформації може завдати шкоди національній безпеці (Якобсен, 2013 р.).

КРИТЕРІЇ ТА РІВНІ СЕКРЕТНОСТІ

Рівні секретності були стандартизовані таким чином, що в багатьох країнах ОЕСР можна знайти однакові системи секретності. Серед країн ОЕСР гарним прикладом того, як реалізується робота з державною таємницею, є Нова Зеландія. У Новій Зеландії офіційна інформація захищається відповідно до критеріїв, які базуються на суворому визначенні необхідності захисту офіційної інформації: інформація повинна бути захищена в тій мірі, яка відповідає суспільним інтересам та збереженню конфіденційності. Секретність такої інформації визначається спробами класифікувати її відповідно до шкоди, яка буде викликана несанкціонованим розкриттям таких даних, та визначає захисні заходи, які слід застосувати.[4] Згідно з новозеландськими керівними положеннями, секретність сама по собі не забезпечує замовчування офіційної інформації; скоріше інформація повинна розглядатися по суті, використовуючи критерії,

3 Доступно за посиланням: http://www.defense.gouv.fr/sga/le-sga-en-action/droit-et-defense/secret-defense/secret-defense

4 Закон про офіційну інформацію Нової Зеландії 1982 р.

встановлені законом.[5] Австралійська система визначення секретності цікава тим, що вона містить чіткі вказівки щодо засекречення та розкриття таємної інформації.[6]

Рівні секретності в Новій Зеландії, які відповідають широко вживаній міжнародній практиці, виглядають наступним чином, залежно від суспільного блага, що підлягає захисту:

- Дані, пов'язані з національною безпекою: розкриття інформації може поставити під загрозу безпеку, оборону чи міжнародні відносини країни, чи відносини з дружніми урядами, або
- Дані, пов'язані з урядовою політикою та/або конфіденційністю: розкриття інформації може загрожувати функціонуванню уряду або спричиняти збитки для людини.

Інформація про національну безпеку захищається на наступних рівнях за допомогою таких критеріїв:

1. **Цілком таємно**: розголошення даних може надзвичайно серйозно зашкодити національним інтересам:
    - Становити безпосередню загрозу внутрішній стабільності Нової Зеландії (НЗ) чи дружніх країн
    - Призвести до значних людських втрат
    - Завдати надзвичайної шкоди безпеці сил НЗ або союзників
    - Завдати надзвичайної шкоди оперативній ефективності сил НЗ або дружніх сил
    - Завдати надзвичайної шкоди ефективності важливих операцій з безпеки чи розвідки
    - Завдати надзвичайної шкоди відносинам з іншими урядами
    - Завдати серйозної довготривалої шкоди значущій національній інфраструктурі
2. **Таємно**: розголошення даних може завдати серйозної шкоди національним інтересам:
    - Підвищити міжнародну напругу
    - Завдати серйозної шкоди відносинам з дружніми урядами
    - Завдати серйозної шкоди безпеці сил НЗ чи дружніх сил
    - Завдати серйозної шкоди оперативній ефективності сил НЗ або дружніх сил
    - Завдати серйозної шкоди ефективності важливих операцій з безпеки чи розвідки
    - Завдати серйозної шкоди внутрішній стабільності НЗ чи дружніх країн
    - Призвести до припинення чи суттєвих порушень у діяльності значущої національної інфраструктури
3. **Конфіденційно**: розголошення даних може значним чином зашкодити національним інтересам:
    - Завдати матеріальної шкоди дипломатичним відносинам – призвести до офіційних протестів чи інших санкцій
    - Завдати шкоди оперативній ефективності сил НЗ або дружніх сил
    - Завдати шкоди безпеці сил НЗ чи дружніх сил
    - Завдати шкоди ефективності важливих операцій з безпеки чи розвідки
    - Завдати шкоди внутрішній стабільності НЗ чи дружніх країн
    - Призвести до порушень у діяльності значущої національної інфраструктури

5 Керівні положення Нової Зеландії щодо захисту офіційної інформації. Доступно за посиланням: https://protectivesecurity.govt.nz/home/information-security-management-protocol/new-zealand-government-security-classification-system/

6 Австралія (2014 р.): Керівні принципи управління безпекою інформації. Австралійська урядова система секретності. Доступно за посиланням: https://www.protectivesecurity.gov.au/informationsecurity/Documents/AustralianGovernmentclassificationsystem.pdf

4. **Для службового (обмеженого) використання**: розголошення даних може мати негативний вплив на національні інтереси:
    - Негативно вплинути на дипломатичні відносини
    - Перешкоджати оперативній ефективності сил НЗ або дружніх сил
    - Перешкоджати безпеці сил НЗ чи дружніх сил
    - Негативно вплинути на внутрішню стабільність НЗ чи дружніх країн
    - Негативно вплинути на економічне благополуччя НЗ чи дружніх країн

Урядова політика та конфіденційні дані приватних осіб захищаються на наступних рівнях за допомогою таких критеріїв:

1. **Закриті дані з обмеженим доступом**: їх розкриття може завдати шкоди інтересам уряду або загрожувати громадянам:
    - Загрожувати безпеці будь-якої людини
    - Завдати серйозної шкоди економіці НЗ
    - Перешкоджати урядовим переговорам
2. **Дані на умовах конфіденційності**: їх розкриття може завдавати шкоди правопорядку, перешкоджати діяльності уряду, негативно впливати на приватність громадян:
    - Перешкоджати дотриманню законів
    - Мати несприятливий вплив на приватність фізичних осіб
    - Завдати шкоди комерційній інформації громадян
    - Завдати шкоди зобов'язанням щодо конфіденційності
    - Завдати шкоди заходам, спрямованим на захист здоров'я чи безпеки населення
    - Завдати шкоди економічним інтересам НЗ
    - Завдати шкоди заходам, що запобігають або зменшують матеріальні збитки суспільства
    - Порушувати конституційні конвенції
    - Перешкоджати ефективному веденню державних справ
    - Порушувати юридичні професійні привілеї
    - Перешкоджати комерційній діяльності уряду
    - Розголошення або використання інформації для неналежного отримання вигоди чи інших переваг

Як вже зазначалося, подібні маркування та критерії секретності інформації можуть бути знайдені у багатьох країнах ОЕСР. Навіть у Туреччині, де правила таємності не є загальнодоступними, відомі певні рівні секретності (Якобсен, 2013 р.). Швеція була єдиною країною, яка надала відповіді в ході дослідження, проведеного Якобсен (2013 р.), де закон не визначає рівні секретності інформації, оскільки у Швеції секретність виконує суто адміністративну функцію.

Інші аспекти, пов'язані з секретністю інформації (наприклад, процедури секретності, вимоги до маркування, орган секретності, зобов'язання щодо надання обґрунтування секретності, відповідальність за неналежну секретність, органи нагляду тощо), значним чином різняться в країнах Європи (див. дослідження Якобсен 2013 р. та Трансперенсі Інтернешнл Великобританія, 2014 р.).

КРИТЕРІЇ РОЗСЕКРЕЧЕННЯ

У європейських країнах розсекречення інформації визначається трьома основними критеріями: часові межі, подія-тригер для цього або обов'язковий період перегляду даних. Основна мета в цьому аспекті – запобігти безстроковому засекреченню інформації. Однак, нерідко можна зустріти країни, де в законодавстві чи в адміністративних практиках не передбачено критеріїв

розсекречення. Середнє обмеження строку секретності, згідно з розрахунками Якобсен (2013 р.), у європейських країнах становить 30 років, при цьому специфічні часові рамки варіюються від 10 років у Нідерландах до 100 років у Румунії і до невизначеного терміну в Іспанії та Туреччині. Останнє, однак, є досить винятковим у Європі.

Найпоширеніший термін обов'язкового перегляду секретної інформації складає 5 років. У Швеції не існує попередньо встановленого обов'язкового перегляду, але збереження таємності будь-якої інформації повинно бути переглянуте щоразу, коли подається запит про розкриття інформації. Практика автоматичного розсекречення (тригерної події) відрізняється в різних країнах, але в більшості з них головним аспектом є дискреційне рішення уряду про розкриття різних класів інформації. Таке рішення також може бути прийняте внаслідок виконання Закону про доступ до інформації, процедури якого реалізуються громадянами чи громадськими організаціями.

ЗАСТОСУВАННЯ ТЕСТІВ ДЛЯ УТРИМАННЯ КОНТРОЛЮ НАД СЕКРЕТНІСТЮ: ТЕСТ НА МОЖЛИВУ ШКОДУ ТА ТЕСТ ЗБАЛАНСОВАНОСТІ СУСПІЛЬНОГО ІНТЕРЕСУ

За даними *Right2INFO.org* – неурядової організації, яка пропагує належне законодавство та практики, так званий тест на визначення можливої шкоди (Harm Test) та тест збалансованості суспільного інтересу (Public Interest Test) витікають з вимоги відносно того, що обмеження права на доступ до інформації повинні бути пропорційними та дійсно необхідними.[7] OECP-SIGMA (2010 р.) пропонують широкий і ретельний концептуальний підхід до понять, що стоять за цими тестами, вихо-

7 Доступно за посиланням: http://www.right2info.org/exceptions-to-access/harm-and-public-interest-test

дячи із розрізнення абсолютних і відносних обмежень у питаннях доступу до інформації. До числа перших, як правило, відносяться ті, що стосуються оборони та національної безпеки.

ТЕСТ НА МОЖЛИВУ ШКОДУ

Відповідно до тесту на визначення можливої шкоди, державний орган повинен продемонструвати, що оприлюднення певної інформації може загрожувати і зашкодити захищеним інтересам, а тому розкриття не повинно відбутися. Тест на визначення шкоди вимагає, щоб держава підтвердила ризик істотної очевидної шкоди даному легітимному інтересу. Має бути продемонстровано те, що обмеження стосується визначеного легітимного інтересу і що розголошення може завдати істотної шкоди цьому інтересу. Така шкода повинна бути досить конкретною, точно визначеною, неминучою та прямою, а не спекулятивною чи сумнівною.

ТЕСТ ЗБАЛАНСОВАНОСТІ СУСПІЛЬНОГО ІНТЕРЕСУ

Тест збалансованості суспільного інтересу стосується пропорційності. Для цього вимагається оцінка балансу, тобто шкода від оприлюднення інформації оцінюється відносно суспільного інтересу, який задовольняється через розкриття цієї інформації. Умови, за яких явний і конкретний суспільний інтерес може переважати над потребою у таємності/конфіденційності, повинні бути визначені національним законодавством. У відповідності до багатьох національних моделей застосування секретності, включаючи міжамериканську та африканську, суспільний інтерес стає обов'язковим і переважає над іншими інтересами, коли мова йде про інформацію, яка стосується порушень прав людини чи злочинів проти людства. Тест на збалансованість суспіль-

ного інтересу вимагає, щоб державний чи контролюючий орган зважили шкоду, яку розкриття інформації може заподіяти певному захищеному інтересу у порівнянні із суспільним інтересом, який задовольняється розкриттям цієї інформації.

Визначення того, що становить суспільний інтерес, варіюється в різних країнах і часто вимагає оцінки в кожному конкретному випадку. Загалом, суспільні інтереси, що сприяють розкриттю інформації, зазвичай стосуються питань громадського обговорення, участі громадськості у політичних дебатах, підзвітності за розподіл та витрату державних коштів, питань суспільної безпеки. Питання, пов'язані з безпекою суспільства і довкілля, з суттєвими загрозами здоров'ю та серйозними порушеннями прав людини, як правило, вважаються такими, що виправдовують обов'язковий пріоритет суспільного інтересу в розкритті такої інформації.

Деякі країни видали керівні положення щодо адміністративних процедур у діяльності державних службовців. Наприклад, в Новому Південному Уельсі, Австралія, державні службовці повинні застосовувати тест збалансованості суспільного інтересу, коли приймаються рішення щодо оприлюднення інформації. Це означає, що вони повинні зважувати фактори на користь розкриття інформації відносно факторів суспільного інтересу проти розкриття.[8] Відповідно до цих рекомендацій, тест збалансованості суспільного інтересу включає три кроки:

1. Визначити суспільний інтерес на користь розкриття інформації.
2. Визначити суспільний інтерес проти розкриття інформації.
3. Зважити співвідношення суспільного інтересу за і проти розкриття інформації та визначити баланс між цими інтересами.

Незважаючи на чітку позицію австралійського законодавства на користь оприлюднення інформації, провінційні закони про доступ до інформації визначають ряд ситуацій, коли презумпція полягає в утриманні інформації та захисті секретності. Найбільш значущою є інформація, яка підпадає під дію закону про переважаючу секретність – 26 спеціально визначених законних актів. Це відповідає загальній тенденції, поширеній у багатьох країнах ОЕСР, за якої закони про свободу інформації (FOIA) на практиці перестали бути актуальними на перетині з традиційним законодавством, що стосується державної таємниці. Державна таємниця постійно знаходиться поза сферою дії законодавства про свободу доступу до інформації. Крім того, в більшості країн, як правило, докладається недостатньо зусиль для гармонізації традиційного законодавства про державну безпеку з новими законами щодо свободи доступу до публічної інформації.

Той факт, що багато законів про свободу інформації залишили практично недоторканими питання секретності, пов'язаної з національною безпекою, означає, що законодавство та звернення до судів поки що виявилися недостатньо ефективними інструментами для зменшення загальної тенденції щодо зростання рівня конфіденційності та таємності в роботі агенцій у сфері безпеки та розвідки. Такі установи з традиційним та часто непрозорим способом роботи з конфіденційною інформацією в основному не підпадають під дію законів про свободу інформації, незважаючи на поширену міжнародну тенденцію на користь більшої державної прозорості та запиту громадянського суспільства щодо реалізації

8 Доступно за посиланням: http://www.ipc.nsw.gov.au/fact-sheet-what-public-interest-test

його «права знати».

Це вказує на той факт, що питання введення в дію загального законодавства, яке ефективно врівноважує секретність та відкритість, є складним, як концептуально, так і на практиці. Одна з причин цього полягає в тому, що державні органи чи агенції, які найчастіше засекречують інформацію, як правило, мають зовсім інші цілі та мотивацію у своїй роботі та практиках. Це сприяє розвитку різних адміністративних культур, пов'язаних з безпекою. Наприклад, військові органи, як правило, зосереджуються насамперед на безпеці технологій озброєння та оперативних планів, розвідувальні органи – на захисті джерел інформації та методів роботи, дипломати переймаються міжнародними наслідками засекречення та розкриття дипломатичної інформації, поліція прагне захистити своїх інформаторів та оперативні плани. Це призводить до того, що кожне відомство чи установа розробляють власні керівні норми, процедури та протоколи, які, як правило, залишаються чинними роками, не підлягаючи перегляду та серйозному аналізу. Крім того зрозуміло, що всередині агентств, на зразок перелічених вище, співробітники, як правило, віддають перевагу грі на безпечній території задля уникнення небажаних проблем, що часто призводить до проявів надмірної секретності (Афтергуд, 2009 р.).

Як результат, поінформовані спостерігачі та практикуючи спеціалісти вважають, що, навіть якщо засекречення здійснюється відповідним органом, то відомство з повноваженнями щодо розсекречення повинно знаходитися за межами цього органу. Це найкращий спосіб звести нанівець власні інтереси цього органу та очистити його від зловживань надмірною таємністю (Афтергуд, 2009 р., стор. 412). Деякі успішні спроби досягти цього були здійснені у США, наприклад, через *Міжвідомчу апеляційну комісію з питань присвоєння секретності* (ISCAP)[9] та *фундаментальний аналіз політики секретності* (FCPR).[10] Комісія з питань секретності національної оборони (CSDN) у Франції є ще одним прикладом (див. вище). Американський досвід, описаний Афтергуд (2009 р.), по суті показує, що «якщо відомство не може успішно пояснити та переконати вище керівництво або колегію з інших відомств, чому саме національна безпека вимагає секретності певного документу, тоді є підстави сумніватися у необхідності його засекречення взагалі».

ВИСНОВКИ

1. Законодавство, що регулює таємність інформації в галузі безпеки та оборони, є дуже потрібним і воно має бути максимально точним. Таке законодавство повинно передбачати критерії засекречення та розкриття інформації, зважаючи на те, що таке законодавство по своїй суті буде загальним, а отже, зазначені у ньому критерії також будуть загальними. Законодавство, регулююче конфіденційність, яке в багатьох країнах передує законодавству про вільний доступ до інформації, повинно бути узгоджене з останнім, з метою уникнення невідповідностей у національному правовому порядку.
2. Поряд із надійною правовою базою, необхідно забезпечити свідоме та вміле управління на рівні агенцій для застосовування правових критеріїв секретності у раціональний і розсудливий спосіб, щоб максимально сприяти посиленню демо-

9 Доступно за посиланням: https://www.archives.gov/declassification/iscap

10 Доступно за посиланням: https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/ODNI%20FY2017%20FCGR.pdf Див. також новаторський аналіз Міністерства енергетики 1994 р. Доступно за адресою: https://www.osti.gov/opennet/forms.jsp?formurl=od/fcprsum.html

кратичних цінностей та принципу суспільної прозорості. Свідоме розуміння необхідності балансування різних факторів повинно стати частиною організаційної культури. Керівники відповідних відомств повинні сприймати це як своє завдання – досягнення збалансованого підходу між легітимною конфіденційністю та легітимною прозорістю.

3. Зменшення невиправданих зловживань таємністю і досягнення балансу між правом суспільства знати та імперативами національної безпеки, а також іншими законними причинами секретності – є складним завданням. Перетворення культури таємності на культуру прозорості у сфері оборони навряд чи є можливим у найближчому майбутньому у більшості країн ЄС та ОЕСР.[11]
4. Від працівників і представників сфери безпеки та оборони очікується лояльність, повага до встановлених процедур та обачність у цьому питанні. Ці якості є справді обов'язковими, але, тим не менш, слід заохочувати і нові ідеї та новаторство, навіть якщо їхня роль у процесі змін може виявитися незначною. Крім того, необхідно зробити критичний аналіз того, як досягти оптимального балансу між легітимною секретністю, з одного боку, і легітимним доступом до інформації з іншого.
5. Персонал, відповідальний за виконання законів у сфері секретності або політик з питань конфіденційності, повинен мати спеціальну підготовку, щоб бути здатним узгодити демократичну потребу у відкритості та прозорість уряду, і в той же час чітко розуміти, що, в межах законодавства, має залишатися прихованим від очей громадськості. Нерозбірлива відкритість не є альтернативою нерегульованій секретності. Висока якість роботи та компетентність персоналу, який працює у сфері безпеки та оборони, є надважливими, оскільки це має прямі наслідки для демократичного суспільства та відносин між органами безпеки та громадськістю.
6. Незалежна установа, наприклад, міжвідомча комісія з питань розсекречення, яка працює за межами сфери впливу найважливіших органів, що мають відношення до секретності, таких як військові, розвідувальні та поліцейські відомства, повинна мати повноваження переглядати та періодично розсекречувати інформацію, яка утримується у таємниці певними органами. Судові органи загалом проявили занадто поблажливе ставлення до виконавчого привілею в питаннях державної таємниці, і наразі є дуже мало причин для того, щоб очікувати змін у цьому плані.
7. Здається, нарешті з'являється гарний досвід, який демонструє зменшення дискреційних практик порівняно з тими, які характеризують традиційні практики таємності: рішення щодо засекречення та розсекречення інформації мають бути прийняті не окремою особою, а незалежним комітетом чи комісією, спроможними діяти неупереджено у власних судженнях щодо необхідності засекречення чи розкриття певної інформації – повністю або частково. Такий спеціалізований підрозділ повинен керуватися встановленими законодавством критеріями для визначення шкоди та проводити перевірку і тести для балансування всіх факторів. Членство в такому незалежному комітеті чи комісії має бути обмежене, наприклад, вони можуть складатися з 5-7 членів і включати експертів у сфері безпеки від виконавчої влади, парламенту, депутатів, омбудсмена та представників судової влади.

11 Навіть якщо здається, що Румунії вдалося цього досягти (Матей, 2007 р.).

ВИКОРИСТАНІ ДЖЕРЕЛА

Aftergood, Steven (2009):"*Reducing Government Secrecy: Finding What Works*," в Yale Law & Policy Review, Видання 27, №2 (весна, 2009 р.), стор. 399-416. Доступно за посиланням: https://www.jstor.org/stable/40239716?seq=1#page_scan_tab_contents

Fenster, Mark (2010): *Seeing the State: Transparency as Metaphor*, в Administrative Law Review, стор. 617-672, доступно за посиланням: http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1571&context=facultypub

Fuchs, Meredith (2006): *Judging Secrets: The Role Courts Should Play в Preventing Unnecessary Secrecy*, in Administrative Law Review, видання 58, № 1, зима, 2006 р., стор. 131-176..

Jacobsen, Amanda L. (2013): *National Security and the Right to Information in Europe*. Доступно за посиланням: http://www.right2info.org/resources/publications/national-security-page/national-security-expert-papers/jacobsen_nat-sec-and-rti-in-europe

Matei, Florina Cristiana (2007): *Reconciling Intelligence Effectiveness and Transparency: The Case of Romania*, в Strategic Insights, видання VI, випуск 3 (травень, 2007 р.). Доступно за посиланням: https://calhoun.nps.edu/bitstream/handle/10945/11297/mateiMay07.pdf?sequence=1

OECP (2010), "*The Right to Open Public Administrations in Europe: Emerging Legal Standards*", документи SIGMA, №46, видавництво OECP, Париж. Доступно за посиланням: http://dx.doi.org/10.1787/5km4g0zfqt27-en

Riese, Dorothée (2014): *Secrecy and Transparency*, документ представлено на конференції Європейського консорціуму політичних досліджень у Глазго, 3-6 вересня 2014 р. Доступно за посиланням: https://ecpr.eu/Filestore/PaperProposal/2cedead9-5191-42de-ae36-7d320a28a304.pdf

Sartre, Patrice & Ferlet, Philippe (2010): *Le secret de défense en France* in Revue Études 2010/2, том 412, лютий 2010 р., стор. 165-175. Доступно за посиланням: https://www.cairn.info/revue-etudes-2010-2-page-165.htm

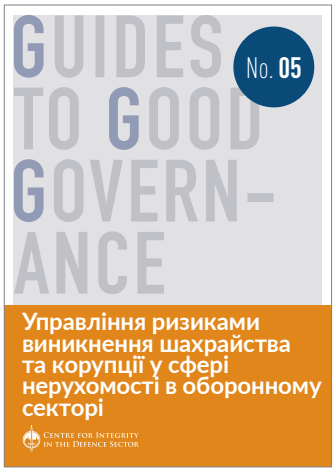
Sauvé, Jean-Marc (2011): *Culture du secret contre transparence sans limite : quel équilibre pour garantir l'intérêt général ? Transparence, valeurs de l'action publique et intérêt général*, виступ в Національній Асамблеї, вівторок, 5 липня 2011 р., симпозіум організований Трансперенсі Інтернешнл Франція. Доступно за посиланням: http://www.conseil-etat.fr/content/download/2597/7819/version/1/file/discours-transparence-international.pdf

Setty, Sudha (2012): *The Rise of National Security Secrets*, in Connecticut Law Review, видання 44, №5, липень 2012, стор. 1563-1582.

Трансперенсі Інтернешнл Великобританія (2014 р.): Секретна інформація: огляд 15 країн. Доступно за посиланням: http://ti-defence.org/wp-content/uploads/2016/03/140911-Classified-Information.pdf

Серія посібників з належного врядування


GUIDES TO GOOD GOVERN-ANCE
No. 04
Доступ до інформації та обмеження у відкритості діяльності державних органів для суспільства
Centre for Integrity in the Defence Sector


GUIDES TO GOOD GOVERN-ANCE
No. 05
Управління ризиками виникнення шахрайства та корупції у сфері нерухомості в оборонному секторі
Centre for Integrity in the Defence Sector

Посібники з належного врядування - це серія невеликих буклетів, у кожному з яких обговорюється конкретна тема, що має важливе значення для належного управління у сфері оборони. Довідники призначені для осіб, зацікавлених у тому, щоб більше дізнатися про одну чи декілька тем, що безпосередньо стосуються належного управління в оборонному секторі, або в державному секторі загалом. Вони також можуть використовуватися в освітніх цілях.

Опубліковано: Центр з розбудови доброчесності в оборонному секторі
Дизайн: www.melkeveien.no
Друк: Норвезька державна організація з безпеки та обслуговування
Травень 2018 р. Тираж 500 прим.

Centre for Integrity in the Defence Sector
www.cids.no

NATO OTAN

Переклад оригінальної англійської версії на українську мову був люб'язно наданий Організацією Північноатлантичного договору