ЗМІСТ

СВіП в Україні

СВіП у світі

СВіП в Україні

ЗВЕРНЕННЯ ЛУГАНСЬКОГО ОБЛАСНОГО ВІДДІЛЕННЯ КВУ ДО СТАХАНОВСЬКОГО МІСЬКОГО ГОЛОВИ

Комітет виборців України
Луганське обласне відділення
вул. Леніна, 14, оф. 26, м. Сєвєродонецьк,
Луганської області, 93404,
тел/факс (+380)645242196,
e-mail: <cvuluhansk@sdtcom.lg.ua >,
сайт: <http://cvu-lg.narod.ru>
№ 46 Стаханівському міському голові
від 11.07.2011 р. Борисову Ю.В.

ЗВЕРНЕННЯ

стосовно рішення виконкому Стаханівської міської ради від 30 червня 2011 р. № 356

Вважаємо, що зазначене рішення виконкому Стаханівської міської ради є протиправним і обмежує право громадськості, у тому числі нашої організації на доступ до публічної інформації.

Відповідно до статті 34 Конституції України право збирати та поширювати інформацію може бути обмежено законом.

Згідно частини другої статті 6 Закону України «Про доступ до публічної інформації» (далі — Закону) обмеження доступу до інформації здійснюється відповідно до закону.

Тож рішенням органу місцевого самоврядування, його виконавчого органу, виконавчого органу державної влади не можуть бути встановлені обмеження щодо доступу до інформації, які не передбачені чинними законами.

До інформації з обмеженим доступом, розпорядником якої суб'єкт владних повноважень (далі — СВП), відповідно до частини першої статті 6 Закону відносяться:

— конфіденційна інформація — надана СВП фізичною чи юридичною особою, яка встановила обмеження щодо її поширення. Відповідно до статті 11 Закону України «Про інформацію» до конфіденційної інформації, яка не підлягає поширенню, належать також дані про національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження особи;
— таємна інформація — інформація, що містить державну, лікарську, банківську, комерційну, професійну таємницю, таємницю голосування та усиновлення, іншу передбачену законом таємницю, за незаконне поширення такої інформації передбачена кримінальна відповідальність;
— службова інформація.

На нашу думку, до переліку службової інформації не можна відносити інформацію, яка відповідно до Закону є конфіденційною чи таємною, оскільки за порушення обмежень поширення цих видів інформації наступають різні правові наслідки.

Відповідно до частини першої статті 9 Закону до службової інформації відносяться відомості:

1) що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Зазначена норма містить вичерпний перелік підстав для віднесення інформації до службової. Проте за правозастосувальною практикою останніх місяців СПД включають до складу службової інформації також відомості, поширення яких обмежено спеціальними законами, і які не відносяться до конфіденціальної та таємної інформації. Наприклад, інформацію про неповнолітніх правопорушників тощо.

Частиною третьою статті 6 Закону передбачено, що органи державної влади, органи місцевого самоврядування, інші суб'єкти владних повноважень складають перелік відомостей, що становлять службову інформацію. Це є одним із складних питань при впровадженні Закону, оскільки нормативні чи методичні документи загального призначення щодо змісту таких пе-

реліків не розроблені, і підходи різних відомств до їх складання суттєво різняться. Більш того, є чинною Постанова Кабміну від 27 листопада 1998 р. № 1893 щодо конфіденційної інформації, яка суперечить вимогам Закону.

Тож не дивно, що станом на 10 липня вимогу закону про складання переліків відомостей, що становлять службову інформацію, в Луганській області виконали тільки Луганська обласна рада, Новопсковська райдержадміністрація та виконком Стаханівської міської ради[1]. При цьому тільки стаханівський перелік має змістовний, а не формальний характер.

Тож сам факт прийняття виконкомом Стаханівської міської ради рішення від 30 червня 2011 р. № 356 «Про затвердження Переліку відомостей, що становлять службову інформацію» (далі — Перелік), варто вітати. Зазначене рішення оприлюднено на офіційному сайті Стаханівської міської ради http://stakhanov.net.ua/_dr/5/573_356.doc.

Але що стосується змісту Переліку, то він викликав численні заперечення інститутів громадянського суспільства Луганської області.

За нашою оцінкою, ці заперечення цілком справедливі. Бо зазначеним рішенням вводяться обмеження в доступі до таких видів публічної інформації, які чинними законами до інформації з обмеженим доступом не віднесені, і стають такими виключно в наслідок прийняття рішення виконкому. На таких підставах змінюється статус інформації в 26 пунктах з 85, що включає Перелік. Наразі це стосується пунктів 2 (до службової віднесена конфіденційна інформація), 3 (до службової віднесена інформація, що завдає шкоди правосуддю, в дійсності така має вилучатися), 4 (до службової віднесена інформація, яка завдає шкоди честі, гідності та репутації осіб, в дійсності така має вилучатися), 7 (до службової віднесена аналітична інформація), 10 (протоколи сесій), 13 (документи про нагородження), п. 14 (відомості з баз даних), п. 18 (декларації про доходи посадових осіб), п. 22 (інформація про особисті дані — це конфіденційна, а не службова інформація), п. 26 (посадові інструкції працівників виконкому), п. 27 (відомості зі списків кадрового резерву на посади виконавчих органів міської ради), п. 28 (обмеження, начебто передбачені статтями 11, 17 Закону України «Про регулювання містобудівної діяльності», яких в дійсності в цих статтях немає), п. 29 (відомості з генерального плану міста), п. 30 (інформація з планово-картографічних матеріалів), п. 31 (інформація з каталогів координат та висот пунктів геодезичної мережі), п. 32 (відомості з плану міста, виконані на топографічних матеріалах (картографічний матеріал) у масштабі: 1:10000, створених у державній системі координат УСК-2000, або СК-42, 1:5000, 1:2000, 1:500), п. 33 (відомості з робочих проектів на будівництво і реконструкцію об'єктів), п. 34 (відомості з планів, узгоджених зі службами міста, що експлуатують підземні комунікації (міськгаз, водоканал, електромережа, зв'язок і т.д.), п. 35 (відомості з журналів виконаних будівельних робіт), п. 36 (відомості з виконавчої технічної документації (акти на приховані роботи, виконавчі схеми, протоколи випробувань, акти приймання окремих вузлів і робіт), п. 37 (відомості з актів виконаних робіт форми КБ-2в, КБ-3, договірні ціни, календарні плани виконання робіт, графіки фінансування робіт), п. 38 (відомості з титулів на проектні та будівельні роботи), п. 39 (відомості з податкових розрахунків про суми доходів і використання коштів неприбутковими установами), п. 40 (відомості з кошторисної документація на будівництво, реконструкцію та ремонт об'єктів), п. 41 (відомості з рішень виконкому про затвердження проектно-кошторисної документації), п. 42 (відомості з договорів підряду на проектні, вишукувальні, будівельні роботи, реконструкцію — та капітальний ремонт об'єктів), п. 43 (відомості з договорів на придбання обладнання для об'єктів будівництва), п. 44 (відомості з тендерної документації).

Більш того, 13 пунктами зазначеного рішення обмежено доступ до такої інформації, доступ до якої згідно законів України не може бути обмежений.

Наприклад, пунктом 1 Переліку до інформації з обмеженим доступом віднесено відомості з документів, якими регламентується порядок роботи виконавчих органів міської ради. Але це суперечить статті 15 Закону, якою передбачено обов'язкове оприлюднення інформації про діяльність суб'єктів владних повноважень, прізвище, ім'я та по батькові, службові номери засобів зв'язку, адреси електронної пошти керівника органу та його заступників, також керівників структурних та регіональних підрозділів, основні функції структурних та регіональних підрозділів, розклад роботи, перелік і службові номери засобів зв'язку підприємств, установ та організацій, що належать до сфери їх управління, та їх керівників, тощо.

Пунктом 5 Переліку обмежено доступ до документів, що містять інформацію про фізичних та юридичних осіб, з якими Стахановська міська рада чи її виконавчі органи перебувають у правовідносинах. Пунктом 15 — відомості щодо штатно-кошторисної дисципліни та інвентаризації. Пункту 19 — відомості щодо ревізій та перевірок фінансової діяльності. Пунктом 20 — зведені відомості щодо комп'ютерних програм у виконавчих органах міської ради. Пунктом 39 Переліку — відомості з податкових розрахунків про суми доходів і використання коштів неприбутковими установами. Пунктом 44 — відомості з тендерної документації. Пунктом 81 — відомості (за окремими показниками) про потребу в асигнуваннях та фактичні фінансові витрати на мобілізаційну підготовку виконкому міської ради. Усі ці перелічені обмеження суперечать частині п'ятій статті 6 Закону, згідно якої не може бути обмежено доступ до інформації про розпорядження бюджетними коштами, володіння, користування чи розпорядження державним, комунальним майном, у тому числі до копій відповідних документів, умови отримання цих коштів чи майна, у тому числі прізвища, імена, по батькові фізичних осіб та найменування юридичних осіб, які отримали ці кошти або майно.

Пунктом 6 Переліку обмежено доступ до судових процесуальних документів (рішення, вироки, ухвали, постанови тощо), надісланих до відома чи виконання. Це суперечить частині першій статті 11 Закону України «Про судоустрій та статус суддів», згідно якої кожен, хто не є стороною у справі, має право на вільний доступ до судового рішення.

Пунктом 12 обмежено доступ до відомостей особистого характеру про депутатів Стахановської міської ради та керівного складу органів самоорганізації населення; посадових осіб виконавчих органів міської ради. Це суперечить частині шостій статті 6 Закону, закону про вибори депутатів місцевих рад тощо.

Пунктом 29 Переліку обмежено доступ до відомостей з генерального плану міста (графічна частина та пояснювальна записка), а пунктом 30 — до інформації з планово-картографічних матеріалів. Це суперечить частині одинадцятій статті 17 Закону України «Про регулювання містобудівної діяльності».

Пункт 58 Переліку, яким до службової інформації відносяться відомості про хімічно небезпечні об'єкти господарської діяльності I–Ш ступенів хімічної небезпеки (дислокація, види і кількість небезпечних хімічних речовин (НХР), кількість працюючих, план території, місця розташування сховищ НХР та інші спеціальні дані) — суперечить частині четвертій статті 15 Закону, згідно якої невідкладному оприлюдненню підлягає будь-яка інформація про факти, що загрожують життю, здоров'ю та/або майну осіб, і про заходи, які застосовуються у зв'язку з цим.

Нарешті, обмеження доступу до інформації, введені пунктами 10 та 11 Переліку, хоча формально й не порушують норми законодавства, проте обмеження в доступі до цієї інформації (протоколи сесій, засідань постійних комісій міської ради та виконкому, документація до рішень з землеустрою щодо права власності (оренди) на земельні ділянки є невиправданими у світлі частини другої статті 6 Закону.

Тож вважаємо, що зазначене рішення виконкому Стаханівської міської ради від 30 червня 2011 р. № 356 «Про затвердження Переліку відомостей, що становлять службову інформацію» є протиправним і обмежує право громадськості, у тому числі нашої організації щодо доступу до публічної інформації, у зв'язку з чим пропонуємо його скасувати — в порядку досудового вирішення спору.

Наша організація готова надати конкретну допомогу у складанні нової редакції Переліку, у тому числі через участь у робочій групі чи шляхом надання пропозицій та експертних висновків.

Олексій Свєтіков,
голова правління ЛОВ ВГО КВУ

КОМЕНТАР ДО ЗВЕРНЕННЯ ДМИТРА КОТЛЯРА

Це положення (ч. 3 ст. 9) Закону про доступ до публічної інформації є дійсно проблематичним. У ньому йдеться про «перелік відомостей», а не категорій відомостей. При цьому «відомостей, що становлять службову інформацію», тобто таких, які вже було віднесено до службової інформації, а не тих, що може бути віднесено в майбутньому. Це суперечить ч. 2 ст.6 та самій статті 9 Закону, в яких кілька разів наголошується, що обмеження доступу здійс-

нюється тільки після застосування трискладового тесту, тобто не можна наперед визначати, які відомості є службовою інформацією, це повинно визначатися в кожному конкретному випадку з урахуванням обставин ситуації та із застосуванням вимог ч. 2 ст. 6 (тобто трискладового тесту). Отже, для того, щоб не було суперечності з цим принциповим положенням Закону, у ч. 3 ст. 9 мало б йтися або про перелік конкретних документів, яким вже надано гриф ДСК, або про перелік категорій відомостей, які може бути віднесено до службової інформації для деталізації положень ч. 1 ст. 9. Саме за одним з цих варіантів і слід тлумачити цю норму, інші варіанти будуть суперечити ч. 2 ст. 6.

Для того, щоб реалізувати цю норму на практиці, я бачу два варіанти.

1. Слід уважно подивитися на відмінності між пунктами 1 і 2 частини першої статті 9 Закону про доступ. У пункті 1 йдеться про певні документи, які можуть містити службову інформацію («документи, які становлять внутрівідомчу кореспонденцію...»). Тому за цим пунктом визначати «перелік відомостей» немає сенсу, бо немає значення, які відомості, наголос робиться на тому, в якому документі вони фіксуються і яким може надаватися гриф ДСК (з урахуванням ч. 2 ст. 6 звичайно). Тобто переліку категорій відомостей за цим пунктом не може бути, бо тоді треба окреслювати зміст всіх питань, з якими має справу розпорядник і які можуть потрапити у його внутрівідомчу кореспонденцію. За цим пунктом ч. 1 ст. 9 Закону може бути складено тільки перелік документів з грифом ДСК.

Тоді як у пункті 2 частини першої статті 9 йдеться про сфери, в яких збирається інформація, тобто визначення робиться через зміст інформації, і тут наявність переліку категорій відомостей може мати сенс і можна навіть обґрунтувати необхідність визначення таких категорій і складання відповідного переліку.

Спробуємо осягнути, що могло матися на увазі в ч. 3 ст. 9. Відомо, що існували (і ще мало де скасовані) «переліки відомостей, що становлять конфіденційну інформацію, яка є власністю держави», які складалися на рівні кожного органу. У цих переліках окреслювалися категорії інформації, що є конфіденційною в розумінні старого Закону про інформацію, за сферами, у тому числі у сфері оборони. Хоча самі ці акти називалися «переліками відомостей», але по суті йшлося про переліки категорій відомостей. Була також практика закриття доступу до самих таких переліків грифом ДСК. І норма ч. 3 ст. 9, імовірно, як раз і була спрямована на те, щоб заборонити обмеження доступу до таких переліків. Звідси і саме формулювання «переліки відомостей», яке перейшло в Закон про доступ до публічної інформації.

Тепер: чи буде порушенням Закону про доступ складання переліку категорій інформації для деталізації пункту 2 частини першої статті 9 (якщо не брати до уваги формулювання ч. 3 ст. 9 буквально)? На мою думку, ні, якщо бути йтися про переліки категорій відомостей, які може бути віднесено до службової інформації, а не про опис відомостей, які наперед віднесено до такої інформації.

Ці три сфери («зібрана у процесі оперативно-розшукової діяльності», «зібрана у процесі контррозвідувальної діяльності» і «у сфері оборони») є достатньо широкими і нечіткими. Тому складання переліку того, які саме відомості входять до цих сфер, необхідне для їх чіткого визначення. І тут вступає в дію заборона ч. 3 ст. 9 — ці переліки є відкритими і підлягають громадському контролю за тим, чи є вони обґрунтованими. Тобто наявність такого переліку навпаки може запобігати підведенню під пункт 2 необмеженого кола інформації. Тим більше, що це стосується таких закритих сфер, як правоохоронна діяльність, розвідка, оборона, де є серйозний ризик того, що під цю категорію (пункт 2 ч. 1) будуть підводити все, що заманеться.

Отже за цією логікою тлумачення:

— «переліки відомостей, що становлять службову інформацію» повинні затверджуватися суб'єктами владних повноважень, які збирають інформацію в процесі оперативно-розшукової діяльності чи контррозвідувальної діяльності, або які володіють інформацією у сфері оборони;
— такі переліки містять категорії відомостей (у зазначених сферах), що можуть бути віднесені в конкретних ситуаціях до службової інформації, за умови виконання вимог ч.2 ст.6 Закону;
— такі переліки є відкритою інформацією;
— переліки відомостей не складаються для інформації, що міститься в документах, визначених в п. 1 ч. 1 ст. 9.

2. Вищеописана схема не вирішує проблему з формулюванням частини третьої ст. 9, в якій

йдеться одночасно про перелік «відомостей», що «становлять» службову інформацію, що є внутрішньо суперечливим, оскільки в п. 1 ч. 1 ст. 9 йдеться про категорії документів, не «відомостей».

Тому другий варіант вирішення цієї проблеми такий: вважати, що йдеться про перелік конкретних документів (назви, реквізити), яким вже було надано гриф ДСК, і що це є додаткова гарантія відкритості такого переліку. Але тут виникає проблема з поясненням, навіщо потрібна ця норма (ч. 3 ст. 9), якщо цей перелік вже охоплюється системою обліку, яка також є відкритою за ст. 18 Закону.

Підсумок. Практика застосування закону вже пішла шляхом перезатвердження «переліків відомостей» і включення до них необмеженого кола питань. Цій практиці буде сприяти і тенденція до автоматичного зрівняння «конфіденційної інформації, що є власністю держави» у старому Законі про інформацію із «службовою інформацією» у Законі про доступ і переведення всіх процедур, які існували раніше для ДСК на службову інформацію за новим законом.

Тому хоча другий варіант (перелік документів з грифом ДСК) є простішим для пояснення, перший варіант (перелік категорій відомостей, які може бути віднесено до службової інформації з дотримання вимог ч. 2 ст. 6) дозволяє спрямувати практику в правильному напрямі. Слід, правда, визнати, що обидва варіанти не є бездоганними, оскільки в обох випадках приходиться «творчо» тлумачити формулювання, вжиті в ч. 3 ст. 9 Закону.

У будь-якому разі, звичайно, безпідставним є включення до переліку відомостей, які становлять службову інформацію, інших видів інформації з обмеженим доступом (конфіденційна, таємна). Якщо для службової інформації ще є якась юридична підстава у вигляді ч. 3 ст. 9, то для інших видів — ні.

Ще кілька коментарів.

1. Частина третя статті 21 Закону про інформацію встановлює, що порядок віднесення інформації до таємної або службової, а також порядок доступу до неї регулюються законом. Це положення також повторюється в іншому формулюванні в статтях 6, 8 та 9 Закону. Тобто постанова Кабміну № 1893 суперечить новим законам, як і суперечитиме законам перезатвердження цієї постанови для службової інформації.

2. Згідно з частиною першою статті 9 віднесення до службової інформації відомостей, зазначених в пунктах 1–2 цієї частини, не є автоматичним, воно здійснюється на розсуд розпорядника. Закон не вимагає застосовувати гриф ДСК до всієї внутрівідомчої кореспонденції, лише якщо в цьому є потреба і дотримано вимог трискладового тесту.

Оксана Нестеренко

ДЕЯКІ ПРОБЛЕМИ ЗАСТОСУВАННЯ ЗАКОНУ УКРАЇНИ «ПРО ДОСТУП ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ»

ЯК ВИЗНАЧИТИ ІНФОРМАЦІЮ, ЩО СТАНОВИТЬ СУСПІЛЬНИЙ ІНТЕРЕС?

Інформація, що становить суспільний інтерес[1] — категорія, що є предметом осмислення майже кожного сучасного дослідження, пов'язаного з питаннями свободи слова чи доступом до інформації. Природою цієї зацікавленості є практичний попит, оскільки визнання певної інформації суспільно значимою гарантує звільнення від відповідальності за розголошення інформації з обмеженим доступом. Не слід скидати з рахунку також той факт, що визнання інформації суспільно необхідною є безперечним юридичним фактом, котрий дозволяє поставити питання про поширення такої інформацію без згоди її власника. Наталія Петрова справедливо стверджує, що «тема суспільної значимості інформації виникає щоразу, коли є легітимні підстави обмеження доступу до певної інформації, і з'являється право громадськості дізнатися про неї»[2].

Що ж стосується вирішення цього питання у прийнятих на початку цього року Законі

---

[1] Також у науковій літературі можна зустріти терміни «суспільно важлива інформація», або «суспільно необхідна інформація», «суспільна значима інформація».

[2] *Петрова Н., Якубенко В.* Медіа право. — Київ: ТОВ «Київська типографія», 2007. — С. 64.

України «Про доступ до публічної інформації» та нової редакції Закону України «Про інформацію», то ситуація виглядає неоднозначно. Адже, незважаючи на той факт, що у Законі України «Про доступ до публічної інформації» термін «суспільно необхідна інформація» згадується декілька разів, визначення останнього відсутнє. Звісне, перше питання, яке спадає на думку, чому розробники закону не закріпили визначення цього терміна в Законі «Про доступ до публічної інформації»? Пояснення є дуже простим: станом на листопад 2010 р., тобто до останніх узгоджень та правок законопроекту про доступ до публічної інформації, визначення терміну «інформація що становить суспільний інтерес (суспільно значима або суспільно необхідна) інформація», містилося у ст. 1 законопроекту[3], проте, під час доопрацювання останнього депутати із Партії регіонів наполягли на тому, щоб цей термін було виключено із закону. Адже, на їх думку, давати визначення терміну «інформація що становить суспільний інтерес» у цьому законі нема потреби, та й предметом регулювання цього закону є лише доступ до публічної інформації. Не вплинули на депутатів і аргументи на кшталт, що необхідність визначення цієї правової конструкції є вкрай необхідною, адже доведення у суді факту, що певна інформація з обмеженим доступом є суспільно необхідною, дає підставою для прийняття рішення про надання такої інформації за запитами (наприклад, інформація про стан здоров'я кандидатів у президенти, або президента чи скажімо народних депутатів). Або такий аргумент: на підставі встановлення факту, що певна інформація з обмеженим доступом є суспільно значимою, особа може бути звільнена від відповідальності за розповсюдження цієї інформації з обмеженим доступом. Свою відмову залишити у Законі «Про доступ до публічної інформації» термін «інформацію, що становить суспільний інтерес (суспільно значима, суспільна необхідна)» народні депутати пояснили також тим, що тлумачення відповідного терміна є в оновленій редакції Закону України «Про інформацію». Отже, із остаточної редакції Закону про доступ до публічної інформації визначення суспільно необхідної інформації зникло. Натомість у оновленій редакції Закону України «Про інформацію» дійсно з'явилося положення відповідно до якого під суспільно необхідною інформацією[4] розуміється інформація, що є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від її поширення.

Разом із тим виникає необхідність з'ясувати, що саме означає категорія «суспільний інтерес». Для цього необхідно відповісти на три запитання.

1. *Коли з'являється потреба апелювати до цієї категорії?*

Це відбувається кожного разу, коли у журналіста, громадського активіста чи просто пересічного громадянина є потреба отримати певну публічну інформацію, а вона була неправомірно віднесена до інформації з обмеженим доступом. Тоді необхідно звертатися до суду з вимогою визнати незаконність дій суб'єкту владних повноважень. Відмова в наданні інформації може бути мотивована суб'єктом владних повноважень або юридичною особою приватного права тим, що запитувана інформація є конфіденційною. Тоді слід вимагати судового рішення щодо надання цієї інформації через те, що вона становить суспільний інтерес. Наприклад, стан здоров'я народних депутатів, відомості про доходи і майно вищих посадових осіб тощо. Нарешті, ми згадуємо, що інформація становить суспільний інтерес, коли одночасно доступ до неї обмежений, і за розповсюдження такої інформації притягають до відповідальності.

2. *За якими критеріями та за яких умов можна стверджувати, що інформація становить суспільний інтерес?*

Звернемося до ст. 29 Закону України «Про внесення змін до Закону України «Про інформацію». Відповідно до цієї статті «Інформація з обмеженим доступом може бути поширена, якщо вона є суспільно необхідною, тобто є предметом суспільного інтересу, і право громадськості знати цю інформацію переважає потенційну шкоду від її поширення. Предметом суспільного інтересу вважається інформація, яка свідчить про загрозу державному суверенітету, територіальній цілісності України; забезпечує реалізацію конституційних прав, свобод

---

[3] Див. Законопроект «Про доступ до публічної інформації».

[4] Треба звернути увагу, що у попередній редакції Закону України «Про інформацію» від 1992 року, законодавець вживав термін «суспільна значима інформація».

і обов'язків; свідчить про можливість порушення прав людини, введення громадськості в оману, шкідливі екологічні та інші негативні наслідки діяльності (бездіяльності) фізичних або юридичних осіб тощо».

Тобто, відповідно до цієї статті необхідно встановити: 1) яка інформація суспільно необхідною, тобто є предметом суспільного інтересу; 2) чи право громадськості знати цю інформацію переважає потенційну шкоду від її поширення. Труднощі тут полягають в тому, що термін «предмет суспільного інтересу» є також оціночною категорією.

Практичні рекомендація, яка ж, власне, інформація становить суспільний інтерес, пропонують автори книги «Свобода інформації: теорія та практика»[5]. Зокрема, Р. Карвер, пропонує при вирішенні питання, чи є інформація суспільно необхідною, виходити з того, що суспільний інтерес означає, що громадськість має вигоду від того, що певна інформація стане доступною. Він також звертає увагу на той факт, що важко визначити, яка ця вигода могла б бути, тому що, природно, за його словами, що вона змінюватиметься від справи до справи.

Досить слушними можуть виявитися для практичного застосування наведені Річардом Карвером критерії, складені Комітетом з Етики Британського Національного Союзу Журналістів (NUJ): a) Виявлення чи викриття злочину чи серйозного проступку; b) Захист суспільного здоров'я чи безпеки; c) Запобігання введенню в оману громадськості певними твердженнями чи діями з боку особи чи організації; d) Викриття неналежного використання державних коштів чи інших форм корупції в державних органах; e) Розкриття потенційних конфліктів інтересів у тих, хто посідає владні і впливові місця; f) Викриття жадібності корпорацій; g) Викриття лицемірної поведінки тих, хто займає високі посади.

Із представлених у науковій літературі думок з приводу того, яка інформація становить суспільний інтерес, заслуговує на увагу визначення, запропоноване Всеволодом Речицьким, а також критерії, розроблені Наталією Петровою.

В. Речицький пропонує до інформації, що становить суспільний інтерес, відносити інформацію, яка свідчить про загрозу державному суверенітету та територіальній цілісності України, порушення інтересів територіальних громад і права власності народу України; дозволяє здійснити обґрунтований політичний вибір; гарантує обізнаність із подіями та фактами, що безпосередньо впливають на стан і характер життя людини; забезпечує реалізацію конституційних прав, основоположних свобод і обов'язків; запобігає правопорушенням, введенню громадськості в оману, а також шкідливим екологічним та іншим наслідкам від діяльності (бездіяльності) суб'єктів господарювання тощо.

Н. Петрова, яка вже багато років займається питаннями інформаційних відносин, пропонує при вирішенні питання, чи становить інформація суспільний інтерес, брати до уваги: 1) чи суперечить чиясь поведінка посадовому обов'язку; 2) чи йдеться про наявність правопорушення; 3) чи є ознаки зловживання владою; 4) чи йдеться про недбале виконання обов'язків або неналежне управління публічним (державним) органом; 5) чи наявна корупція (невиправдане використання державних / громадських коштів) або шахрайство; 6) чи йдеться про загрозу здоров'ю, безпеці особи, групі осіб, довкіллю; 7) чи посадова особа вводила в оману громадськість публічними заявами; 8) судову помилку; 9) якщо йдеться про інтереси національної безпеки; 10) якщо йдеться про економічний добробут; 11) якщо йдеться про права людини.

Критерії, запропоновані В. Речицьким та Н. Петровою, дають можливість найбільш точно встановити, яку інформацію слід відносити до інформації, що становить суспільний інтерес.[6]

3. *Хто має вирішувати, чи становить інформація суспільний інтерес?*

Така необхідність з'являється у розпорядника інформації, який отримав запит щодо надання інформації з обмеженим доступом, але запитувана інформація становить суспільний інтерес, і тоді розпорядник інформації має застосувати трискладовий тест. Така необхідність виникає у судді, який розглядає позов з вимогою визнати незаконність дій суб'єкту владних повноважень щодо віднесення певної інформації до інформації з обмеженим доступом, або вирішує питання, чи можна надати у відповіді

---

[5] http://www.khpg.org/index.php?id=1128746915

[6] Дивись також «Принципи національної безпеки та доступ до інформації», принцип 16 у СВіПі № 1 за 2011 р. — Прим. Ред.

на запит конфіденційну інформацію, яка становить суспільний інтерес. Визнати, чи є інформація суспільно необхідною, суддя мусить також, коли вирішується питання щодо звільнення від відповідальності за розповсюдження інформації обмеженим доступом через те, що розповсюджена інформація є суспільно необхідною.

Зауважимо, що, оскільки відповідно до ч. 2 ст. 71 Кодексу адміністративного судочинства України «обов'язок доказування в адміністративних справах про протиправність рішень, дій чи бездіяльності суб'єкта владних повноважень покладається на відповідача, якщо він заперечує проти адміністративного позову», то варто вимагати, щоб при розгляді справи суб'єкт владних повноважень довів, що віднесення публічної інформації до інформації з обмеженим доступом відбувалося з дотриманням вимог зафіксованих у ст. 6 Закону «Про доступ до публічної інформації». Тобто представник суб'єкту владних повноважень повинен обґрунтувати в суді, що інформація закривалася для захисту певної легітимної мети, пояснити, яку саме істотну шкоду може завдати розголошення цієї інформації, та чому ця шкода переважає право громадськості мати доступ до цієї інформації.

ПРАВОВИЙ АНАЛІЗ РІШЕННЯ ВИКОНАВЧОГО КОМІТЕТУ СТАХАНОВСЬКОЇ МІСЬКОЇ РАДИ «ПРО ЗАТВЕРДЖЕННЯ ПЕРЕЛІКУ ВІДОМОСТЕЙ, ЩО СТАНОВЛЯТЬ СЛУЖБОВУ ІНФОРМАЦІЮ»

Відомо, що теорія права розробила систему способів тлумачення норм права, якими не можна нехтувати в процесі тлумачення закону. Ігнорування цих способів обов'язково призведе до хибного розуміння букви та духу закону[7] та порушення принципу законності при його правозастосуванні. Зокрема, окрім граматичного та логічного способу тлумачення базовими способами тлумачення, до яких обов'язково потрібно звертатися з метою правильної інтерпретації закону, є телеологічний (цільовий) та системний способи тлумачення. На жаль, на практиці досить часто органи влади й органи місцевого самоврядування нехтують останніми, що в кінцевому результаті призводить до порушення прав людини та основоположних свобод.

Саме так сталося при реалізації положень ст.ст. 6–9 Закону України «Про доступ до публічної інформації» у містах Стаханові та Краматорську. Адже, саме у цих містах органи місцевого самоврядування затвердили переліки відомостей, що становлять службову інформацію, зміст яких доволі яскраво демонструє, як довільна інтерпретація норм закону, без звернення до системного, цільового, граматичного й логічного способів тлумачення може призвести до прийняття підзаконних нормативно-правових актів, які порушують дух, принципи та цілі Закону України «Про доступ до публічної інформації». У рішеннях цих органів місцевого самоврядування порушені порядок та умови віднесення публічної інформації до категорії службової інформації.

Загалом, якщо узагальнити всі змістовні порушення ухваленого в місті Стаханові рішення «Про затвердження Переліку відомостей, що становлять службову інформацію», то вони полягають у віднесенні до службової інформації:

1) конфіденційної інформації. Ми повністю погоджуємося з позицією Д. Котляра, який звертає увагу, що безпідставним є включення до переліку відомостей, які становлять службову інформацію, інших видів інформації з обмеженим доступом[8] (для прикладу, відомості про персональні дані про громадян, факти, події та обставини їх життя, що стали відомі зі звернень громадян до Стахановської міської ради та її виконавчих органів (п. 8));

2) всупереч ч. 5 ст. 6 Закону України «Про доступ до публічної інформації» та ч. 4 ст. 21 Закону України «Про інформацію» до службової інформації віднесена та публічна інформація, яку взагалі заборонено відносити до інформації з обмеженим доступом, зокрема, й до службової (а саме, щодо відведення земельних ділянок у власність (оренду) — п. 11; відомості з кошторисної документація на

---

[7] Теоретики могли б зауважити, що в теорії ведуться спори про те, що треба тлумачити букву чи дух закону, але Ми переконані, що гарний закон це той, в якому дух закону не суперечить його букві, саме таким є Закон «Про доступ до публічної інформації» відповідно не можна й протиставляти його дух та букву.

[8] Котляр Д. Коментар щодо Звернення Луганського обласного відділення КВУ до Стаханівського міського голови»// http://stop-x-files-ua.org/?p=5768

будівництво, реконструкцію та ремонт об'єктів, відомості з рішень виконкому про затвердження проектно-кошторисної документації, відомості з договорів підряду на проектні, вишукувальні, будівельні роботи, реконструкцію та капітальний ремонт об'єктів, відомості з договорів на придбання обладнання для об'єктів будівництва — п. 40–44; Зведені відомості про кількість населення, яке проживає в зонах можливих заражень, можливі втрати, площу можливого зараження — п. 56; та ін.);

3) Публічної інформації без дотримання вимог ч. 2 ст. 6 та ст. 9 Закону України «Про доступ до публічної інформації» (зокрема, відомості із листування з органами влади вищого рівня, органами державної влади та місцевого самоврядування, підприємствами, установами, організаціями, виборчими комісіями, виборцями, політичними партіями — п. 9; інформація, відомості та дані з протоколів сесій, засідань постійних комісій, засідань виконавчого комітету Стахановської міської ради, комісій, створених при виконавчому комітеті міської ради (адміністративної, житлової та ін.), нарад — п. 10; відомості з документів (рішення, подання, клопотання, листи тощо) до протоколів сесій та засідань виконкому Стахановської міської ради з питань, які відносяться до внутрішньо-організаційної діяльності Стахановської міської ради та її виконавчих органів — п. 11; відомості з документів (подання, клопотання, характеристики) про нагородження відзнаками та присвоєння почесних звань — п. 13).

Втім, щоб не бути голослівними, треба обґрунтувати, позицію, чому відповідно до Закону України «Про доступ до публічної інформації» зміст рішення «Про затвердження Переліку відомостей, що становлять службову інформацію» не відповідає ст.ст. 6, 9 Закону України «Про доступ до публічної інформації».

Отже, виходячи із граматичного, логічного, цільового, системного способів тлумачення, відповідно до ч. 2 ст. 1, ст.ст. 6, 9:

1. До службової інформації можуть бути віднесені лише такі категорії інформації, як (ст. 9 Закону України «Про доступ до публічної інформації»):

— внутрівідомча, службова кореспонденція, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;
— інформація, що зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Якщо публічна інформація підпадає під одну із названих у п. 1 категорій інформації, ця публічна інформація може бути віднесена до службової інформації при дотриманні сукупності таких вимог: 1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя; 2) розголошення інформації може завдати істотної шкоди цим інтересам; 3) шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

Публічна інформація не може бути віднесена до службової інформації, якщо ця інформація міститься у рішенні відповідного органу, у тому числі й в актах індивідуальної дії (указ, наказ, рішення, розпорядження, постанова та ін.), за виключенням інформації, що зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни. Це випливає із ст. 6 Закону України «Про доступ до публічної інформації».

Суб'єктам владних повноважень заборонено відносити до службової інформації, відомості про розпорядження бюджетними коштами, володіння, користування чи розпорядження державним, комунальним майном, у тому числі до копій відповідних документів, умови отримання цих коштів чи майна, прізвища, імена, по-батькові фізичних осіб та найменування юридичних осіб, які отримали ці кошти або майно.

У кожному конкретному випадку при вирішенні питання щодо віднесення публічної інформації до службової інформації обов'язково повинно бути обґрунтування: 1) якому саме з інтересів загрожує надання розголошення інформації (наприклад національній безпеці, територіальної цілісності тощо); 2) у чому саме буде полягати шкода в разі розголошення цієї інформації; 3) пояснити, чому шкода від опри-

люднення такої інформації переважає суспільний інтерес в її отриманні.

Якщо в документі міститься службова інформація, що була віднесена до службової інформації, то органи державної влади, влади автономії, місцевого самоврядування, інші суб'єкти владних повноважень повинні, тим не менш, надати всю іншу інформацію, що міститься в документі. Кожен випадок не відкриття інформації має бути чітко визначений.

Іншими словами, зазначене вище означає, що: 1) інформація, яка міститься у рішеннях органах місцевого самоврядування не може бути віднесена до службової інформації; 2) строго кажучи, не може бути заздалегідь визначеного переліку відомостей, які є службовою інформацією в органах місцевого самоврядування, адже, в кожному конкретному випадку треба обґрунтувати, що розголошення певної інформації спричинить шкоду одному із інтересів зазначених у ст. 6 закону, розголошення інформації може завдати істотної шкоди цим інтересам, й шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні й в кожному конкретному випадку повинне бути обґрунтування; 3) максимум, що можуть віднести до службової інформації органи місцевого самоврядування це відомості, що містяться в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень та й лише за умови, що зможуть обґрунтувати це відповідно до вимог ст. 6 Закону України «Про доступ до публічної інформації».

Вражає й той факт, що ухвалене розпорядження обмежує доступ до інформації про розпорядження комунальним майном та бюджетними коштами, адже віднесення цієї інформації до службової прямо заборонено ч. 5 ст. 6 Закону «Про доступ до публічної інформації». Більш того, інформація про виділення земельних ділянок, що є власністю територіальної громади, є відкритою, суспільно значущою інформацією, не лише відповідно до Закону України «Про доступ до публічної інформації». Відповідно до ст.ст. 142, 143 Конституції України саме територіальна громада є власником комунального майна, а органи місцевого самоврядування, зокрема, місцеві ради лише здійснюють управління ним. Тобто у вирішенні питання про розпорядження комунальним майном місцеві ради діють лише як представники територіальної громади. Таким чином, будь-яке рішення про виділення земельної ділянки в оренду чи в безоплатне користування та інше — це, фактично, угода, яка укладається між територіальною громадою (жителями села чи добровільного об'єднання у сільську громаду жителів кількох сіл, селища та міст) і суб'єктом, який отримує цю земельну ділянку. А міська рада в цій угоді є лише представником територіальної громади. Навряд чи можна уявити ситуацію, коли власник (у нашому випадку — територіальна громада) певного майна погодиться віддати земельну ділянку особі (фізичній чи юридичній) у разі, якщо йому не відоме навіть її ім'я чи найменування. І навряд чи він дозволить своєму представнику (в нашому випадку — місцева рада) заключити угоду з цією невідомою особою, бо ціна питання є досить великою. Ця позиція знаходить своє підтвердження у Конституції України, де зазначається, що «Територіальні громади села, селища, міста безпосередньо або через утворені ними органи місцевого самоврядування управляють майном, що є в комунальній власності...» (Стаття 143).

Зрозуміло, що в переважній більшості випадків це управління майном здійснюють утворені нами органи місцевого самоврядування, адже технічно не можливо, щоб територіальна громада в кожному конкретному випадку вирішувала питання про виділення землі, чи розпорядження іншим майном. Саме для цього й обираються місцеві ради. Однак, це також означає, що ми (територіальна громада) повинні бути проінформовані, як саме ведуться наші майнові справи і, власно кажучи, кому і на яких умовах передається земля, яка нам (територіальній громаді) належить. Отже, якщо переходити на мову інформаційного законодавства, ця інформація є суспільно значущою. Такий висновок випливає, зокрема, із Закону України «Про місцеве самоврядування». Відповідно до ст. 1 цього Закону «право комунальної власності — право територіальної громади володіти, доцільно, економно, ефективно користуватися і розпоряджатися на свій розсуд і в своїх інтересах майном, що належить їй, як безпосередньо, так і через органи місцевого самоврядування». Необхідно також звернути ува-

гу на ч. 3 ст. 16 цього Закону, в якій зазначається, що «матеріальною і фінансовою основою місцевого самоврядування є рухоме і нерухоме майно, доходи місцевих бюджетів, інші кошти, земля, природні ресурси, що є у комунальній власності територіальних громад сіл, селищ, міст, районів у містах, а також об'єкти їхньої спільної власності, що перебувають в управлінні районних і обласних рад». Тобто право комунальної власності (до комунальної власності відноситься, зокрема, й земля) належить саме територіальній громаді, а не місцевим радам. І саме територіальна громада має право: а) володіти; б) доцільно, економно і ефективно користуватися і в) розпоряджатися нею на свій розсуд і в своїх інтересах, як безпосередньо, так і через органи місцевого самоврядування. Отже, дійсно територіальна громада делегувала це право органу місцевого самоврядування, але це зовсім не означає, що вона делегує право приховувати інформацію відносно такого управління!

Підтверджує цю позицію ст. 10 Закону України «Про місцеве самоврядування», де зазначається, що саме «сільські, селищні, міські ради є органами місцевого самоврядування, що представляють відповідні територіальні громади та здійснюють від їх імені та в їх інтересах функції і повноваження місцевого самоврядування, визначені Конституцією України, цим та іншими законами».

Отже, місцеві ради не виступають в якості власника при вирішенні питань відносно передачі земельних ділянок, а лише представляють відповідні територіальні громади та здійснюють свої функції від імені територіальної громади та лише в її інтересах. Таким чином, з цієї норми органічно випливає, що всі рішення рад повинні бути доведені до відома територіальної громади, щоби ця громада, як власник, могла зробити висновок, наскільки рада діяла в його інтересах. Громада повинна мати вичерпну інформацію про дії свого представника. Тобто діяльність міської ради повинна бути гласною (ст. 4 «Основні принципи місцевого самоврядування»), адже серед принципів, які є основою місцевого самоврядування, є принципи гласності, підзвітності та відповідальності перед територіальними громадами їх органів та посадових осіб. Тобто знов таки законодавець підкреслює, що за всі свої рішення та угоди місцева влада повинна звітувати перед територіальною громадою.

ЯК ТЛУМАЧИТИ ПОНЯТТЯ «ПЕРЕЛІКУ ВІДОМОСТЕЙ, ЩО СТАНОВЛЯТЬ СЛУЖБОВУ ІНФОРМАЦІЮ»?

Другим проблемним питанням цих переліків, є те, що, виходячи із системного способу тлумачення, такі переліки в принципі не можливі, бо сам Закон чітко окреслив категорії інформації, що можуть бути віднесені до службової. Якщо певні відомості підпадають під одну з двох категорій (тобто предмет службової інформації є достатньо вузьким), тоді за умови, як ми вже зазначили, якщо суб'єкт владних повноважень зможе довести, що розголошення конкретної інформації спричинить істотну шкоду одному із інтересів зазначених у ст. 6 закону, й шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні, лише тоді ця інформація може бути віднесена до службової.

Строго кажучи, не може бути заздалегідь визначеного переліку відомостей, які є службовою інформацією в органах місцевого самоврядування. Крім того, у кожному конкретному випадку при вирішенні питання щодо віднесення публічної інформації до службової інформації обов'язково повинно бути обґрунтування: 1) якому саме з інтересів загрожує розголошення інформації (наприклад національній безпеці, територіальній цілісності тощо); 2) у чому саме буде полягати шкода в разі розголошення цієї інформації; 3) пояснити, чому шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні.

Тобто, як зазначає Д. Котляр, перелік відомостей може бути прийнятий на виконання п. 3 ст. 9 Закону України «Про доступ до публічної інформації», щодо деталізації пункту 2 частини першої статті 9 (якщо не брати до уваги формулювання ч. 3 ст. 9 буквально), якщо йдеться про переліки категорій відомостей, які може бути віднесено до службової інформації, а не про опис відомостей, які наперед віднесено до такої інформації[9].

Отже, за великим рахунком, в органах місцевого самоврядування взагалі не може бути службової інформації. Звичайно можна зазначити, що це не можливо, щоб майже вся інформація про діяльність влади ставала відкритою, щоб до-

---

[9] Котляр Д. Коментар щодо Звернення Луганського обласного відділення КВУ до Стаханівського міського голови»// http://stop-x-files-ua.org/?p=5768

кументи, на які ставили гриф «Для службового користування», в принципі стали дуже рідким винятком. Але саме в цьому й полягає мета Закону України «Про доступ до публічної інформації» — подолати надмірну секретність й зробити діяльність влади дійсно відкритою для публіки, зробити революцію в сфері реалізації права на доступ до публічної інформації. Крім того, фактично знову ж таки виходячи із системного способу тлумачення ст. 9 Закону України «Про доступ до публічної інформації», а саме, що предметом службової інформації за виключенням інформації про оперативно-розшукову діяльність, контррозвідувальну діяльність, та інформації в сфері оборони *може бути лише внутрівідомча службова кореспонденція, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень.* Іншими словами, фактично на статус службової інформації може претендувати лише внутрішнє листування та обговорення перед прийняттям конкретного рішення, або документи щодо здійснення перевірок до прийняття рішення про результати перевірок. Це означає, що публічна інформація не може бути віднесена до службової, якщо ця інформація вже міститься у рішенні відповідного органу, у тому числі й в актах індивідуальної дії (указ, наказ, рішення, розпорядження, постанова та ін.), за виключенням, як я вже зазначала, інформації, що зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни. Таким чином, рішення органів виконавчої влади не можуть бути віднесені до службової інформації. Для прикладу, не може бути надано гриф «ДСК» Постанові, Розпорядженню Кабінету Міністрів України, Наказу Податкової Адміністрації України та ін. Утім, всім відомо, що Кабінет Міністрів продовжує видавати акти, що мають грифи ДСК, досі не скасована Постанова Кабінету Міністрів № 1893 (про конфіденційну інформацію, що є власністю держави) та не відкриті Постанови та Розпорядження Кабміну, що мають гриф «ДСК».

Звичайно, суб'єкти владних повноважень можуть заперечити: а як же бути із виконанням п. 3 ст. 9 Закону України «Про доступ до публічної інформації»?

Відповідь на це запитання така. Ця норма виглядає, як в тій всім відомій приказці: хотіли, як краще, а вийшло, як завжди. Тобто, бажали включити додаткову гарантію забезпечення права на доступ до публічної інформації, а виходить, як її почали тлумачити органи місцевого самоврядування, що вона перекриває і ч. 1 ст. 9, і ч. 2 ст. 6 Закону. Але, коли формулювали ч. 3 ст. 9, під переліком малося на увазі ті відомості, які вже після трискладового тесту були віднесені до службової інформації.

Втім, дійсно проблема полягає в тому, що фактично на практиці це зробити вельми важко, бо це великий обсяг роботи й, крім того, можна казати, що із цього переліку вже можна зробити висновок, що саме закрили.

Найбільш ґрунтовне тлумачення п. 3 ст. 9 Закону України «Про доступ до публічної інформації» запропонував Дмитро Котляр, який був одним із учасників робочої групи з розробки Закону «Про доступ до публічної інформації». Зокрема, на переконання Д. Котляра, положення ч. 3 ст. 9 Закону України «Про доступ до публічної інформації» є дійсно проблематичним. У ньому йдеться про «перелік відомостей», а не категорій відомостей. При цьому «відомостей, що становлять службову інформацію», тобто таких, які вже було віднесено до службової інформації, а не тих, що може бути віднесено в майбутньому. Це суперечить ч. 2 ст. 6 та самій ст. 9 Закону України «Про доступ до публічної інформації», в яких кілька разів наголошується, що обмеження доступу здійснюється тільки після застосування трискладового тесту, тобто не можна наперед визначати, які відомості є службовою інформацією, це повинно визначатися в кожному конкретному випадку з урахуванням обставин ситуації та із застосуванням вимог ч. 2 ст. 6 (тобто трискладового тесту).

Отже, для того, щоб не було суперечності з цим принциповим положенням Закону України «Про доступ до публічної інформації», у ч. 3 ст. 9, — за словами Д. Котляра — мало би йтися або про перелік конкретних документів, яким вже надано гриф ДСК, або про перелік категорій відомостей, *які може бути віднесено до службової інформації* для деталізації положень ч. 1 ст. 9. Саме за одним з цих варіантів і слід тлумачити цю норму, інші варіанти будуть суперечити ч. 2 ст. 6., — наголошує Д. Котляр[10].

Д. Котляр пропонує два варіанта реалізації цієї норми на практиці.

---

[10] Котляр Д. Коментар щодо Звернення Луганського обласного відділення КВУ до Стаханівського міського голови»// http://stop-x-files-ua.org/?p=5768

Варіант перший.

Д. Котляр пропонує уважно подивитися на відмінності між пунктами 1 і 2 частини першої статті 9 Закону України «Про доступ до публічної інформації». У пункті 1 йдеться про певні документи, які можуть містити службову інформацію («документи, які становлять внутрівідомчу кореспонденцію...»). Тому за цим пунктом визначати «перелік відомостей» нема сенсу, бо немає значення, які саме відомості, наголос робиться на тому, в якому документі вони фіксуються і яким може надаватися гриф ДСК (з урахуванням ч. 2 ст. 6, звичайно). Тобто переліку категорій відомостей за цим пунктом не може бути, бо тоді треба окреслювати зміст всіх питань, з якими має справу розпорядник і які можуть потрапити у його внутрівідомчу кореспонденцію. За цим пунктом ч. 1 ст. 9 Закону може бути складено тільки перелік документів з грифом ДСК (Д. Котляр)[11].

Тоді як у пункті 2 частини першої статті 9 йдеться про сфери, в яких збирається інформація, тобто визначення робиться через зміст інформації, і тут наявність переліку категорій відомостей може мати сенс і можна навіть обґрунтувати необхідність визначення таких категорій і складання відповідного переліку (Д. Котляр). Ці три сфери, — звертає увагу Д. Котляр (інформація, «зібрана у процесі оперативно-розшукової діяльності», «зібрана у процесі контррозвідувальної діяльності» і «у сфері оборони») — є достатньо широкими і нечіткими. Тому складання переліку того, які саме відомості входять до цих сфер, необхідне для їх чіткого визначення. І тут вступає в дію заборона ч. 3 ст. 9 — ці переліки є відкритими і підлягають громадському контролю за тим, чи є вони обґрунтованими. Тобто наявність такого переліку навпаки, може запобігати підведенню під пункт 2 необмеженого кола інформації. Тим більше, що це стосується таких закритих сфер, як правоохоронна діяльність, розвідка, оборона, де є серйозний ризик того, що під цю категорію (пункт 2 ч. 1) будуть підводити все, що заманеться[12].

Отже, за цією логікою тлумачення «переліки відомостей, що становлять службову інформацію» повинні затверджуватися суб'єктами владних повноважень, які збирають інформацію в процесі оперативно-розшукової діяльності чи контррозвідувальної діяльності, або які володіють інформацією у сфері оборони. Такі переліки містять категорії відомостей (у зазначених сферах), що можуть бути віднесені в конкретних ситуаціях до службової інформації, за умови виконання вимог ч.2 ст. 6 Закону, і є відкритою інформацією. Переліки відомостей не складаються для інформації, що міститься в документах, визначених в п. 1 ч. 1 ст. 9[13].

Варіант другий.

Разом з тим, оскільки Д. Котляр, розуміє, що схема, описана в першому варіанті, не усуває суперечливостей частини третьої ст. 9, в якій йдеться про перелік «відомостей», що «становлять» службову інформацію, і п. 1 ч. 1 ст. 9, де йдеться про категорії документів, а не «відомостей», він пропонує другий варіант вирішення цієї проблеми. А саме: вважати, що йдеться про перелік конкретних документів (назви, реквізити), яким вже було надано гриф ДСК, і що це є додаткова гарантія відкритості такого переліку. Але тут виникає проблема з поясненням, навіщо потрібна ця норма (ч. 3 ст. 9), якщо цей перелік вже охоплюється системою обліку, яка також є відкритою за ст. 18 Закону[14].

Д. Котляр також звертає увагу, що, практика застосування закону вже пішла шляхом перезатвердження «переліків відомостей» і включення до них необмеженого кола питань, й за прогнозами Д. Котляра, цій практиці буде сприяти і тенденція до автоматичного зрівняння «конфіденційної інформації, що є власністю держави» у старому Законі про інформацію із «службовою інформацією» у Законі про доступ і переведення всіх процедур, які існували раніше для ДСК на службову інформацію за новим законом. Хоча, другий варіант (перелік документів з грифом ДСК) є простішим для пояснення, перший варіант, переконаний Д. Котляр, (перелік категорій відомостей, які може бути віднесено до службової інформації з дотримання вимог ч. 2 ст. 6) дозволяє спрямувати практику в правильному напрямі. Слід, правда, визнати, що обидва варіанти не є бездоганними, оскільки в обох випадках випадках прихо-

---

[11] Там само.

[12] Там само.

[13] Котляр Д. Коментар щодо Звернення Луганського обласного відділення КВУ до Стаханівського міського голови» // http://stop-x-files-ua.org/?p=5768

[14] Там само.

диться «творчо» тлумачити формулювання, вжиті в ч. 3 ст. 9 Закону[1].

ВИСНОВКИ

Підводячи риску під правовим аналізом рішення стахановської міської ради та інших подібних рішень, треба наголосити, що практика затвердження подібних переліків «відомостей, що становлять службову інформацію» є незаконною відповідно до ухваленого Закону України «Про доступ до публічної інформації», бо, це прямо суперечить п. 1 ч. 1 ст. 4, ст. 6, ст. 9 Закону України «Про доступ до публічної інформації» та й в загалі суперечить принципам діяльності органів місцевого самоврядування, проголошених Законом України «Про місцеве самоврядування», зокрема принципу гласності.

Сьогодні фахівці в сфері доступу до інформації, а також організації громадянського суспільства і жителі територіальних громад повинні робити не лише відкрите звернення, а й через прокуратуру, суд вимагати скасування чи перегляд цих переліків, відповідно до яких фактично вся інформація саме про діяльність органів місцевого самоврядування, й перш за все розпорядження бюджетними коштами, комунальним майном відповідно до цих переліків стала інформацією з обмеженим доступом. Вражає й той факт, що відомості з документів (подання, клопотання, характеристики) про нагородження відзнаками та присвоєння почесних звань виявляється також є інформацією з обмеженим доступом.

В противному випадку, якщо зараз ми промовчимо, органи влади та місцевого самоврядування зроблять загальноприйнятою практикою відносити будь-яку інформацію про діяльність органів місцевого самоврядування до службової. А це буде означати, що ми потерпіли повне фіаско і не змогли реалізувати потенціал, закладений у Законі України «Про доступ до публічної інформації». Й фактично погоджуємося, що принцип верховенства права є звичайною фікцією, а в сучасній Україні, як і за радянських часів, вищу юридичну силу мають не правові закони, а інструкції, жити за якими нас привчали протягом всієї історії існування Радянського Союзу.

---

[1] Там само.

Олег Мартыненко

ДОСТУП К ПУБЛИЧНОЙ ИНФОРМАЦИИ: ВЕРСИЯ МВД УКРАИНЫ

МВД Украины утвердило «Перечень ведомостей, составляющих служебную информацию в системе Министерства внутренних дел». О чем теперь можно спрашивать МВД и какая информация останется закрытой от общественного контроля?

09 июня 2011 г. МВД Украины издало приказ № 309, которым утвердило «Перечень ведомостей, составляющих служебную информацию в системе Министерства внутренних дел». На сайте МВД этот приказ в рубрике «Нормативные акты» отсутствует, но сам перечень размещен в разделе «Доступ к публичной информации»: http://mvs.gov.ua/mvs/control/main/uk/publish/article/625096

Напомним, что вся служебная информация помечается специальным грифом ограничения доступа «Для служебного пользования» и в большинстве своем навсегда становится закрытой как для обычного гражданина, так и для народа Украины в целом.

В первую очередь нужно, конечно, честно похвалить сотрудников МВД, поскольку составление и публикация перечня закрытой информации значительно облегчает работу тех организаций, которые направляют информационные запросы в адрес МВД и занимаются анализом правоохранительной деятельности.

А вот во вторую очередь хочется акцентировать внимание наших законодателей и специалистов Министерства юстиции на тех вопросах, которые возникают при прочтении всего перечня закрытых сведений.

Итак, давайте послушаем вопросы обычного украинца о содержании служебной информации по пунктам:

2.2. «...численность лиц, которые ... были объектами оперативно-розыскных дел...» — какую важную тайну охраняет это ограничение? Неужели гражданам нельзя знать, что к примеру, в 2009 г. такими объектами оперативной деятельности было 770 тыс. граждан, а в 2010 г. эта цифра перевалила за 4 млн. или наоборот, упала до 20 тыс. чел.? А как же мы тогда сможем оценить нелегкую, но скрытую работу оперативников?

2.6. тактика и организация «...розыска без вести пропавших детей...» — а разве родителей не касается, что именно будут делать или что должны сделать работники милиции, чтобы найти их ребенка?

10.1.1. «Порядок уничтожения изъятых из незаконного оборота наркотических средств, психотропных веществ и прекурсоров, а также оборудования для их изготовления, использование которого в законном обороте признано нецелесообразным» — почему граждане не могут убедиться в том, что такой порядок составлен подробно, качественно и не допускает тех не единичных случаев, когда оперативники вместо уничтожения изъятых наркотиков ими же потом и торгуют?

11.2. «Содержание ... служебной и профессиональной подготовки личного состава подразделений оперативной службы...» — зачем скрывать такую информацию? Ведь и в резолюции № 690 (1979 г.) Парламентской ассамблеи Совета Европы «Декларация о полиции» четко указано: «Процесс общей подготовки сотрудников должен быть максимально от¬крытым для общества» (ст. 27). Вряд ли подлежит сомнению, что граждане Украины должны быть уверены в том, что наши оперативные уполномоченные учатся и первую медицинскую помощь оказывать, и права человека не нарушать, и служебную этику соблюдать. Равно как и знать, обучают ли оперативников правильно применять огнестрельное оружие, изучают ли сотрудники новые законы и нормативные акты, умеют ли пользоваться специальной (и потому дорогой) техникой.

11.3. «Анализ состояния и причин суицидальной активности в органах внутренних дел Украины...» — очень проблематичный и спорный пункт. Представьте только себе следующую сцену разговора между хозяином и своим мажордомом:

— А что, Степан, слуги у нас вешаются или как?

— Да по-всякому бывает, барин. Случается, что и вешаются, и стреляются. Но Вы за то не беспокойтесь, мы все уладим

— А от чего ж они такое над собой вытворяют? — недоумевает хозяин. — Может, живут плохо или нуждаются в чем? А может, ты с ними чересчур суров?

— Дык это, барин, извините, Вам знать никак нельзя. Это только промеж нас, слуг, про такое говорится.

— В своем ли уме ты, Степан?! — гневно супит брови барин. — Это как это мне, да и знать нельзя?!

— Да вот так-с, барин, никак нельзя. Я и распоряженьице вот выдал. В нем все и прописал — что Вам положено знать в своем доме, а что, извините, для Вас того, служебная информация...

«Бред!» — скажет любой читатель и будет прав. Потому что не может хозяин (народ Украины) не иметь доступа к информации о том, как часто и почему наемные рабочие (государственные служащие, работники милиции) сводят счеты с жизнью. Если мои оппоненты скажут, что такую закрытую информацию контролируют и анализируют специально уполномоченные компетентные органы (Генпрокуратура, Минздрав, Кабинет Министров и т. д.), то это не меняет принципиальной сути вещей — слуги контролируют слуг, не допуская к этому процессу хозяина. И тогда возникает вопрос — а кто, собственно, в доме хозяин?

11.4. «Анализ состояния социально-психологического климата в коллективах органов внутренних дел Украины и причин, влияющих на социально-психологический климат» — помимо аргументов, изложенных выше, хочется добавить, что сотрудники милиции не живут изолированно от нас. И их семьям вовсе не безразлично, что происходит на работе с их близкими — надежный ли там коллектив, хорошая ли атмосфера, справедливый ли начальник. Все это они узнают и так, получая информацию от самих работников милиции. Но в дополнение к этому гражданам Украины нужно еще и видеть, что забота о правоохранителях является отдельным направлением работы государственного аппарата. А как это можно увидеть и тем более, оценить, если информация скрыта за грифом «Для служебного пользования»?

11.6. «Информация о результатах ... психодиагностики с целью выявления у работников ОВД Украины состояний эмоционально-психологической напряженности, переутомления, иных негативных психологических состояний» — здесь снова всплывают образы барина и мажордома Степана. Разумеется, что результаты психодиагностики конкретных лиц и даже категорий должны составлять служебную тайну. Но зачем прятать всю информацию? Ведь в самом обобщенном виде граждане должны иметь сведения о том,

какая часть сотрудников милиции (в %) находится в состоянии, требующем вмешательства и квалифицированной помощи? Министерство транспорта, например, находит в себе мужество сообщать о том, сколько водителей автобусов были выявлены в состоянии хронической усталости и потому сняты с маршрутов. Почему же МВД не может сообщать гражданам, сколько сотрудников милиции, например, были отстранены от несения службы и ношения огнестрельного оружия по причинам «эмоционально-психологической напряженности, переутомления, иных негативных психологических состояний»? Каким устоям государства может угрожать разглашение такой «служебной информации»?

11.18. «...обобщенные результаты специальной проверки относительно лиц, которые принимаются на службу..., поступают на дневные отделения учебных заведений МВД, а также принимаются на должности ... служащих» — зачем лишать налогоплательщиков Украины возможности оценить масштабы работы МВД по отбору персонала? Будет ли являться оправданно закрытой от населения информация МВД о том, что на протяжении, скажем 2010 года, была проведена специальная проверка в отношении 16 тыс. кандидатов на службу в ОВД, при этом у 5% из них были выявлены факты злоупотребления алкоголем, у 2% — ранее совершенные административные правонарушения, у 18% — связи с криминальными элементами?

12.11. Организация «...пропускного режима в МВД, ГУМВД, УМВД, ...высших учебных заведениях ... в условиях мирного времени» — зачем скрывать информацию о том, кто и когда имеет право пройти на территорию подразделений милиции, какие документы нужно предъявлять гражданам и какому должностному лицу? Разве не должны знать граждане о том, кто, когда и в каком журнале фиксирует их приход в райотдел? Об организации пропускного режима в вузы МВД вообще знает любой цивильный студент платного отделения этих же вузов — об этом они информируются в обязательном порядке. Получается, что до выхода данного приказа работники вузов МВД разглашали студентам служебную информацию?

14.1.2. «Порядок проведения проверок соблюдения законодательства при использовании средств на расходы специального предназначения» — вполне возможно, что *результаты* таких проверок и не должны быть в общем доступе. Но зачем скрывать от налогоплательщиков *сам порядок проведения* соблюдения законодательства? Какие тайные механизмы в нем заложены?

14.1.6. «Договоры по закупке имущества, которые заключаются МВД с поставщиками для организации материально-технического обеспечения подразделений» — зачем нужно скрывать всю информацию о таких договорах вместо того, чтобы сделать закрытой только необходимую их часть (банковские реквизиты, персональную информацию, название спецтехники и т. д.)? Ведь за рубежом полиция каждый год отчитывается перед населением, сколько имущества она закупила и на какую сумму, сколько было потрачено на все статьи расходов. Почему население должно оставаться в неведении, если донецкая милиция закупает на казенные деньги топливо по ценам, в 1,5 раза превышающим рыночные? Или МВД вопреки запрету Кабинета Министров закупает престижные иномарки на сотни тысяч гривен?

15.2. «Выполнение планов научной работы научно-исследовательских учреждений МВД» — а все ли результаты научной работы стоит прятать от населения, особенно, если речь идет всего лишь о выполнении планов? Если научно-исследовательская лаборатория разработала методическое пособие по соблюдению прав человека — стоит ли этот факт скрывать за грифом «Для служебного пользования» и если стоит, то от кого?

Как видно из приведенного перечня, вопросов у неискушенного читателя может возникнуть более, чем достаточно. Очевидно, что перечень ограничений, введенный МВД Украины по доступу к публичной информации, должен стать предметом отдельного рассмотрения как институтов гражданского общества, так и государственных специалистов в области нормотворчества. И самым первым шагом в этом направлении, наверное, должна стать инициатива Общественного совета при МВД Украины по обсуждению разработанного перечня совместно с руководством министерства.

http://www.umdpl.info/index.php?id=1313560636

ПОЯСНЮВАЛЬНА ЗАПИСКА

до проекту нормативно-правового акту Державної архівної служби України «Порядок користування документами Національного архівного фонду України, що належать державі, територіальним громадам»

Нині в Україні є чинним «Порядок користування документами Національного архівного фонду України, що належать державі, територіальним громадам», затверджений наказом Державного комітету архівів України від 24 листопада 2005 р. № 139 (з подальшими змінами). Цей порядок значною мірою успадкував традиційний радянський підхід щодо обмеженого доступу громадян до архівних документів.

Його характерними рисами, зокрема, є:

— дозвільний характер доступу користувачів до документів Національного архівного фонду (далі — НАФ);
— вимога до користувачів мотивувати свою потребу у документах Національного архівного фонду;
— обмеження доступу до документів певними хронологічними і тематичними рамками;
— надання переваг у користуванні документами юридичним особам та особам, які виконують службове завдання;
— створення умов для обмеження керівництвом архіву кількості документів, що видається користувачеві, і строків користування ними;
— закріплення максимальних норм видавання документів користувачеві за відсутності мінімальних норм.

Цей Порядок неодноразово критикувався науковцями і правозахисниками. На необхідність його удосконалення, зокрема, вказувалося в резолюції Міжнародної науково-практичної конференції «Удосконалення законодавства і практики щодо забезпечення доступу до архівної інформації в Україні», яка відбулася у Києві 25–26 листопада 2010 р. за ініціативою Харківської правозахисної групи, Державного комітету архівів України, Інституту держави і права імені В.М. Корецького Національної академії наук України та Міжнародної асоціації істориків права.

Виходячи з наведеного, нами було розроблено проект нової редакції Порядку користування документами Національного архівного фонду України, що належать державі, територіальним громадам з метою узгодження зазначеного підзаконного акта з оновленим інформаційним законодавством України та відповідними європейськими стандартами, що знайшли відображення у Рекомендації № R (2000) 13 Комітету Ради Європи міністрів державам-членам про європейську політику щодо доступу до архівів.

У проекті, який пропонується для обговорення, на нашу думку, вдалося позбутися ряду недоліків чинного Порядку. Зокрема, в ньому:

— забезпечено заявницький, а не дозвільний порядок оформлення доступу до користування документами НАФ;
— закріплено презумпцію вільного необмеженого доступу користувачів до всіх документів НАФ і, зокрема, знято безпідставні обмеження на користування документами за тематичною або хронологічною ознакою;
— закріплено мінімальні, а не максимальні норми видавання документів НАФ користувачам;
— створено нормативно-правові передумови для дистанційного користування документами НАФ, подання заяв на доступ до документів та замовлень на видавання конкретних документів електронною поштою;
— закріплено право користувачів на вільне створення цифрових та інших копій наданих у їх користування документів з одночасним встановленням їх обов'язку безоплатно передавати архівам один примірник створених копій;
— зрівняно юридичні і фізичні особи у їх правах щодо користування документами НАФ;
— закріплено право користувачів на здорові й безпечні умови праці в архівах;
— скасовано обов'язковість подання користувачами відомостей про напрям їх досліджень та деякої іншої інформації, яка має подаватися користувачами лише добровільно з метою сприяння аналітичній та іншій діяльності архівів тощо.

Підготовлений проект пропонується направити в Державну архівну службу України і з врахуванням позиції цього державного органу після відповідного доопрацювання винести на широке обговорення.

Розробники проекту:

І.Б. Усенко, кандидат юридичних наук, професор, заслужений юрист України, лауреат Державної премії України в галузі науки і техніки;

К.Є. Новохатський, почесний член Спілки архівістів України, відмінник архівної справи, заслужений працівник культури України, лауреат премії імені Василя Веретенникова.

Проект

ПОРЯДОК користування документами Національного архівного фонду України, що належать державі, територіальним громадам

1. Загальні положення

1.1. Цей Порядок розроблено відповідно до Законів України «Про Національний архівний фонд та архівні установи», «Про інформацію», «Про внесення змін до деяких законодавчих актів України щодо посилення протидії незаконному обігу архівних документів» та Положення про Державну архівну службу України, затвердженого Указом Президента України від 6 квітня 2011 року № 407, з подальшими змінами і доповненнями.

1.2. Державні архівні установи, архівні відділи міських рад (далі — архіви) надають документи Національного архівного фонду (далі — НАФ), що належать державі, територіальним громадам, для користування; створюють для цього необхідний загальнодоступний довідковий апарат; відповідно до наявних технічних можливостей забезпечують умови для віддаленого доступу до довідкового апарату і документів НАФ, що користуються найбільшим попитом; видають архівні довідки, копії документів та іншим шляхом задовольняють запити фізичних і юридичних осіб; повідомляють про документи, у яких містяться відомості, що можуть бути використані органами державної влади і органами місцевого самоврядування та іншими заінтересованими сторонами; публікують, експонують та в іншій формі популяризують архівні документи; виконують інші функції, спрямовані на ефективне використання відомостей, що містяться в документах НАФ.

1.3. Цей Порядок установлює основні вимоги щодо оформлення осіб для роботи в читальних залах (секторах користування документами, віртуальних читальних залах) архівів, організації доступу до документів НАФ загального користування, що належать державі або територіальним громадам, видавання цих документів у тимчасове користування, роботи з цими документами та їх копіювання, а також визначає права та обов'язки користувачів.

1.4. Дія цього Порядку поширюється на центральні державні архіви, Державний архів в Автономній Республіці Крим, державні архіви областей, міст Києва і Севастополя, архівні відділи районних державних адміністрацій, архівні відділи міських рад, галузеві державні архіви, архівні підрозділи органів державної влади, органів місцевого самоврядування, державних і комунальних установ, підприємств і організацій, а також архівні підрозділи державних наукових установ, музеїв та бібліотек.

Порядок користування документами НАФ, що належать іншим власникам, визначається власником документів з урахуванням рекомендацій Державної архівної служби України.

1.5. Відвідування користувачами читальних залів архівів, ознайомлення з довідковим апаратом і надання фізичним особам для користування документів НАФ, що належать державі, територіальним громадам, відповідно до встановлених у пункті 3.3 цього Порядку нормативів, а також юридичним і фізичним особам, які передали зазначені документи на зберігання, здійснюються безоплатно.

1.6. Платні послуги користувачам надаються згідно з Переліком платних послуг, які можуть надаватися державними архівними установами, що утримуються за рахунок бюджетних коштів, затвердженим постановою Кабінету Міністрів України від 7 травня 1998 року № 639 (зі змінами).

1.7. Графік роботи читального залу, затверджений наказом керівництва архіву, має відповідати режимові роботи архіву, передбачати можливість праці у суботні дні та вечірні години і регулюватися відповідно до кількості користувачів та частоти відвідувань ними читального залу.

Графік роботи читального залу має бути вивішено у доступному для відвідувачів місці, а також оприлюднено на веб-сайті архіву, у місцевих засобах масової інформації, довідково-інформаційних виданнях архіву або в інший спосіб.

1.8. Цей Порядок має бути вивішено у доступному для відвідувачів місці.

2. Оформлення осіб для користування документами НАФ у читальних залах (секторах користування документами, віртуальних читальних залах) архівів

2.1. Особи, які мають намір користуватися документами НАФ у читальних залах (секторах користування документами, віртуальних читальних залах) архівів, подають паспорт (посвідчення особи), ознайомлюються з Порядком користування документами архіву і заповнюють заяву встановленого зразка (додаток 1). Своїм підписом у заяві (позначкою в електронній формі) вони засвідчують факт ознайомлення з цим Порядком та зобов'язання його виконувати. Заяву користувач може надіслати поштою, зокрема, електронною (за наявності в архіві такої пошти).

2.2. Іноземці та особи без громадянства, що перебувають в Україні на законних підставах, користуються тими самими правами доступу до документів НАФ і мають такі самі обов'язки щодо користування ними, як і громадяни України.

2.3. Особи, які мають намір користуватися документами, щодо яких юридичні і фізичні особи, котрі передали зазначені документи на зберігання, встановили певні обмеження доступу, додатково подають відповідний лист-доручення або лист-згоду від фондоутворювачів або їх правонаступників. Порядок оформлення доступу до документів, які містять державну таємницю, службову або конфіденційну інформацію, визначається відповідним законодавством.

2.4. Керівник архіву перевіряє повноту і правильність наведення у заяві обов'язкових відомостей про користувача, а у разі потреби також наявність у нього повноважень представляти юридичну особу або належно оформленого права працювати з документами, доступ до яких обмежено відповідно до законодавства, і з відповідною резолюцією передає заяву до читального залу.

Забороняється вимагати від користувачів надання документів, не передбачених цим Порядком.

2.5. На підставі документа, що посвідчує особу, та згідно з резолюцією керівника архіву на заяві користувача завідувач читального залу або особа, яка виконує його обов'язки, видає користувачеві перепустку до читального залу архіву або інформацію, необхідну для забезпечення дистанційного доступу до документів.

2.6. Завідувач читального залу формує на кожного користувача справу, до якої входять його заява, замовлення користувача на видавання конкретних документів НАФ, копії відмов у доступі до документів та інші документи, що стосуються користування документами НАФ.

2.7. У разі, якщо документи НАФ копіюються чи іншим чином використовуються з комерційною метою, архів укладає з користувачем або з особою, яку він представляє, окремий цивільно-правовий договір.

2.8. Керівництво архіву (або, за його поданням, керівництво Державної архівної служби України) має право припинити або обмежити доступ до документів НАФ, особі, яка грубо порушила цей Порядок (у разі псування, знищення, підроблення, розкрадання документів НАФ, або свідомого перекручення чи фальсифікації відомостей, що містяться в документах, порушення з вини користувача строків повернення документів, наданих у тимчасове користування за межами архіву), незалежно від того, в якому архіві вчинено це порушення. Про відмову (обмеження) в доступі до документів НАФ користувачеві повідомляється письмово із зазначенням підстав відмови.

3. Організація роботи користувачів у читальних залах архівів, їх права та обов'язки

3.1. Архіви надають користувачам відповідно до їхніх замовлень копії документів НАФ з фондів користування, а в разі їх відсутності оригінали документів (справи, кіно-, фоно-, відеодокументи), довідковий апарат (довідники, путівники, описи, каталоги, огляди, покажчики, картотеки тощо), а за обґрунтованої потреби й згодою керівництва архіву — облікові документи (справи фондів, реєстри описів фондів).

Користувачі можуть користуватися виданнями, що зберігаються у довідкових бібліотеках архівів і підсобних фондах читальних залів.

3.2. Документи НАФ надаються на підставі письмового замовлення встановленого зразка (додаток 2), яке подається користувачем особисто або поштою, зокрема, електронною.

3.3. Кількість документів, які щоденно можуть видаватися одному користувачеві, визначаються керівництвом архівом, виходячи з розрахунку навантаження, яке припадає на працівників архіву за середньостатистичної для цього архіву кількості відвідувачів. При цьому користувачеві забезпечується одержання щоденно не менше 5 описів, 10 бюксів мікрокопій, однієї тисячі аркушів архівних справ (але загалом не більше 20 справ), 50 кальок науково-технічної документації, 20 одиниць зберігання кінодокументів, а також звукозаписів, що за загальним обсягом не перевищують чотирьох годин звучання, та відеодокументів, що за загальним обсягом не перевищують чотирьох годин екранного часу.

Дозволяється подання замовлень користувачем одночасно не більше, ніж на три робочі дні вперед.

3.4. Збільшення обсягів щоденного видавання документів НАФ користувачеві понад встановлені норми може бути передбачено як платна послуга.

3.5. Справи та документи, на які в архівах існують фонди користування, видаються до читальних залів архівів лише в копіях.

За наявності якісних копій замовлених документів у фонді користування оригінали документів НАФ з метою забезпечення їх збереженості видаються з дозволу керівництва архіву лише у виключних випадках — для спеціального джерелознавчого дослідження, що потребує вивчення матеріалу носія інформації, зовнішніх ознак документа тощо.

3.6. Працівники архівосховища зобов'язані здійснювати поаркушне перевіряння одиниць зберігання та справ перед їх видаванням користувачеві, а працівники читального залу — після їх повернення користувачем, що фіксується у замовленні на видавання справ (додаток 2). На вимогу користувача перевірка повернутих документів має здійснюватися у його присутності.

3.7. Замовлені користувачем документи НАФ у читальному залі зберігаються у спеціальних шафах, доступ до яких мають лише працівники читального залу.

У разі, якщо документ (одиницю зберігання) одночасно замовили кілька користувачів, порядок користування ним визначається завідувачем читального залу.

3.8. Описи, інші нетиражовані архівні довідники видаються користувачам на строк до 5 днів, копії та видання — до одного місяця, оригінали документів НАФ — до 10 днів, оригінали унікальних та особливо цінних документів — до 5 днів.

Строк користування обчислюється з дня видавання документів з архівосховища. Подальше подовження строків здійснюється за погодженням з керівництвом архіву на підставі мотивованої письмової заяви користувача.

3.9. Якщо користувач не звертається за замовленими документами, то їх повертають до архівосховища після закінчення строку, зазначеного у п. 3.8. цього Порядку.

3.10. Друковані видання, примірники описів, що зберігаються безпосередньо в читальних залах архівів, видаються користувачам у день замовлення.

Строк видавання інших описів, справ, документів не повинен перевищувати двох робочих днів від часу оформлення замовлення, без урахування дня замовлення.

Якщо документи з конкретного віддаленого архівосховища через технічні умови видаються лише раз на тиждень, то норма видавання таких документів для користувача збільшується втричі. Якщо ж документи видаються рідше, ніж раз на тиждень, то дозволяється на вимогу користувача перевезення їх до читального залу транспортом користувача або іншим транспортом за його рахунок у кількості, що забезпечить місячну потребу користувача у документах.

На прохання користувача у разі наявності технічної можливості замовлені документи за рішенням керівництва архіву можуть бути видані невідкладно як платна послуга.

3.11. Справи та документи, що перебувають у незадовільному стані, видаються користувачам, як правило, лише після проведення науково-технічного опрацювання, ремонту, реставрації, оправлення, консерваційно-профілактичного оброблення, створення страхових копій. Строк такого обмеження не може перевищувати одного року з дня замовлення.

У виключних випадках нетривале у часі ознайомлення з конкретною інформацію, що міститься в таких документах, здійснюється за погодженням з керівництвом архіву у присутності завідувача читального залу.

3.12. Підставою для відстрочки у видаванні користувачам документів НАФ є:

— установлення фондоутворювачем, власником, уповноваженою ними особою або правонаступником особливих умов ко-

ристування документами особового походження;
— необхідність науково-технічного опрацювання, поліпшення фізичного стану, перевіряння наявності документів;
— перебування документів у тимчасовому користуванні за межами архіву.

3.13. Користувачі документами НАФ мають право:
— користуватися в читальному залі архіву копіями документів з фондів користування, а у разі їх відсутності — оригіналами, якщо доступ до них не обмежено на підставах, визначених законом, а також відповідно до закону користуватися документами обмеженого доступу;
— отримувати від архівів довідки про відомості, що містяться в документах, доступ до яких не обмежено;
— отримувати за письмовою згодою керівництва архіву документи або їх копії в тимчасове користування за межами архіву;
— отримувати в працівників архіву консультації про зміст і місцезнаходження документів, зокрема, щодо документів, які зберігаються в інших архівах;
— виготовляти, у тому числі за допомогою технічних засобів, копії документів і витяги з них, якщо це не загрожує стану документів та не порушує авторських та суміжних прав, а також вимагати, щоб ці копії або витяги були засвідчені архівом;
— публікувати, оголошувати, цитувати та іншим чином відтворювати зміст документів НАФ з обов'язковим посиланням на місця їх зберігання і з дотриманням умов, передбачених законодавством;
— користуватися за погодженням з керівництвом архіву технічними засобами, що полегшують їх роботу з документами НАФ (мікрокалькулятор,комп'ютер, смартфон, диктофон, фотоапарат тощо), за умови, що вони не завдають шкоди документам НАФ і не заважають іншим користувачам;
— користуватися за погодженням з керівництвом архіву послугами перекладача та спеціаліста з копіювання документів образотворчого та графічного характеру, яких оформлюють як окремих користувачів;
— оскаржувати в порядку підлеглості або в судовому порядку дії посадових осіб архіву, що перешкоджають реалізації законних прав користувачів;
— вносити керівництву архіву пропозиції щодо поліпшення організації діяльності архіву та умов роботи з документами НАФ;
— у разі виявлення в архівних документах недостовірних відомостей про особу, вимагати від архіву долучення до цих документів письмового обґрунтованого спростування чи доповнення зазначених відомостей.

Особи з обмеженими фізичними можливостями мають право безоплатно отримувати додаткові послуги залежно від свого стану, спрямовані на забезпечення користування документами НАФ.

3.14. Обов'язки користувачів документів НАФ:
— вчасно інформувати працівників архіву в разі зміни анкетних даних під час роботи в архіві чи користування документами НАФ поза архівом;
— дотримуватися встановленого порядку користування документами НАФ, зокрема своєчасно виконувати законні вимоги працівників архіву, запобігати пошкодженню документів, не виносити їх із читального залу, не передавати іншим особам, які не несуть відповідальності за їх зберігання, не робити в них позначок та підкреслювань, не писати на аркушах паперу, розміщених безпосередньо на архівних документах; не заносити до архіву сторонніх архівних документів у будь-якому вигляді (їх копій) та видань без дозволу керівництва архіву; під час роботи з кіно-, відео-, фото-, фонодокументами, електронними документами та мікрокопіями дотримуватися вимог поводження з цими документами та апаратурою;
— забезпечувати збереженість і вчасне повернення документів НАФ, довідкового апарату, видань, наданих їм у користування, негайно інформувати працівників читального залу (керівництво архіву) про виявлені випадки пошкодження чи недостачі документів;
— заповнювати аркуш користування архівними документами (додаток 3);
— у разі копіювання документів НАФ власними технічними засобами погоджувати з керівництвом архіву технічні умови цього копіювання і безкоштовно передавати архіву один примірник кожної копії (як правило, у цифровому вигляді);

— не допускати перекручень або фальсифікацій використаних відомостей, що містяться в документах НАФ, а також порушень права інтелектуальної власності, розголошень персональних даних та іншої охоронюваної законом інформації;
— надавати архівам бібліографічну інформацію про видання, у яких використано інформацію архівних документів;
— не використовувати з комерційною метою відомості, що містяться в документах НАФ, без укладання відповідного договору з архівом.

4. Видавання документів НАФ працівникам архіву та в тимчасове користування за межами архіву

4.1. Документи НАФ видаються працівникам архіву на їх робочі місця для виконання службових завдань.

Строки і обсяги видавання документів для архівних робіт обумовлюються планами роботи і встановлюються керівництвом архіву.

Залучення для виконання службових завдань працівниками архіву архівних документів (їх копій) з інших архівних установ чи приватних архівних зібрань здійснюється за письмовим дозволом керівництва.

Працівники архіву, які отримують документи НАФ у користування на робочих місцях, зобов'язані виконувати обов'язки, зазначені у пункті 3.14 цього Порядку.

4.2. Як виняток, з огляду на особливості використання документної інформації (експонування на виставках, богослужіння, підготовка факсимільних видань, здійснення порівняльного джерелознавчого аналізу, судово-слідчі дії, інтенсивне термінове використання великого обсягу інформації з конкретною виробничою метою тощо) оригінали документів НАФ можуть видаватися у тимчасове користування за межами архіву.

Унікальні документи НАФ у тимчасове користування за межами архіву не видаються.

4.3. В офіційному запиті на адресу керівництва архіву користувач обґрунтовує необхідність надання документів НАФ у тимчасове користування, зазначає строк, на який бажано передати документи, а також дає гарантії забезпечення збереженості документів та їх вчасного повернення. Для прийняття рішення щодо можливості надання документів у користування за межами архіву керівництво архіву організовує перевірку працівниками архіву умов забезпечення збереженості документів у майбутнього користувача.

4.4. У разі згоди керівництва архіву на надання документів НАФ у тимчасове користування за межі архіву укладається договір архіву з користувачем. Видавання документів оформлюється актом (додаток 4).

4.5. Документи НАФ видаються для користування поза архівом, як правило, на строк, що не перевищує одного місяця.

Релігійним організаціям документи богослужбового характеру (предмети культу) можуть видаватися у тимчасове користування на строк, що не перевищує одного року, за умови проведення їх грошової оцінки, а також страхування одержувачем.

4.6. Подовження встановлених строків перебування документів НАФ у користуванні за межами архіву допускається в особливих випадках з дозволу керівництва архіву лише на підставі письмового звернення користувача з поясненням причин необхідності продовження користування виданими документами та перевіркою працівниками архіву за дорученням керівництва архіву їх наявності і дотримання нормативних умов зберігання.

4.7. Архів має право в будь-який час без попереднього повідомлення перевірити наявність і умови зберігання документів, виданих у користування за межами архіву.

5. Організація копіювання документів на замовлення користувача

5.1. На замовлення користувачів і відповідно до технічних можливостей та стану документів архіви виготовляють ксерокопії, мікрокопії, фотокопії, цифрові копії документів, а також копії кіно-, відео-, фото-, фонодокументів, які в них зберігаються.

5.2. Замовлення на копіювання документів НАФ оформлюється користувачем на бланку встановленого зразка і передається працівникові читального залу (додаток 5).

5.3. Копіювання архівом документів здійснюється після оплати вартості замовлення.

5.4. Копіювання документів особових фондів та фондів, для яких за розпорядженням фондоутворювача або власника встановлено особливі умови користування, провадиться відповідно до умов, установлених ними з урахуванням рекомендацій Державної архівної служби України.

5.5. Строки та спосіб виготовлення копій визначаються керівництвом архіву за погодженням із замовником з урахуванням наявності відповідних технічних засобів і стану документів НАФ, але не можуть перевищувати одного місяця.

5.6. Копіювання фондів, колекцій у повному обсязі здійснюється лише у виключних випадках, з дозволу керівництва архіву та у разі, якщо для цього є спеціальні застереження фондоутворювачів.

5.7. Якщо користувач замовляє копії унікальних або особливо цінних документів НАФ за наявності їх мікрокопій або цифрових копій, то вони виготовляються лише з цих копій.

Не приймаються замовлення на копіювання документів НАФ у незадовільному стані або якщо копіювання наявними копіювальними засобами може спричинити погіршення стану документів.

5.8. Копії документів НАФ, виготовлені на замовлення користувачів, можуть бути видані їм або їх повноважним представникам в архівах або надіслані за вказаною адресою користувача. Поштові витрати відносять на рахунок замовників.

5.9. Винесення з архіву копій документів НАФ, виготовлених користувачем або на його замовлення, оформлюється спеціальною перепусткою за підписом керівництва архіву.

6. Відповідальність за порушення Порядку користування документами Національного архівного фонду України, що належать державі, територіальним громадам

6.1. Особи, винні в порушенні законодавства про Національний архівний фонд та архівні установи, несуть відповідальність за статтями 42 і 43 Закону України «Про Національний архівний фонд та архівні установи».

6.2. Спори, пов'язані з порушенням цього Порядку та відшкодуванням винною особою завданої шкоди, вирішуються в судовому порядку.

Додаток 1

ФОРМА ЗАЯВИ КОРИСТУВАЧА

«Видати читацький квиток»
Керівник архіву
Підпис Розшифрування підпису
Дата

_____

_____
(найменування посади і прізвище керівника архівної установи, якому адресується заява)

громадянина _____ (*країна*)_____ (ПІБ),
паспорт _____(*серія, номер, яким органом і коли виданий*), який постійно мешкає за адресою _____

ЗАЯВА

Прошу оформити мене як користувача документами НАФ, що зберігаються у _____ _____ (*назва архіву*).

З Порядком користування документами НАФ ознайомився(лась) і зобов'язуюсь його додержуватися.

Додатково повідомляю про себе такі відомості (*заповнюється на добровільних засадах для сприяння узагальненню статистичної інформації про користувачів документами НАФ і створення умов для покращання інформаційного обслуговування користувачів*)

Рік народження _____

Місце роботи, посада _____

_____

Освіта, науковий ступінь, учене звання _____

_____

Мета роботи _____

(підготовка статті, монографії, дисертації тощо)

Тема (теми) роботи, хронологічні межі _____
_____
_____
Використання документної інформації з комерційною метою _____ *(так, ні)*
Контактна інформація: _____
№ телефону _____ Факс _____ E-mail: _____

Дата Підпис _____

Додаток 2

ФОРМА ЗАМОВЛЕННЯ НА ВИДАВАННЯ СПРАВ

Найменування архівної установи
ЗАМОВЛЕННЯ

_____ № _____
на видавання справ до
читального залу

ДОЗВОЛЯЮ видавання справ
Керівник архіву
Підпис Розшифрування підпису
Дата

Прошу видати _____
(прізвище, ініціали і посада користувача)
такі справи:

Фонд №	Опис №	Справа №	Заголовок справи	Кількість аркушів	Підпис користувача	Підпис працівника читального залу
1	2	3	4	5	6	7

Підпис замовника Розшифрування підпису
Дата

Додаток 3

ФОРМИ АРКУШІВ КОРИСТУВАННЯ АРХІВНИМИ ДОКУМЕНТАМИ

Найменування архівної установи
АРКУШ КОРИСТУВАННЯ АРХІВНИМИ ДОКУМЕНТАМИ
Фонд № _____ Опис № _____ Справа № _____
Заголовок справи _____
_____

Дата користування	Прізвище, ініціали користувача	Характер користування (копіювання, перегляд, витяги тощо)	Номери аркушів, з яких зроблено копії, витяги тощо	Підпис користувача
1	2	3	4	5

Найменування архівної установи

АРКУШ КОРИСТУВАННЯ КІНО-, ВІДЕОДОКУМЕНТАМ

Одиниця обліку № _____ Рік виробництва_____

Дата користування	Користувач (організація або особа)	Мета користування	Примітка
1	2	3	4

Додаток 4
Найменування архівної установи

АКТ

_____ № _____
_____
(місце складання)

ВИДАВАННЯ СПРАВ У ТИМЧАСОВЕ КОРИСТУВАННЯ

_____
(прізвище, ім'я, по-батькові фізичної особи-користувача,
_____
найменування установи-користувача, їх поштова адреса)

Підстава_____
_____
З якою метою видаються справи _____
_____
Видаються такі справи з фонду _____
(назва фонду)

№ з/п	Опис №	Справа №	Заголовок справи	Крайні дати документів справи	Кількість аркушів справи	Примітки
1	2	3	4	5	6	7

Разом видаються _____ справ (загальною
(цифрами і літерами)
кількістю аркушів, часу звучання, метражем) _____ на термін до _____.

Справи видані в упорядкованому стані, оправлені в обкладинки, з пронумерованими аркушами й засвідчувальними написами.

Отримувач зобов'язується не надавати справи, отримані в тимчасове користування, стороннім особам, не видавати на їх підставі копій, витягів і довідок, не публікувати документи без дозволу архіву.

Отримувач зобов'язується повернути справи в термін, зазначений в акті.

Користувача попереджено про відповідальність за порушення законодавства про НАФ та архівні установи.

Видав справи
_____
(назва посади)
Підпис Розшифрування підпису
Дата
Керівник установи,
що видала справи
Підпис Розшифрування підпису
Дата
Печатка

Отримав справи
_____
Підпис Розшифрування підпису
Дата
Керівник установи,
що отримала справи
Підпис Розшифрування підпису
Дата
Печатка

Справи повернені в повному обсязі та збереженості

Прийняв справи
_____
(назва посади)
Підпис Розшифрування підпису
Дата

Здав справи
_____
Підпис Розшифрування підпису
Дата

Додаток 5

ЗРАЗОК ЗАМОВЛЕННЯ НА КОПІЮВАННЯ ДОКУМЕНТІВ

Найменування архівної установи

ЗАМОВЛЕННЯ

_____ № _____

ДОЗВОЛЯЮ
копіювання документів
Керівник архіву
Підпис
Розшифрування підпису
Дата

НА КОПІЮВАННЯ ДОКУМЕНТІВ

Прошу виготовити копії документів _____
(прізвище, ініціали користувача)
таких справ:

Фонд №	Опис №	Справа №	Номери аркушів*	Спосіб відтворення	Кількість негативів**	Розміри та кількість позитивів
1	2	3	4	5	6	7

* Слід обов'язково зазначати наявність зворотного боку аркушів, якщо вони підлягають копіюванню (напр., арк. 1 та зворот або арк. 4 та зворот). Якщо аркуші справи копіюються підряд, то потрібно зазначити, з якого до якого аркуша копіювати, не перераховуючи зворотів (напр., 1–10 та звороти).

** Необхідно підрахувати кількість аркушів, що підлягають копіюванню, з урахуванням їх зворотного боку.

Найменування та адреса установи (особи), яка оплачує замовлення

_____

«___»_____ 20___ р. _____
(підпис замовника)

Відмітка про оплату вартості замовлення _____

«___»_____ 20___ р. _____
(підпис бухгалтера)

Прийнято на копіювання «___» _____ 20___ р. _____
(підпис виконавця)

Виконано «___»_____ 20___ р.

Замовлення одержав «___» _____ 20___ р. _____
(підпис замовника, його повноважного представника або працівника архіву, якщо замовлення надіслане поштою)

СВіП у світі

СВіП друкує збірку матеріалів, присвячених балансу захисту національної безпеки у боротьбі з тероризмом і дотримання права на приватність в США.

НАМ НЕ ПОТРІБНИЙ СЕКРЕТНИЙ «КІБЕРСУД» ДЛЯ ХАКЕРІВ: ЧОМУ НЕДАВНЯ ПРОПОЗИЦІЯ КОМІСІЇ ГИЛМОРА ПОВИННА БУТИ ВІДХИЛЕНА

Аніта Рамасастрі

Середа, 24 жовтня 2001 року

Уявіть собі заголовки: «Кіберсуд приходить у наше місто». Звучить як назва науково-фантастичного роману? А, може бути, це — спин-офф телесеріалу «Темний ангел»? Або, може бути, новий фільм Арнольда Шварценеггера?

На жаль, ідея кіберсуду далека від фантастики й може стати реальністю — і незабаром. Минулого тижня урядова антитерористична комісія рекомендувала створити «кіберсуд» для судового переслідування хакерів. Ця рекомендація була прийнята, зокрема, у відповідь на теракти 11 вересня.

Губернатор Джеймс Гилмор (Вірджинія), голова комісії, стверджує, що причина створення нового суду полягає в тому, що наразі судді працюють недостатньо швидко, щоб забезпечувати правоохоронні органі ордерами при розслідуваннях онлайн-злочинів.

Однак замість пропозиції, аби федеральні й державні судді одержували більш професійну підготовку або більше ресурсів для прискорення видачі ордерів, Гилмор рекомендував створити новий «кіберсуд», який буде наділений спеціальними повноваженнями з проведення перевірок і нагляду, і робота якого, імовірно, вестиметься секретно.

Нам не потрібний новий «кіберсуд», і особливо нам не потрібно, щоб такий суд працював під завісою таємниці.

Захист кіберпростору — але не секретною «Зоряною палатою»

У прес-релізі, випущеному Комітетом з національної науки, Гилмор заявив: «Чи проявляється загроза у вигляді фізичних атак на комп'ютерне встаткування й апаратне забезпечення, що забезпечує Інтернет у країні, або у формі кібератак на програмне забезпечення комп'ютерів, кіберпростір Америки потребує захисту».

Зараз кіберпростір може потребувати захисту більш ніж будь-коли, але це не повинне відбуватися у форматі секретної «Зоряної палати». Комісія Гилмора надала деякі подробиці щодо так званого кіберсуду, але нам відомо , що суд функціонуватиме відповідно до Закону про контроль над зовнішньою розвідкою (Foreign Intelligence Surveillance Act — FISA) — це буде секретний суд, побудований за принципом ротації суддів федеральних округів.

Суд FISA уже давно зазнає критики з боку правозахисних організацій через те, що це — секретний суд, що проводить слухання за закритими дверима. Він був створений для урядового контролю з метою контррозвідки. Суд FISA не дотримується традиційних прав на захист, передбачених Четвертою поправкою.

Судді FISA розглядають запити Міністерства юстиції щодо здійснення електронного спостереження над особами, які нібито являють собою загрозу для національної безпеки, і проведення обшуків. До сьогоднішнього дня, за винятком пари випадків, суд завжди задовольняв запити Міністерства юстиції.

Оскільки суд працює винятково секретно, відповідач може ніколи й не довідатися, що в його будинку проводився обшук, або що його телефон прослуховувався. Ордери на спостереження видаються, а причини, чому вони були видані, утаємничуються й зберігаються в таємниці від відповідача, за винятком випадків, коли йому вдається добитися розкриття цих причин. Це рідка й, по суті, майже нечувана подія.

Ще більш дивним є той факт, що докази, зібрані на підставі ордеру суду FISA, можуть бути використані при наступному кримінальному переслідуванні. Дійсно, особі, чиє приватне життя порушене, ніколи не повідомляється про проведення спостереження або обшук на підставі

ордера суду FISA до початку кримінального переслідування, якщо таке має місце. При такому переслідуванні неможливо добитися розкриття матеріалів, що стосуються видачі ордера судом FISA, оскільки вони є секретними, і тому немає можливості ефективно заперечити незаконно проведений обшук або прослуховування.

Процедури суду FISA не повинні бути перенесені в кіберсуд. Ці процедури є репресивними у своєму обмеженому контексті. І процедури суду FISA, імовірно, стануть ще гіршими: антитерористичне законодавство, що перебуває зараз на розгляді Конгресу, може привести до послаблення деяких з небагатьох механізмів захисту, включених в FISA.

Спеціалізовані суди не завжди потрібні

Ми хочемо також запитати, чи дійсно нам потрібний окремий «кіберсуд». Хоча ми критикуємо суддів за те, що вони не є фахівцями або експертами в різних областях, закон і суди витримали випробування часом.

Протягом століть суди мають справи з розвитком технологій — від створення залізниць до появи сучасних телекомунікацій, а тепер і поширення Інтернету. Судді можуть застосовувати існуючі правові норми до нових технологічних розробок. Четверта поправка досить гнучка, і судді можуть застосовувати її в справах, пов'язаних з такими різноманітними обладнаннями, як обладнання глобального супутникового позиціонування або інфрачервоні датчики тепла.

Не можна вважати спеціалізовані суди вирішенням усіх проблем. Хоча підпал є серйозним злочином, і розслідувати підпали важко й складно, ми не створюємо спеціальний суд для розгляду справ про підпали. Також ми не створюємо спеціальний суд для судового переслідування груп бойовиків, тих, хто відмиває гроші, або терористів.

Більшість кіберзлочинів можна розслідувати в рамках стандартних процедур

Губернатор Гилмор стверджує, що: «[а] Суд, що займається кіберзлочинами, може створити необхідну базу знань, щоб проводити відповідні слідчі заходи, забезпечуючи при цьому захист громадянських прав і свобод». Але якщо моделлю є суд FISA, як припускає законодавство, це просто невірно — громадянські свободи не будуть захищені.

Відмінності між типовими федеральними/місцевими судовими процедурами й процедурами суду FISA досить значні. Якщо ордер виданий федеральним судом або судом штату, а не судом FISA, рівень поваги до громадянських свобод набагато вище. При звичайному судочинстві, наприклад, відповідач, будинок якого піддався обшуку, або перемовини якого відслідковувалися (прослуховування або аудіозапис) у рамках ордеру, виданого звичайним уповноваженим органом, може одержати копію цього ордеру або копію запиту до суду на видачу ордеру. Відповідач також може заперечити проведення обшуку, якщо були допущені якінебудь порушення, наприклад, Четвертої поправки. Як вже було вище зазначено, процедури суду FISA дуже відрізняються.

Стандартна процедура повинна бути достатньою для багатьох видів кіберзлочинності. Наприклад, з урахуванням того, що суд буде органом, що санкціонує обшук і спостереження з єдиною метою кримінального переслідування (а не стримування або охорони громадського порядку), здається за розумне вимагати, аби уряд мав вагомі причини для одержання дозволу на моніторинг комп'ютерної діяльності підозрюваного.

Хакери — кібертерористи?

Але що робити у випадках, які стосуються національної безпеки, включаючи можливі терористичні акти? Щоб вирішувати такі питання, вже існує суд FISA. Таким чином, не потрібно продовжувати використовувати трагедію 11 вересня як виправдання для створення секретного кіберсуду. Питання на кшталт тих, які були породжені 11 вересня, можуть бути розглянуті існуючим судом FISA.

Хоча хакерство є серйозним злочином, не всі види хакерства є «кібертероризмом». Існує широкий спектр злочинної діяльності, яка підпадає під категорію «хакерства» — псування веб-сайтів за допомогою так званих «*script kiddies*» дуже далекі від широкомасштабних атак, спланованих ворогами з наміром дестабілізувати наш уряд.

Перші правопорушення можуть розглядатися державними й федеральними судами в межах звичайної процедури, а другі повинні розглядатися судом FISA. Знову ж, немає ніякої необхідності в новому, секретному суді, який би займався всіма питаннями кіберзлочинності.

Деякі проекти антитерористичного законодавства, які розглядаються в Конгресі, вклю-

чають довічне тюремне ув'язнення для хакерів. Довічний висновок повинний, як мінімум, стосуватися найбільш серйозних різновидів хакерства — тих, які можна прирівняти до тероризму.

За певних обставин, злам і знищення комп'ютерних мереж і інфраструктури можуть являти собою віртуальний акт тероризму, те саме, що фізичний саботаж, який відбувся 11 вересня. Важливо, однак, детально обговорити, які типи комп'ютерних злочинів заслуговують на більш серйозне покарання, а також що вважати «віртуальним тероризмом» або «кібертероризмом».

Губернатор Гилмор правий, закликаючи звернути пильну увагу на комп'ютерну безпеку в Сполучених Штатах, і застерігаючи нас від потенційної погрози кібертероризму. Але перш ніж ми створимо інший суд, ми повинні спочатку визначити масштаби проблеми, а потім провести роботу, щоб з'ясувати, чи можна використовувати існуючі інститути в даній ситуації.

ЧОМУ СУД FISA БУВ ПРАВИЙ, ВІДМОВИВШИ МІНІСТЕРСТВУ ЮСТИЦІЇ

Аніта Рамасастрі

Середа, 4 вересня 2002 року

Нещодавно адміністрація Буша одержала чутливий правовий удар у своїй війні проти тероризму. Удар був нанесений з несподіваної сторони: з боку секретного федерального суду, відповідального за розгляд запитів уряду на санкціонування спостереження за підозрюваними в тероризмі.

Цей суд, відомий як суд Закону про контроль над зовнішньою розвідкою (FISA), відмовився затвердити певні процедури, запропоновані Генеральним прокурором Ешкрофтом. Пішовши на безпрецедентний крок, у серпні цього року суд також привселюдно проголосив своє рішення. Дискусія почалася в травні, коли суд виразив своє невдоволення із приводу процедур, а також переконання, що ці процедури суперечать чинному федеральному законодавству.

Процедура надала б прокурорам з кримінальних справ регулярний доступ до інформації, отриманої шляхом обшуків і прослуховування телефонних розмов у рамках контррозвідки, без достатніх підстав, що підтверджують, що злочин був або незабаром буде скоєний. (Контррозвідка, за визначенням FISA, — це збір інформації й заходи, здійснювані для захисту від шпигунства, іншої розвідувальної діяльності, саботажу, вбивств, зроблених іноземною державою або від її імені, іноземною організацією або іноземцем, а також міжнародної терористичної діяльності).

Відхиляючи ці процедури, суд FISA ухвалив, що вони дадуть прокурорам занадто великий контроль над контррозвідувальними розслідуваннями, а також дозволять використовувати розвідувальну інформацію в кримінальних справах.

Рішення суду FISA було абсолютно вірним, і, у розпал стрімкого розширення повноважень виконавчої влади, похвально, що судова система в цьому випадку зробила правильно. Традиційний розподіл контррозвідки й органів кримінального розслідування має бути збережений, за винятком випадків, коли Конгрес надає Міністерству юстиції чітку вказівку зневажити цим розподілом, чого він ще не робив.

Наразі ця справа розглядається апеляційним судом FISA, що складається з трьох спеціальних суддів, що переглядають рішення суду. Ця апеляція є першим офіційним оскарженням рішення суду FISA за всю його 23-річну історію. Апеляційний суд повинен залишити це рішення у силі.

У Сполучених Штатах контррозвідка й традиційне кримінальне слідство розглядаються як окремі й різні процеси, починаючи з кінця 1970-х. Стеження за шпигуном і спроба піймати злодія — абсолютно різні речі. Процедури, запропоновані Міністерством юстиції, можуть покінчити із цим важливим поділом.

Нещодавно суд FISA озвучив свою думку, що «уряд не робить секрету із цієї політики, наполягаючи на своєму тлумаченні нових поправок до Закону, які «дозволять використовувати FISA головним чином для правоохоронних цілей».

У березні 2002 року в меморандумі Федеральному бюро розслідувань Генеральний прокурор Ешкрофт описав нові процедури передачі прокурорам з кримінальних справ інформації, зібраної в рамках контррозвідувальної діяльності ФБР.

Запропоновані в 2002 році процедури дозволяють проводити широкомасштабні консультації між ФБР і прокурорами з кримінальних справ з метою координації зусиль для розслідування або захисту від «фактичного або потенційного напа-

ду, диверсії, міжнародного тероризму й таємної розвідувальної діяльності з боку іноземних держав і їх агентів...»

Ці процедури включають три основні положення, спрямованих на надання прокурорам з кримінальних справ більш широкого доступу до інформації контррозвідки. По-перше, положення про «поширення інформації» надасть прокурорам з кримінальних справ доступ до всієї інформації, отриманої в ході контррозвідувальних розслідувань ФБР, у тому числі інформації, отриманої в рамках FISA.

По-друге, положення, що стосується «консультацій», дозволить прокурорам консультуватися з розвідкою щодо стратегії й цілей розслідування.

Третє положення дозволить прокурорам з кримінальних справ консультуватися з посадовими особами розвідки ФБР щодо початку, реалізації, продовження або розширення обшуків або спостереження в рамках FISA. Простіше говорячи, це дозволить прокурорам з кримінальних справ безпосередньо брати участь у розслідуваннях контррозвідки. Замість того, щоб одержати традиційний ордер суду, прокурори з кримінальних справ зможуть одержати ту ж інформацію за допомогою процедур FISA. Зрештою, прокурори, по суті, матимуть можливість прямої контррозвідувальної діяльності.

Проблеми із процедурами

Уряд не обов'язково має зазначати підстави для подачі запиту на одержання спеціальних контррозвідувальних «ордерів» при проведенні традиційних кримінальних розслідувань. Небезпека розслідуваного злочину може бути вагомою причиною для видачі такого ордера. Навпаки, при розслідуванні звичайних злочинів слід уникати необґрунтованих обшуків і арештів. Цього вимагає Четверта поправка.

Пропоновані процедури, однак, дозволять ФБР обійти Четверту поправку. Якщо вони набудуть чинності, уряд зможе ділитися інформацією, зібраною згідно з нормами суду FISA, із правоохоронними органами й прокурорами, які, найчастіше, займаються звичайними злочинами. Це означає, що відомості, зібрані відповідно до правил, що стосуються терористів, можуть бути використані для осуду невдачливого магазинного злодюжки, який скористався телефоном посольства, щоб обговорити те, що він поцупив.

Збереження розподілу між контррозвідкою й кримінальним розслідуванням

Як я відзначала в попередній статті, суд FISA є таємною організацією — він діє в обстановці повної таємності, удалині від очей громадськості. Дійсно, до 11 вересня багато громадян не знали про його існування. Наразі суд складається з 11 суддів, призначуваних головним суддею Верховного суду США. До кінця серпня суд ніколи не публікував своїх рішень.

Закон FISA, прийнятий Конгресом в 1978 році в результаті пов'язаного із внутрішнім шпигунством скандалу в часи президентства Ніксона, увів окремі процедури для традиційних кримінальних розслідувань і для збору відомостей іноземною розвідкою. Навіщо потрібний такий розподіл? Конгрес уважає, що кримінальне розслідування дуже відрізняється від розслідування діяльності іноземних держав, покликаного захистити нашу національну безпеку. Отже, норми, що регулюють кожний вид розслідування, мають відрізнятися.

Спеціальні процедури FISA для збору контррозвідувальної інформації

Закон FISA встановив секретні процедури й створив секретний суд для розгляду запитів на прослуховування телефонів і проведення обшуків для спостереження за шпигунами, терористами й ворогами Сполучених Штатів. Ці процедури й суд призначали тільки для цілей контррозвідки, а не для звичайних кримінальних розслідувань.

Суд видає «ордера» FISA, але ці так звані «ордери», на відміну від традиційних ордерів у кримінальних справах, не вимагають вагомих доказів конкретної злочинної діяльності. Скоріше, це особливі ордери суду, призначені для використання з метою контррозвідки.

Суд FISA видає близько 1000 таких ордерів на рік, і тільки в рідких випадках він відхиляє запити на ордер. Особам, що є суб'єктами ордерів FISA, ніколи не відомо про це. Агент ФБР може проникнути в будинок підозрюваного, оглядітися й піти, не повідомивши, що він там був.

Що відбувається, якщо в результаті обшуку знайдені докази звичайних злочинів, що веде до кримінального переслідування? Суб'єктові може не повезти. Ордер і підстави, на яких він був виданий, можуть залишатися в таємниці, і, таким чином, не підлягають оскарженню, якщо

Генеральний прокурор дає клятву, що інформація повинна зберігатися в таємниці з міркувань національної безпеки.

Як «Патріотичний Акт» США розширив підстави для видачі ордерів FISA

Спочатку, до прийняття «Патріотичного Акту» США, що набув чинності після 11 вересня, правоохоронні органи могли намагатися одержати ордер FISA, тільки якщо основною метою проведення розслідування був збір розвідувальних даних. Але «Патріотичний Акт» США дозволив правоохоронним органам запитувати ордер FISA, якщо збір розвідувальних даних є важливою, але не обов'язково основною метою проведення розслідування.

Хоча таке розширення може здатися суперечливим, Конгрес затвердив його. Але Ешкрофт, без схвалення Конгресу, вжив заходів для ще більшого розширення використання ордерів FISA, дозволивши передавати докази, зібрані на підставі ордерів FISA, правоохоронним органам, що займаються кримінальними розслідуваннями, і навіть дозволивши таким правоохоронним органам брати безпосередню участь у зборі інформації.

Сьогодні суд FISA зазвичай схвалює створення інформаційних «екранів» між розвідкою ФБР і прокурорами з кримінальних справ у випадках, коли дії кримінального слідства й розвідки дублюються. Процедури Міністерства юстиції, як представляється, спрямовані на ліквідацію цих «екранів».

17 травня суд FISA ухвалив, що дана пропозиція неприпустима відповідно до чинного федерального законодавства. Постанова була підписана попереднім головою суду, окружним суддею Ройсом С. Ламбертом. Видане воно було вже новим головою, окружним суддею Коллином Коллар-Котеллі.

У Постанові було зазначено, що пропоновані процедури суперечать закону FISA, оскільки, згідно з рішенням Конгресу, FISA повинен розділяти збір доказів для контррозвідки й збір доказів для звичайного кримінального розслідування. Постанова також указувала, що, навіть без цих процедур, Міністерство юстиції при адміністраціях Клінтона й Буша вже ігнорувало поділ між контррозвідкою й поліцією.

Відповідно до показань свідків в суді, як було зазначено у постанові, Міністерство юстиції неправильно використовувало процедури FISA і вводило суд в оману щонайменше десяток разів. Міністерство юстиції й ФБР надавали суду неправильну інформацію в більш ніж 75 запитах на ордер на обшук і прослуховування, у тому числі один з таких запитів був підписаний тодішнім директором ФБР Луїсом Фри.

Суд також указав на докази того, що влада, щонайменше чотири рази, неправомірно передавала розвідувальну інформацію агентам і прокурорам, що розслідують кримінальні справи в Нью-Йорку. (Міністерство виявляє порушення й повідомляє про них суду FISA з 2000 року.)

Крім того, суд відзначив, що під час правління Клінтона в «тривожній кількості випадків» ФБР, очевидно, діяло неправильно. У ряді випадків, ФБР і Міністерство юстиції робили «помилкові заяви» у запитах на прослуховування «про дії, що дублюються, розвідки й слідчих з кримінальних справ і несанкціонованому обміні інформацією, що підпадає під закон FISA, між ФБР і кримінальними слідчими й прокурорами».

Суд заявив, що спостерігалася «тривожна кількість неточних показань ФБР у багатьох заявах до суду FISA», а також порушень судових наказів. Неточності й порушення виявлялися «практично у всіх випадках», що стосуються «обміну інформацією і її несанкціонованої передачі кримінальним слідчим і прокурорам».

«Судом не з'ясовано, як відбувалися ці порушення», говориться в постанові, що звучить трохи зловісно. Відхиляючи деякі частини нової процедури, суд також ухвалив, що співробітники правоохоронних органів не можуть давати поради, пов'язані зі спостереженням, слідчим, що проводять обшук або прослуховування. (Згідно з березневим меморандумом Ешкрофта, консультації або обмін інформацією можуть містити в собі обмін порадами й настановами про те, як робити спостереження й обшук.)

Аргументи, які адміністрація висуватиме в апеляційному суді FISA

Навіть якщо закон FISA призначений для поділу контррозвідки й звичайного карного розслідування, «Патріотичний Акт» США розмив цю грань, заявить адміністрація. Насправді, однак, закон FISA зовсім виразно говорить про поділ, а «Патріотичний Акт» США не містить прямого або непрямого скасування цього поділу.

Необхідна однозначна заява Конгресу, особливо якщо обговорюється введення практики,

яка завдасть серйознішої шкоди правам, передбаченим Четвертою поправкою. Дозвіл вільно передавати інформацію, зібрану в ім'я національної безпеки, прокурорам — це саме те, чого закон FISA повинен запобігати. Конгрес ще не здався, і, на щастя, суд FISA теж.

Чому ці питання видачі ордерів FISA не стосуються справи Муссауі

З моменту свого створення й до нинішнього конфлікту суд FISA погоджував усі, крім одного, запити на ордер, подані урядом. Проте, керівництво ФБР і представники Міністерства юстиції стверджують, що попередній конфлікт із судом FISA змусив уряд бути більш обережним при запиті ордерів FISA.

За даними уряду, за рік до арешту Закаріаса Муссауі судді суду FISA скаржилися, що вони були введені в оману ФБР, що просив санкціонувати спостереження за «Хамас», групою палестинських бойовиків. У результаті скарги Міністерство юстиції початоло внутрішнє розслідування поведінки старших офіцерів ФБР і Міністерства юстиції.

Одним з наслідків скандалу, заявило ФБР, стало його небажання запитувати ордер FISA на перевірку комп'ютера й інших речей Муссауі — тепер нібито «двадцятого угонщика» і члена Аль-Каїди. У серпні 2000 року Муссауі був заарештований у Міннесоті, але його справа не була повністю розслідувана.

Важливо підкреслити, однак, що ці два питання — чи повинні нові процедури бути затверджені, і чому ФБР не повністю розслідувала справу Муссауі — варто розглядати окремо. Міністерство юстиції й ФБР повинні усунути існуючі проблеми, пов'язані із процедурою одержання ордерів, а не створювати нові.

Діючи таким чином, вони неминуче знову потраплять у замкнене коло, спочатку викликаючи невдоволення суду FISA викривленням фактів, а потім проявляючи обережність при звертанні до суду для одержання ордерів. Перед тим, як намагатися ще більш розширити свої повноваження в рамках FISA, Міністерство юстиції й ФБР повинні навести порядок у своєму будинку — говорити суду тільки правду, щоб з достатньою впевненістю звертатися до суду, коли їм потрібний ордер.

Знову ж, нові процедури — це окреме питання, і постанова суду FISA щодо них було правильним. Конгрес може одного разу прийняти рішення щодо зміни існуючого закону, дозволивши регулярне співробітництво між контррозвідкою й органами кримінального розслідування. Але, незважаючи на всі законодавчі акти, прийняті після 11 вересня, Конгрес ще не зробив цього. Ухвалювати рішення, робити це чи ні, повинен, зрештою, Конгрес, а не Джон Ешкрофт, як справедливо ухвалив суд FISA.

АПЕЛЯЦІЙНИЙ СУД ЗАКОНУ ПРО КОНТРОЛЬ НАД ЗОВНІШНЬОЮ РОЗВІДКОЮ СТВОРЮЄ МОЖЛИВІСТЬ ЗНЕВАЖИТИ ПРАВАМИ, ПЕРЕДБАЧЕНИМИ ЧЕТВЕРТОЮ ПОПРАВКОЮ, У ДЕЯКИХ ВИПАДКАХ ПРОСЛУХОВУВАННЯ В МЕЖАХ КРИМІНАЛЬНОГО РОЗСЛІДУВАННЯ

Аніта Рамасастрі

Вівторок, 26 листопада 2002 року

Нещодавно апеляційний суд Закону про контроль над зовнішньою розвідкою (FISA), уперше у своїй історії, опублікував свою постанову. Ця постанова значно полегшить органам кримінального розслідування можливість одержання доказів у випадках, коли особа підозрюється в шпигунстві або участі в тероризмі, без необхідності надання суду традиційних «достатніх підстав».

У нинішній обстановці цілком виправданого страху перед тероризмом це може звучати дуже добре — принаймні, на перший погляд. Але насправді наслідки для прав, передбачених Четвертою поправкою, і для приватного життя людей у цілому, викликають тривогу. Загалом, ця постанова говорить, що за певних обставин «імовірними чинниками», на яких ґрунтується Четверта поправка, можна зневажити, навіть якщо докази будуть використані в кримінальному суді.

Враховуючи цей факт, апеляційний суд повинен утриматися від прийняття цієї постанови, оскільки вона сприяє зловживанням. Зокрема, вона дозволить ФБР працювати в тандемі

з місцевими органами кримінального розслідування, ігноруючи Четверту поправку.

Звісно, апеляційний суд FISA, принаймні, ретельно обмежив застосування своєї постанови. Він дав зрозуміти, що уряд може «порушувати межу» між ФБР і місцевими органами кримінального розслідування тільки стосовно злочинів, пов'язаних із зовнішньою розвідкою, а не для звичайних, побутових злочинів. Як відзначив апеляційний суд, «процедури FISA не можуть використовуватися як інструмент для розслідування абсолютно непов'язаних звичайних злочинів».

Але як щодо слабко пов'язаних звичайних злочинів? Чи зможуть правоохоронні органи обійти Четверту поправку в таких випадках?

Постанова дозволить Міністерству юстиції ігнорувати вимоги Четвертої поправки для того, щоб підслуховувати наші телефонні розмови, читати нашу електронну пошту або проводити обшуки в наших будинках, не повідомляючи нас про спостереження. Яким чином? Шляхом проведення розслідувань через суд FISA, а не через кримінальний суд.

Чому має існувати відмінність між збором інформації зовнішньою розвідкою й збором доказів з кримінальних справ? Через цілі, для яких ці відомості використовуються.

Коли громадянин може бути позбавлений волі, Четверта поправка й Конституція США дають надійні гарантії проти втручання з боку урядових органів.

Суд FISA і Апеляційний суд FISA

Закон про контроль над зовнішньою розвідкою (FISA) наразі розглядає запити урядових органів на видачу ордерів у випадках, приблизно пов'язаних зі шпигунством або терористичною діяльністю. У травні минулого року сім членів суду FISA оприлюднили своє перше рішення, відхиливши прохання уряду про розширення наглядових повноважень.

Суд FISA відзначив, зокрема, що Міністерство юстиції допустило безліч помилок і неточностей стосовно обміну розвідувальною інформацією із правоохоронними органами без дотримання необхідних гарантій.

Суд FISA також відхилив нові процедури, запропоновані Генеральним прокурором Ешкрофтом і спрямовані на усунення процедурних бар'єрів між ФБР і органами кримінального розслідування. Апеляційний суд FISA переглядає рішення суду FISA із правом скасовувати його рішення. Він складається із трьох напіввідставлених федеральних апеляційних суддів. Як відзначалося вище, це був його перший досвід роботи.

При розгляді апеляції апеляційний суд заслуховує тільки аргументи виконавчих органів, а не суб'єкта розслідування. Як наслідок, його робота, по своїй суті, є однобічною. У цьому випадку, однак, апеляційний суд дозволив декільком відомим правозахисним організаціям, у тому числі Американському союзу громадянських свобод і Центру за демократію й технології, надати «зовнішні» (*amicus*) короткі аргументи проти тлумачення законів урядом.

Значна зміна законів про прослуховування після 11 вересня

Більшості людей відомо, що таке стандартні «достатні підстави» для звичайного прослуховування; вони вимагають від уряду пред'явити достатні підстави, які дозволяють вважати, що людина робить, зробила або збирається вчинити злочин.

Як відзначено в зовнішніх аргументах, цей стандарт (втілений у федеральному законі про прослуховування, розділ III) традиційно застосовується навіть у випадку злочинів, пов'язаних з національною безпекою й тероризмом. Менш відомо, однак, що зараз застосовуються зовсім інші, менш суворі стандарти, коли уряд вважає, що особа є шпигуном або бере участь у терористичній діяльності, пов'язаною з іншою державою, і прагне зібрати відповідну розвідувальну інформацію.

Завдяки «Патріотичному Акту» США, прийнятому після 11 вересня, ФБР тепер може одержати ордер на прослуховування, якщо задовольняються дві ключові умови. (Крім того, урядовий орган повинен підтвердити, що він не може одержати відповідну інформацію іншими засобами, але тільки уряд вирішує, чи потрібне це підтвердження.)

Перше зі згаданих умов — «імовірна причина», але, що важливо, не звичайна «імовірна причина». Припущення, що «суб'єкт електронного спостереження є агентом іноземної держави», буде вважатися «імовірною причиною». Так, наприклад, достатньою ймовірною причиною буде припущення, що «суб'єкт є іракським шпигуном». Для одержання дозволу на прослуховування не обов'язково доводити, що особа, підозрювана в шпигунстві, робить, або навіть планує робити що-небудь протизаконне.

По-друге, «значною» метою розслідування повинна бути зовнішня розвідка. Таким чином, розслідування діяльності іракського шпигуна не повинне проводитися, наприклад, з метою розслідування підозр у порушенні ним правил паркування або використанні ним послуг проституток. Раніше зовнішня розвідка повинна була бути «головною метою» розслідування. Тепер вимога обмежується тільки «значною метою». Іншою метою — по суті навіть «основною метою» — тепер може бути не збір інформації, що стосується діяльності іноземної розвідки, а збір доказів для кримінального переслідування, пов'язаного з діяльністю іноземної розвідки.

Рішення апеляційного суду FISA щодо прослуховування й міжвідомчого співробітництва

На думку Суду, було б чудово, якби два розслідування поєднувалися в деяких випадках, і разом регулювалися несуворими, багатозначними стандартами прослуховування, про які йшлося вище. Крім того, було б добре, як запропонував Ешкрофт у своєму меморандумі в березні 2002 року, послабити процедурні обмеження, що регулюють, як і коли правоохоронні органі й відділ національної безпеки ФБР можуть обмінюватися інформацією й проводити розслідування.

Згідно з меморандумом Ешкрофта, прокурори з кримінальних справ можуть тепер мати доступ до всієї інформації, отриманої в ході контррозвідувальних розслідувань ФБР. Це включає, серед іншого, інформацію, зібрану в рамках процедур FISA, які не відповідають Четвертій поправці.

Прокурори можуть також проводити консультації стосовно «усіх питань, необхідних для проведення розслідувань або захисту від нападу ззовні...» Крім того, вони можуть надавати поради контррозвідці ФБР щодо початку, здійснення й продовження обшуків і спостереження в межах FISA.

Нарешті, апеляційний суд окремо ухвалив, що нові, знижені стандарти одержання ордера в межах процедур FISA не порушують передбачених Четвертою поправкою прав на захист від необґрунтованого «обшуку й арешту», враховуючи важливі інтереси уряду в сфері національної безпеки.

У підтримку своєї постанови, апеляційний суд послався на справу *Сполучені Штати проти Окружного суду Сполучених Штатів (Кит)*. У цій справі Верховний суд США визнав, що менш суворі стандарти, які стосуються обшуку й арешту, можуть бути придатні для справ, пов'язаних з національною безпекою. Але він також дав зрозуміти, що менш суворі стандарти припустимі тільки стосовно збору інформації, пов'язаної з контррозвідкою, а не тоді, коли уряд «намагається зібрати докази по конкретній кримінальній справі».

Отже, Кит не вважає, що правила збору інформації, пов'язані із зовнішньою розвідкою, можуть використовуватися, якщо основна мета полягає в кримінальному переслідуванні; більше того, він заявив прямо протилежне.

Крім того, перед справою FISA Апеляційний суд США в четвертому окрузі розглядав справу *Сполучені Штати проти Труонг*. Суд аналогічно й переконливо довів, що національна безпека й кримінальне переслідування — дуже різні речі. Інтереси національної безпеки відступають, а питання особистої конфіденційності виходять на передній план, проголосив суд у справі *Труонг*, коли «уряд у першу чергу намагається одержати підстави для кримінального переслідування», а не для збору розвідувальної інформації.

Реакція апеляційного суду в цьому випадку викликала розчарування, якщо не сказати більше. Суд заявив, що дуже важко провести межу між збором розвідувальних даних і кримінальним переслідуванням.

Це може бути правильним принаймні в деяких випадках, але це ще не причина відмовлятися від ідеї в цілому, особливо коли альтернативою є зневага основними гарантіями Четвертої поправки. Коли важко провести межу, суд повинен схилятися на користь захисту прав особистості відповідно до Четвертої поправки.

Результатом є те, що зараз органи кримінального розслідування можуть на законній підставі направляти, або, принаймні, значно впливати на розслідування ФБР, пов'язані із зовнішньою розвідкою. Дійсно, для цього є серйозний стимул: робота із ФБР буде означати можливість обійти вимоги, засновані на Четвертій поправці.

Крім того, що ця тенденція тривожна сама по собі, вона означає, що масштаби електронного спостереження, імовірно, збільшуватимуться. Принаймні, воно стане більш доступним, і в той же час більш корисним для державних органів.

Оскільки одержати так званий ордер FISA стане легше, правоохоронні органі зможуть збільшити кількість людей, за якими ведеться спостереження з метою збору даних і інформа-

ції. Правоохоронні органи зможуть також, користуючись можливістю, що з'явилася, використовувати цю процедуру для спостереження над більш широкими категоріями осіб від імені контррозвідки.

Суб'єкти розслідувань у межах FISA не будуть повідомлятися про таємні обшуки й спостереження. У випадку звичайного ордеру на обшук, правоохоронні органи повідомляють про це — або до, або після обшуку.

Якщо хто-небудь зазнає кримінального переслідування на підставі доказів, зібраних за допомогою ордеру FISA, запит правоохоронних органів на одержання ордеру може бути засекречений. Таке відбувається, якщо Генеральний прокурор упевнився, що це відповідає інтересам національної безпеки. Таким чином, обвинувачуваний не зможе заперечити підстави, на яких був виданий ордер.

Імовірна причина злочину вже не повинна буде викладатися правоохоронними органами при кримінальних розслідуваннях, пов'язаних із зовнішньою розвідкою. Докази, зібрані відповідно до цих розмитих стандартів, будуть вважатися припустимими в суді. Або, можливо, правоохоронні органи просто будуть використовувати ці розслідування для збору доказів, які ніколи не будуть пред'явлені суду, але будуть корисними для них.

По суті справи, апеляційний суд створив «зону, вільну від Четвертої поправки», якою може скористатися не тільки ФБР, але й інші правоохоронні органі. Поки розслідування проводяться з «істотною» (але не обов'язково «головною») метою зовнішньої розвідки, а самі злочини також пов'язуються із зовнішньою розвідкою, будуть існувати несуворі стандарти.

На початку цього року суд FISA відзначив, що, навіть коли так званий «бар'єр» існував, інформація просочувалася між ФБР і правоохоронними органами в багатьох випадках. Тепер, коли такий бар'єр необов'язковий, ситуація може тільки погіршитися.

Верховний суд США усе ще може переглянути постанову апеляційного суду FISA. Однак, оскільки Міністерство юстиції було єдиною «стороною» цієї апеляції, це представляється досить малоймовірним. Можна тільки сподіватися, що суд FISA сам стане більш пильним при розгляді запитів правоохоронних органів на ордери, пов'язані із зовнішньою розвідувальною діяльністю.

ЧОМУ НАС ТУРБУЄ ПРОЕКТ «ТОТАЛЬНЕ ВОЛОДІННЯ ІНФОРМАЦІЄЮ» І ІНШІ АНТИТЕРОРИСТИЧНІ СТРАТЕГІЇ ДЛЯ ІНТЕРНЕТ

Аніта Рамасастрі

Вівторок, 31 грудня 2002 року

В 2003 році ми, швидше за все, будемо спостерігати розвиток двох нових ініціатив уряду з використання комп'ютерних технологій для попередження тероризму. Кожна з них дасть уряду більш широкий доступ до даних у мережі Інтернет.

Одна з них стосується нового федерального центру моніторингу мережі, описаного в проекті Національної стратегії із забезпечення безпеки кіберпростору, запропонованому урядом у вересні. Друга стратегія, що нагадує фантазію Оруелла, передбачає створення Управління володіння інформацією, яке займатиметься проектом, спрямованим на «тотальне володіння інформацією». Обидві стратегії є причиною для занепокоєння.

Добре відомо, що терористи використовували — і, очевидно, усе ще використовують — Інтернет, тому що користуючись Інтернетом, можна зберігати анонімність при міжнародному спілкуванні. Крім того, уряд відзначив, що Dos-Атаки з боку терористів (або звичайних хакерів) являють собою потенційну загрозу для нашої національної інфраструктури.

Відповіддю уряду на той факт, що Інтернет може бути використаний для пособництва тероризму, стала спроба використовувати його для боротьби з тероризмом і попередження тероризму. Ідея полягає в зборі даних і виробленню стратегій, які зупинять терористів, перш ніж ті почнуть діяти. Якщо Інтернет може стати зброєю в руках наших ворогів, логічно припустити, що він також може стати засобом, який допоможе нашому уряду виявляти терористів і боротися з ними.

Навіть без нових ініціатив, деякі методи Інтернет-боротьби з тероризмом уже застосовуються. Агенти ФБР можуть звернутися до суду для одержання ордера на перегляд електронної пошти підозрюваного. Спираючись на «Патріотичний Акт» США, правоохоронні органи можуть, наприклад, попросити Інтернет-провай-

дера надати їм перелік своїх абонентів. Проте, дві нові пропозиції, впроваджені в повному обсязі, можуть просунути ситуацію значно далі.

Це викликає занепокоєння через три основні чинники. По-перше, нові пропозиції можуть викликати широкомасштабні порушення приватности в Інтернеті.

По-друге, вони також можуть дозволити урядовим органам обійти захист від необґрунтованих обшуків і арештів, передбачений Четвертою поправкою.

По-третє, їхня робота може бути зовсім даремною: залишається відкритим питання, чи дійсно створення глобальної бази даних про американців допоможе попередити терористичні атаки, і є вагомі підстави вважати, що не допоможе.

Національна стратегія із забезпечення безпеки кіберпростору й CNOC

По-перше, давайте розглянемо нинішній проект Національної стратегії по забезпеченню безпеки кіберпростору. Він створений Радою Президента із захисту критичної інфраструктури. Проект покликаний налагодити державне й приватне співробітництво з метою захисту національних комп'ютерних мереж від різних факторів, від шкідливих вірусів до терористичних атак. Кінцевий план, приблизно, зажадає ухвалення Конгресом.

Нинішній проект рекомендує, щоб постачальники послуг Інтернету (провайдери) і компанії, пов'язані з безпекою інформаційних технологій, зокрема, створили Центр управління мережею кіберпростору (CNOC). В Інтернеті налічуються тисячі провайдерів, від маленьких незалежних компаній до таких великих конгломератів, як AOL і Microsoft. Таким чином, трохи незрозуміло, як це зробити.

Стратегія передбачає, що CNOC, фізичний або віртуальний, «забезпечуватиме обмін інформацією й координацію для підтримки безпеки й надійності Інтернет-операцій у Сполучених Штатах». CNOC «не буде державним органом, і буде управлятися приватним сектором; федеральний уряд має вивчити яким шляхом він міг би співробітничати з CNOC».

Однак останні новини дають підстави припускати, що цей проект незабаром буде змінений таким чином, щоб CNOC управлявся урядом, а не приватним сектором. Також можна припустити, що Адміністрація незабаром зможе просити провайдерів надати федеральному уряду прямий доступ до безлічі даних для запобігання терористичних кібератак.

Мета — моніторинг мереж для запобігання майбутніх кібератак — представляється розумною й похвальною. Але проблема полягає в тому, що CNOC, керований державою, надасть уряду можливість відслідковувати індивідуальне використання Всесвітньої павутини, що несе потенційну загрозу недоторканності приватного життя.

Коли втручання підпадає під дію Четвертої поправки?

З юридичної точки зору, залишається неясним момент, коли широкомасштабне втручання уряду стає індивідуалізованим спостереженням (у цьому випадку, мова йде про електронне спостереження), до якого застосовується Четверта поправка. Ця область права, на жаль, усе ще залишається білою плямою.

Сьогодні, коли федеральний уряд прагне контролювати електронну пошту, використовуючи обладнання Інтернет-спостереження, відоме як «Carnivore», воно має одержати судовий ордер. Деякі коментатори розглядають CNOC як «мега-Carnivore»: внаслідок створення CNOC уряд одержить у набагато більшому масштабі доступ до Інтернет-каналів. Але тепер уряд зможе зайняти таку позицію, що ордеру суду не потребуватиме.

Окрім того, якщо CNOC дійсно є двостороннім державно-приватним партнерством, як передбачає поточний проект Національної стратегії, уряд може спробувати скористатися федеральним законом, що дозволяють приватний моніторинг електронної пошти без санкції суду в деяких ситуаціях. Тобто, він може попросити своїх приватних партнерів поділитися інформацією, яку вони законно контролюють у приватному порядку. (У попередній статті я описала, яким чином Міністерство юстиції Ешкрофта вже використовує аналогічну стратегію, коли справа стосується спостереження).

Дотепер адміністрація Буша намагалася розв'язати питання в цій царині, пов'язані з конфіденційністю. Наприклад, Річард Кларк, радник Президента з питань кіберпростору, нещодавно оприлюднив лист представників промисловості, де вони просять забезпечити відсутність прослуховування громадян урядом.

Це трохи утішає. Але остаточна доповідь Білого дому має бути більш певною, що стосується ролі уряду й промисловості в широкомасштабному моніторингу Інтернет-трафіка. Він також повинен більш ясно вказувати, що відбуватиметься у зв'язку з таким моніторингом, і пояснити, як не порушити Четверту поправку при спостереженні мережі.

Тотальне володіння інформацією: цифрове профілювання?

2003 року, на додаток до Національної стратегії й CNOC, ми також станемо свідками реалізації програми адміністрації Буша «Тотальне володіння інформацією» (Total Information Awareness — TIA). Програма буде реалізовуватися Управлінням володіння інформацією, що є частиною федерального Агентства перспективних оборонних досліджень (Defense Advanced Research Agency — DARPA).

Адмірал у відставці Джон Пойндекстер, радник з національної безпеки колишнього президента Рональда Рейгана, повернувся в Пентагон у лютому для того, щоб зайняти пост керівника Управління володіння інформацією й програми TIA. Первісні асигнування на програму TIA становлять близько 200 мільйонів доларів.

У нинішньому своєму вигляді, TIA може стати самим всебічним застосуванням технологій спостереження в історії США. Як така, вона являє собою безпрецедентну загрозу для громадянських свобод і конституційних прав.

TIA передбачає створення величезної централізованої національної бази даних, що містить інформацію, отриману з існуючих державних і комерційних банків даних. Зібрані й консолідовані матеріали будуть містити в собі банківську звітність, податкові декларації, дані про водійські посвідчення, покупки по кредитних картах, придбані авіаквитки і зброю, дозволи на роботу і багато іншого.

Що будуть робити із цією інформацією? Ідея полягає в тому, що терористи будуть відслідковуватися з використанням комп'ютерних алгоритмів для виявлення підозрілих моделей поведінки. Проблема, однак, полягає в тому, що ми не знаємо, хто може бути терористом.

Яке рішення пропонує Уряд? Просто стежити за кожним, щоб зрозуміти, чи можна визначити моделі поведінки, які допоможуть виявити терористів.

Однак для стеження за всіма людьми, інформація повинна бути прив'язана до конкретних осіб, або, принаймні, окремим «цифровим особистостям». Таким чином, хоча пропозиція про національні посвідчення особи було відкинуто, ми можемо одержати їхній комп'ютерний еквівалент.

У результаті, уряд одержить можливість суттєво контролювати наше життя — наші подорожі, наші операції тощо. Усе це буде робитися без ордеру суду. І це може призвести до знищення особистої конфіденційності.

Проблеми ефективності, справедливості й точності у зв'язку із програмою TIA

Оскільки в приватному секторі є безліч комп'ютерної інформації, збір даних урядом буде суттєво полегшений. І тепер він може використовуватися в набагато гірших цілях. Неточна інформація не стане причиною висилки вам не того каталогу або одержання дратівного спама. Вона може призвести до вашого помилкового арешту.

Це — досить тривожна ситуація, тому що багато відомостей є неточними. Наприклад, новим національним дослідженням Американської федерації споживачів було встановлено, що неточна й неповна інформація в кредитних споживчих звітах часто змушує їх платити більш високі відсотки по заставних.

Однак у нас є можливість виправити наші кредитні звіти й іншу споживчу інформацію, або поскаржитися на неточності. А як будуть обновлятися й виправлятися дані після того, як вони потраплять у базу даних TIA? Чи будуть ці неточності коли-небудь використані проти вас у випадку вашої спроби влаштуватись на державну службу або при перевірці благонадійності? Усі ці питання залишаються без відповіді.

Крім того, чи будуть дотримуватися обмеження при одержанні даних від приватних компаній? Раніше споживачі передавали свої дані компаніям, оскільки вони вважали, що ці дані використовуватимуться компанією в обмежених масштабах, на підставі заявленої політики конфіденційності. Чи буде уряд також дотримуватися цієї політики, або просто збиратиме дані незалежно від комерційної політики? Недобре збирати інформацію з певними обмеженнями, а потім порушувати ці обмеження.

У цілому, сліпа залежність від комп'ютерних даних може ввести в оману. Людина може підходити під ту саму модель поведінки з різних причин.

Наприклад, покупка авіаквитка в один бік була визнана підозрілою, оскільки терористи використовували такі квитки 11 вересня. Багато громадян США часто використовують квитки в один бік — нерідко по кілька разів протягом певного періоду часу. Людина може купити авіаквиток в один бік, тому що він переселяється в інше місто. Інша людина може бути комівояжером, який відвідує кілька місць, а не вертається безпосередньо в місто вильоту. Третя людина може просто скористатися спеціальною пропозицією авіакомпанії, або здійснити туристичну поїздку багатьма містами . Четвертий може бути студентом, можливо, арабо-американцем, який їде в коледж і планує купити новий квиток додому наприкінці навчального року. Жоден із цих людей не є порушником закону.

При зустрічі легко зрозуміти мотиви цих чотирьох людей, але їхню поведінку не можна змоделювати на підставі наявних даних. Більше того, дані можуть поверхово вказувати, що ці чотири людини — можливі підозрювані. Тим часом, справжній терорист не буде купувати авіаквиток в один бік, знаючи, що в такий спосіб він видасть себе. Він також не буде вчитися в американській школі влітку. Проте, будь-яка невинна людина, яка зробить це, може потрапити під підозру.

Терористи й інші злочинці часто вміють передбачити фактори, які правоохоронні органі будуть використовувати для їхнього виявлення, і обходять їх досить просто. Як швидко TIA експерти зможуть змінювати свої методи аналізу, щоб устигати за терористами?

Потенційний серйозний вплив TIA на Четверту поправку

Як я відзначила вище, TIA також піднімає питання, пов'язані із Четвертою поправкою. Дійсно, ця програма може створити проблеми для існуючої доктрини Четвертої поправки. Як правило, Четверта поправка не забороняє уряду використовувати доступну офіційну інформацію — від марки вашої машини до інформації, що хтось бачив, як ви продавали наркотики на розі, або дати вашого народження, повідомленої вами службі соціального забезпечення. Але ця інформація ніколи не піддавалась збору, централізації й всебічному аналізу, як припускає TIA.

З одного боку, виконання такого трудомісткого завдання, як аналіз паперових документів, сильно відрізняється від роботи з великою базою даних, яка може бути відсортована одним натисканням клавіші. Це може виглядати просто як підвищення ефективності роботи, яка вже виконується урядом. Але пам'ятайте також, що зібрана інформація буде тепер використовуватися в нових цілях — цілях, що дуже відрізняються від тих, задля яких її було спочатку зібрано.

Тобто, ви могли погодитися на перевірку зору або медичний огляд, знаючи, що інформація буде використовуватися для ухвалення рішення про одержання вами прав водія, і знаючи про існуючі обмеження. Але чи навряд ви погодитеся на те, щоб ваші медичні дані використовувалися в будь-яких цілях, у яких їх захочуть використовувати відповідні органи.

Коли уряд збирає величезну кількість наших особистих даних, систематизує й зберігає їх, чи не є це необґрунтованим обшуком і арештом?

Недостатність гарантій безпеки, звітності й конфіденційності програми TIA

До речі, як буде забезпечуватися безпека програми TIA? Урядові мережі, бази даних і вебсайти можуть бути так само вразливі, як і комерційні мережі. І якщо вся ця інформація зібрана воєдино, наслідки порушення безпеки будуть дійсно важкими.

Хто буде контролювати TIA? Наразі, у програмі TIA не згадується нагляд і звітність перед Конгресом або будь-яким іншим державним органом. Конгрес повинен провести слухання по TIA перед тим, як програма розпочне свою роботу.

Сенатори Діана Файнштейн і Даніель Іноуе закликали до введення мораторію на витрати TIA, відзначивши, що Конгрес ніколи спеціально не санкціонував TIA. Це слушна ідея. Витрата коштів не повинна зробити TIA фактом, що відбувся, допоки Конгрес не матиме можливості виконати свої обов'язки перед громадськістю, ретельно вивчивши TIA і оцінивши його переваги.

Крім того, у випадку ухвалення рішення про подальшу реалізацію, незважаючи на шкоду, яку TIA може нанести конфіденційності, Конгрес повинен допомогти створити гарантії для мінімізації шкоди з боку TIA.

Конгрес ще може зупинити (або принаймні проаналізувати й переглянути) TIA, а також Стратегію національної безпеки й CNOC. І це саме те, що йому слід робити. Війна з тероризмом, звичайно, серйозне питання, і уряд повинний мати можливість координувати обмін інформацією, як передбачено положеннями «Патріотичного Акту» США й іншими нещодавно прийнятими законами. Але невже стеження за кожним громадянином і збір інформації про нього дійсно є ціною свободи? І якщо ми погодимося на таке широкомасштабне стеження, скільки свободи нам залишиться насправді?

ЧОМУ МИ ПОВИННІ БОЯТИСЯ ПРОГРАМИ «MATRIX». ПРОГРАМА «АНТИТЕРОРИСТИЧНИЙ ОБМІН ІНФОРМАЦІЄЮ МІЖ ШТАТАМИ» ЗАГРОЖУЄ ВІДРОДЖЕННЯМ ТОТАЛЬНОГО ВОЛОДІННЯ ІНФОРМАЦІЄЮ

Аніта Рамасастрі

Середа, 5 листопада 2003 року

30 жовтня 2003 року Американський союз громадянських свобод (American Civil Liberties Union — ACLU) подав одночасні запити штатам Коннектикут, Мічиган, Нью-Йорк, Огайо й Пенсільванія, із проханням повідомити інформацію про участь цих штатів у програмі «Matrix». (Офіційна назва програми — «Multistate Anti-Terrorism Information Exchange», «Антитерористичний обмін інформацією між штатами»). Крім згаданих вище п'яти штатів, у програмі беруть участь ще чотири штати — Алабама, Флорида, Джорджія і Юта.

Метою запитів ACLU було виявлення джерел інформації, на якій заснована програма «Matrix», з'ясування, хто має доступ до бази даних, і яким чином вона зараз використовується. Запити були подані відповідно до Закону про свободу інформації кожного штату. Раніше, у жовтні, ACLU намагався одержати аналогічну інформацію відповідно до Федеральної версії Закону про свободу інформації, і у Флориді, де почала працювати програма.

Що таке програма «Matrix», і чому ACLU так турбується із цього приводу? Цих двох питань я торкнуся в даній статті. Я також покажу, що читачі також повинні бути стурбовані.

Програма тотального володіння інформацією

У вересні минулого року Конгрес проголосував за закриття програми Пентагона «Тотальне володіння інформацією» (TIA). Як я вже писала в попередній статті, TIA дозволила б федеральному уряду збирати й поєднувати величезну кількість даних, які зараз зберігаються в державних і комерційних (тобто, для одержання прибутку) базах даних, з метою створення індивідуального профілю кожного з нас.

Програма TIA ґрунтувалася на переконанні, що компіляція максимально можливого обсягу інформації стосовно максимально можливої кількості людей у широкомасштабну базу даних допоможе боротися з терористичною діяльністю. Метод, називаний «інтелектуальним аналізом даних», полягає в можливості пошуку в базі даних інформації або типів інформації, які могли б ідентифікувати терористів.

Конгрес заслуговує на похвалу за закриття програми TIA. По-перше, Конгрес заборонив використання TIA проти американських громадян, у світлі проблем конфіденційності, а також виразив заклопотаність із приводу можливої помилкової ідентифікації невинних людей як терористів. Програма одержала нову назву — «Володіння терористичною інформацією». Потім Конгрес закрив і цю програму.

На жаль, ті ж методи інтелектуального аналізу даних, на яких ґрунтувалася TIA, з'явилися знову — цього разу у вигляді програми «Matrix».

Що таке програма «Matrix» і як вона працює

Програмою «Matrix» керує приватна корпорація Seisint Inc., Бока Ратон, Флорида, від імені спільної групи урядів штатів. Однак, програма, принаймні частково, фінансується з федерального бюджету, і, можливо, у майбутньому буде можливий федеральний доступ до неї.

Програма одержала 4 мільйони доларів від Міністерства юстиції. Було обіцяно ще 8 мільйонів доларів від Міністерства Національної Безпеки. Крім того, за останньою інформацією, співробітники програми «Matrix»

заявили, що вони розглядають можливість надання доступу ЦРУ.

Що ж робить програма «Matrix»? Згідно із заявами Конгресу й новинам, вона, як представляється, робить те ж, що робила б програма TIA, якби вона набула чинності: зв'язує уряд і комерційні бази даних для того, щоб дозволити місцевим і федеральним правоохоронним органам проводити детальний аналіз досьє конкретних осіб.

На сайті програми «Matrix» зазначається, що зібрані дані будуть містити записи про залучення до кримінальної відповідальності, водійські дані, записи про реєстрацію транспортних засобів, і безліч іншої офіційної інформації. Представники компанії відмовляються розкривати більш докладні відомості про характер і джерела даних. За повідомленнями ЗМІ, ці дані можуть також містити кредитну історію, фотографії із прав водія, записи про шлюби й розлучення, номера соціального страхування, дати народження, а також імена й адреси членів родини, сусідів і партнерів по бізнесу.

Крім того, немає ніякої гарантії, що категорії даних, які збираються в рамках програми «Matrix», не будуть і далі розширюватися. Інформація, що міститься сьогодні в комерційних базах даних, охоплює купівельну активність, передплату на журнали, історію доходів і працевлаштування, і багато чого іншого. Можливо, скоро нас можна буде профілювати на підставі того, що ми читаємо й купуємо, як ми живемо.

У своїй промові в Конгресі США законодавець із Флориди Паула Б. Докері розповіла, як працює програма «Matrix». Вона поєднує урядові записи й «комерційні дані» в «сховища даних». Потім інформація аналізується за допомогою «спеціалізованого програмного забезпечення» для виявлення «аномалій» методами «математичного аналізу». Якщо знайдена «аномалія», вона детально вивчається співробітниками, які шукають докази тероризму або інших злочинів.

Так само, як і у випадку TIA, ідея полягає в «інтелектуальному аналізі даних» — пошуку моделей (у тому числі так званих «аномалій»), які можуть виявити осіб, які є, можливо, причетними до терористичної або іншої злочинної діяльності. Але, як і в TIA, такого роду аналіз даних може виявитися неефективним, і має серйозні недоліки, включаючи завдання шкоди конфіденційності.

Чому «інтелектуальний аналіз даних» небезпечний

Прихильники інтелектуального аналізу даних стверджують, що він невинний, тому що це — просто швидкий спосіб збору даних, який вже застосовується. Вони відзначають, що співробітники поліції, і навіть приватні детективи, вже сьогодні можуть стежити за підозрюваними й збирати дані для складання профілю особистості. Інтелектуальний аналіз даних, говорять вони, це той же процес, тільки прискорений і автоматизований.

Насправді, однак, програма «Matrix» є настільки більш могутнім інструментом, ніж робота окремих детективів або співробітників правоохоронних органів, що таке порівняння є недоречним. «Matrix» дозволяє практично миттєво одержувати десятки документів, що стосуються звичайних американців. Таке одержання інформації можна здійснювати постійно й масово. Потерпілий не повинен йти до поліцейської дільниці, а клієнт не повинен йти до приватного детектива.

Одним натисканням клавіші уряд зможе одержати так багато інформації про нас, що зможе миттєво відновити наше повсякденне життя. Для цього не потрібно буде посилати по наших слідах детективів або встановлювати відеокамери, тому що всі наші пересування можна буде відновити за цими даними. Не потрібно буде шукати підозрюваних — під підозрою будуть усі.

Проте, прихильники інтелектуального аналізу даних говорять: «Чому ви заперечуєте, якщо вам нема чого приховувати? Чому вас турбує те, що ви під підозрою, якщо ви невинуваті?»

Але, як показала історія, цей аргумент підступний. Зрештою, якщо людині нема чого приховувати, чому вона повинна боротися за дотримання свого права на приватне життя, або права на захист від самообмови, або права на звертання до адвоката? Звісно, усе не так просто, і ці права відносяться до переліку найцінніших прав, викладених у Біллі про права.

Принцип презумпції невинуватості теж є фундаментальною частиною нашої системи. Більше того, цей принцип — один з основних американських принципів, який забезпечує, що уряд не турбуватиме людину, якщо немає вагомих підстав підозрювати її в правопорушеннях.

Незрозуміло, у яких випадках правоохоронні органі матимуть доступ до записів в «Matrix». Але, що ще більш важливо, на яких підставах

створюється електронне досьє на індивідуума? Наразі це питання також залишається відкритим.

Ризик визнання невинного підозрюваним

Навіть якщо не розглядати дуже серйозні питання конфіденційності, пов'язані із програмою «Matrix», залишається серйозний ризик так званих неправильних спрацьовувань. «Інформаційні аномалії» далекі від реальних показників винуватості.

Самі дані можуть бути помилковими. Кожний, хто коли-небудь намагався виправити помилковий кредитний звіт, міг побачити, що не так вже легко виправити помилку, якщо вона потрапила в систему. Однак немає жодних відомостей, як можна буде локалізувати й виправити помилку в базах даних «Matrix».

Крім того, дані можуть виглядати погано, але мати безневинне пояснення. Кажуть, що терористи часто переїжджають з місця на місце, мають кілька зафіксованих адрес. Але студенти, незаможні й бездомні, роблять те ж саме. Якщо вже на те пішло, так само живуть і мандрівні письменники.

Насправді, комп'ютери ні зараз, ні, швидше за все, у майбутньому, не зможуть робити висновки про наявність обґрунтованих підозр у злочинній діяльності — це можуть робити тільки люди.

Програма без гарантій являє собою особливу небезпеку

Крім усього іншого, програмі «Matrix» не вистачає гарантій у відношенні цих передбачуваних проблем. На сайті говориться: «Ця система забезпечуватиме, аби співробітники державних і місцевих правоохоронних органів — особи, які найчастіше зустрічаються з терористами й іншими злочинцями — мали кращий і більш оперативний доступ до інформації (точної й повної)». Незважаючи на обіцянку точності, програма не має системи корекції помилок, принаймні, наскільки це відомо громадськості. І незрозуміло, як буде забезпечуватися захист конфіденційності, якщо взагалі буде.

На сайті програми «Matrix» також йдеться, що «інформація, надана будь-яким штатом, може поширюватися тільки відповідно до обмежень і умов, визначених цим штатом, і відповідно до законів і правил цього штату». Але на сайті не описані відповідні положення різних штатів, і те, як ці положення будуть застосовуватися в «Matrix». Наприклад, що робити, якщо дані надходять із декількох штатів? Чи буде застосовуватися більш сувора політика конфіденційності? Або менш сувора?

Усі ці проблеми, пов'язані із програмою «Matrix», дуже серйозні. Можуть існувати й інші проблеми, яких ми поки не усвідомлюємо. Поки ACLU не одержить всеосяжні відповіді на свої запити (якщо взагалі одержить), ми не можемо із упевненістю сказати, які дані будуть збиратися, як така інформація буде використовуватися, і хто буде мати доступ до неї.

Питання прості, але відповіді на них можуть бути дуже важливі. Будемо сподіватися, що ACLU одержить відповіді на поставлені питання. І будемо сподіватися, що «Matrix» осягне та ж незавидна доля, що й TIA.

ACLU ПРОТИ АГЕНТСТВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ. ЧОМУ «ПРИВІЛЕЙ ДЕРЖАВНОЇ ТАЄМНИЦІ» НЕ ПОВИНЕН ПЕРЕШКОДЖАТИ ПОДАЧІ ПОЗОВІВ НА НЕСАНКЦІОНОВАНЕ ПРОСЛУХОВУВАННЯ ТЕЛЕФОННИХ РОЗМОВ АМЕРИКАНЦІВ

Джон Дін

П'ятниця, 16 червня 2006 року

Американський союз громадянських свобод (ACLU) є головним позивачем у федеральному суді, який вимагає, щоб Агентство національної безпеки (NSA) припинило регулярні порушення Закону про контроль над зовнішньою розвідкою (FISA) у зв'язку із програмою прослуховування телефонних розмов американців. ДО ACLU у якості позивачів приєдналась низка *адвокатів, учених, журналістів і інших осіб, які постраждали від програми*. Позивачі стверджують, що програма NSA порушує не тільки FISA, але також Першу й Четверту поправки до Конституції.

Уряд США, через адвокатів Міністерства юстиції, запекло намагався добитися відхилення даного позову, який наразі перебуває на розгляді в окружному суді США східного округу штату

Мічиган. Із цією метою адвокати Міністерства юстиції посилалися на «привілей державної таємниці», заявивши, по суті, що уряд не може пояснити свої дії, оскільки вони пов'язані з національною безпекою.

Адвокати Міністерства юстиції двічі успішно застосовували цю стратегію до перекладача ФБР *Сибел Едмондс*, щоб перешкодити їй свідчити про неналежні дії ФБР. Вони використовували її знову в справі *Махера Арара*, канадця, якого було затримано в аеропорті Кеннеді при поверненні з відпустки, і який був висланий у Сирію, де він зазнав катувань, перш ніж його відпустили у зв'язку з його невинуватістю. Ще раз вони використовували цю стратегію у випадку з *Халідом Ель-Масрі*, німецьким громадянином, помилково заарештованим і висланим в Афганістан, де його утримували під вартою, били й катували співробітники ЦРУ.

Але цього разу результат може бути зовсім іншим. Тому що це — той випадок, коли «привілей державної таємниці» явно не повинен застосовуватися, і суддя повинен мати досить сміливості, щоб прийняти таку постанову.

Дійсно, якщо суддя Ганна Диггс Тейлор прийме таке рішення, вона зможе зробити для Америки те, що Конгрес, контрольований GOP, і федеральні судді, контрольовані республіканцями, дотепер відмовлялися зробити: вона може зажадати від Адміністрації дотримувати закону, і в ході процесу вона зможе реально вивчити питання про обґрунтованість претензій уряду щодо «державної таємниці», а не просто покладатися на твердження, що справа стосується національної безпеки. Оскільки подібні претензії давно є предметом постійних зловживань, така експертиза вже давно назріла.

Позов ACLU проти NSA, і суддя, який його розглядатиме

Позов ACLU просто закликає NSA дотримуватися FISA, який Конгрес зробив єдиним інструментом, за допомогою якого виконавча влада може здійснювати електронне спостереження за американцями.

На відміну від тих суддів, які розглядали справи *Едмондс*, *Арара* й *Ель-Масрі*, суддя Тейлор, як доводить її біографія, має чітку уяву про громадянські права й свободи. Вона є здравомислячим суддею, з 25-річним досвідом роботи у федеральному суді. Вона викидала юристів із залів судових засідань, коли вони спеціально затягували процес (і в цих випадках Апеляційний суд її підтримував). Вона пише добре обґрунтовані думки, які демонструють глибоке співчуття жертвам порушень громадянських свобод. І вона, безумовно, не боїться, що її рішення будуть скасовані більш консервативним Апеляційним судом Шостого округу, який має юрисдикцію над її судом.

Коротше кажучи, якщо є федеральний суддя, здатний протистояти президентові Сполучених Штатів і сказати йому, що він повинен дотримуватися закону, здатний прорватися через нісенітницю, яка зазвичай оточує будь-які посилання на «привілей державної таємниці», то це — суддя Ганна Диггс Тейлор.

ACLU стверджує, що «представники адміністрації привселюдно визнали всі факти», необхідні для того, щоб суддя виніс рішення по законодавчих і конституційних вимогах позивачів. Відповідно, можна сподіватися на винесення часткового рішення за даною справою.

Адміністрація попросила про припинення справи у зв'язку із клопотанням, але, у наказі від 31 травня, суддя Тейлор відхилила прохання про припинення, і 10 червня заслухала усні аргументи. Має бути друге слухання, яке відбудеться 12 липня, за клопотанням адміністрації про припинення справи, оскільки воно стосується державної таємниці. Цілком імовірно, що суддя Тейлор винесе рішення за клопотанням ACLU і адміністрації лише через якийсь час після цього другого слухання, так що, імовірно, рішення слід очікувати наприкінці липня, в серпні або вересні.

Аргументи уряду на користь відмови від розгляду справи — вкрай непереконливі

Уряд надав два аргументи на користь відмови від розгляду справи:

По-перше, уряд стверджує, що позивачі не мають права на подачу позову, оскільки понесена ними шкода є спекулятивною — зрештою, вони не знають, чи перебували вони насправді під спостереженням чи ні.

NSA не повинне мати можливість скористатися атмосферою страху й невизначеності, яку воно створить, добившись відхилення позову на цій підставі, особливо тому, що саме через цей страх і невизначеність Перша поправка дозволяє подавати позов на підставі «ефекту сторожкості». Телефонна розмова репортера або вченого може сильно відрізнятися, коли

вона ведеться під страхом прослуховування, і при усвідомленні, що норми, викладені в законодавстві про прослуховування телефонних розмов, у цей час повністю ігноруються.

У зв'язку з цим адвокати Міністерства юстиції стверджують, що вони не можуть продемонструвати необґрунтованість позову, не ставлячи під загрозу національну безпеку. Але що саме вони мають на увазі? Невже Міністерство юстиції не бажає навіть заявити, що воно не здійснювало спостереження за позивачами? А навіщо йому робити таку заяву, якщо, як відзначалося вище, страх і почуття невизначеності позивачів є окремою підставою для подачі позову?

По-друге, уряд стверджує, що «привілей державної таємниці» не дозволяє йому роз'яснити, чому, програма NSA є, насправді, законною, оскільки це торкнеться питань, пов'язаних з національною безпекою. Але цей аргумент також непереконливий. У випадках, коли люди були помилково затримані й зазнали катувань, були хоч якісь, нехай і погано обґрунтовані аргументи; уряд міг стверджувати, принаймні, що його засоби з'ясування, кого слід затримати, є питанням національної безпеки. Тут, незважаючи на виданий адміністрацією 42-сторінковий документ, що проголошує законність програми NSA, важко уявити, що аргументи, пов'язані з «секретними міркуваннями національної безпеки» можуть зробити кричущо незаконні дії законними.

Державна таємниця: привілей, породжений в неправді

Некрасива історія виникнення «привілея державної таємниці» повинна змусити суддю Тейлор замислитися перед тем, як задовольнити клопотання Міністерства юстиції.

Привілей державної таємниці був уперше визнаний Верховним судом у рішенні 1953 року в справі *Сполучені Штати проти Рейнольдс*. Після загибелі трьох цивільних інженерів в аварії B-29 під час їх роботи на збройні сили, удови цих інженерів зажадали надати їм звіт про аварію й компенсувати збиток, заподіяний смертю їх чоловіків. Однак уряд відмовився надати звіт, стверджуючи, що місія була пов'язана з національною безпекою, і зробити це — означає розкрити таємницю, яка може завдати шкоди народу. Суд погодився з урядом і відхилив цей позов. Суддя підкреслив, що суд поставлений у важке положення: «Суд повинен визначити, чи є обставини прийнятними для заяви про привілей, але зробити це, не розкриваючи того, що ма захищати цей привілей».

Через п'ятдесят років після рішення у справі *Рейнольдс*, дочка одного із загиблих в аварії B-29, Джуді Лефер, виявила, займаючись серфінгом в Інтернеті, що уряд розсекретив звіт про аварію, не задавши собі клопоту повідомити її про це. За 63 долара вона придбала копію в приватній компанії. Із великим здивуванням вона довідалася зі звіту про аварію, що із цим випадком не була пов'язана ніяка державна таємниця; єдиною таємницею тут була груба недбалість із боку військових. Це був нещасний випадок, який не повинен був відбутися.

Після відкриття Лефер, адвокати, що брати участь у справі *Рейнольдс*, подали клопотання, підкресливши той факт, що уряд вдався до шахрайства у федеральному суді. Однак ані Міністерство юстиції, ані Верховний суд не побажали нічого слухати про це. Клопотання було відхилено.

Через усе більш широке використання «привілею державної таємниці», воно було більш уважно вивчене останніми роками. Наприклад, політологи Університету штату Техас Вільям Уівер і Роберт Палітто, вивчивши всі випадки, дійшли висновку, що «привілей державної таємниці застосовується на шкоду інтересам нашого конституційного ладу». Це зловживання, стверджують вони, відбувається тому, що «суди нерозумно уступають виконавчій владі в цьому питанні».

Як влучно сказав один оглядач, «привілей державної таємниці» було «породжено в неправді». Коли уряд починає говорити про «національну безпеку», федеральний суд відразу тушується. Однак кожному, хто працював у цій царині, відомо, що дуже рідко безпека нації дійсно поставлена на мапу, коли уряд заявляє, що це так. Як правило, міркування національної безпеки — усього лише містифікація.

Універсальний привід «національної безпеки». Справа про документи Пентагона

Жодний уряд не може працювати в повній ізоляції. І деяку інформацію дійсно потрібно тримати в секреті, щоб не допустити шкоди безпеці країни. Але такі випадки рідкі. Дуже, дуже рідкі.

Томас Блентон, виконавчий директор Національного архіву безпеки Університету Джорджа

Вашингтона, *недавно писав в «Лос-Анджелес таймс»* про надлишкове застосування засекречування урядом. Він відзначив, що нинішній помічник заступника по контррозвідці знехотя визнав у Конгресі, що принаймні половина всієї секретної інформації надлишково засекречена; голова Комісії 9/11 Том Кин сказав: «Три чверті секретних матеріалів, які я читав [при вивченні готовності уряду до терористичних атак] не повинні були бути засекречені»; виконавчий секретар президента Рейгана в Раді національної безпеки, капітан ВМФ Родні МакДениел, заявив, що тільки десять відсотків засекречених документів «дійсно призначені для охорони державних секретів». Капітан МакДениел занадто великодушний. За моїми спостереженнями, самим волаючим випадком використання урядом приводу національної безпеки є, напевно, справа про документи Пентагону, *Сполучені Штати проти «Нью-Йорк таймс»*.

Працюючи в той час радником президента, я спостерігав, як уряд домагався ухвалення рішення проти «Нью-Йорк таймс» і «Вашингтон пост», щоб запобігти подальшій публікації дослідження походження війни у В'єтнамі, добре знаючи, що жодному з урядових юристів, які брали участь у справі, не був відомий зміст цих документів.

Прокурор Південного округу Нью-Йорку вважав недоречним виступати за введення обмеження для преси (що є грубим порушенням Першої поправки), не знаючи причин. Я погодився й намагався з'ясувати, які можуть бути обґрунтування, для того, щоб домагатися цього надзвичайного заходу. Але Міністерство оборони відмовилося пояснити кому-небудь, що містили ці документи.

Генеральний прокурор є найповажнішим прихильником уряду, і його часто називають десятим членом Верховного суду через довіру, що надається його службі. Проте, Ірвін Грисуолд, колишній декан юридичного факультету Гарвардського університету, який був тоді Генеральним прокурором, не наполягав на розкритті фактичного змісту документів Пентагону, і він ніколи не знав про їхній зміст, навіть коли визнавав важливість збереження їх у таємниці.

Примітною є заява Грисуолда у Верховному суді в червні 1971 року: «Я не маю ані найменшого сумніву, що ті матеріали, які вже опубліковані, і публікація інших матеріалів вплинуть на американське життя, і це питання є вкрай серйозним».

Трьох суддів вдалося переконати, а шістьох — ні. Документи Пентагону були опубліковані, і Америка змогла сама прочитати їх і побачити, що вони не являють собою загрозу для національної безпеки.

Звичайно, Грисуолда засудили за його менш ніж відвертий виступ у справі, пов'язаній з документами Пентагону, і через двадцять вісім років він привселюдно покаявся. 1989 року він писав у редакторській статті «Вашингтон пост»: «Я ніколи не бачив жодних ознак погрози для національної безпеки у зв'язку з публікацією [документів Пентагона]. Я ніколи навіть не припускав, що така реальна загроза мала місце... Будь-якій особі, що має значний досвід роботи з конфіденційними матеріалами, зрозуміло, що існує проблема масового надлишкового засекречування, і що чиновники, які засекречують різні документи, стурбовані, головним чином, не національною безпекою, а скоріше намагаються сховати помилки уряду або щось на кшталт цього». У цілому, є добре документована й багата історія зловживання урядом заявами про національну безпеку. Враховуючи цю історію, федеральні судді не повинні були трактувати сумніви на користь уряду.

Це правильно, що керівник органу виконавчої влади або відомства, пов'язаного із заявою про державну таємницю, повинен особисто свідчити з питань національної безпеки. Але якщо хтось вважає, що міністр оборони або директор національної розвідки має час або бажання вивчати всі документи, а також розглядати пов'язані із цим проблеми, він просто не розуміє, як працює уряд. Ці рішення, по суті, ухвалюються бюрократами (часто повністю самостійно).

Дилема, що стоїть перед суддею Анною Диггс Тейлор

Коли суддя Тейлор буде проводити 12 липня слухання за клопотанням Адміністрації про «привілеї державної таємниці» як підстави для відхилення позову, вона зіштовхнеться із класичною дилемою, що стоїть перед усіма федеральними суддями, які повинні ухвалювати рішення щодо приводу «привілею державної таємниці»: як суддя може знати, чи законні вимоги уряду?

ACLU вважає, що в цьому випадку заяви уряду порушують FISA, зокрема, з юридичної точки зору. Відповідно, посилання на привілей державної таємниці представляється скоріше

знаряддям нападу, ніж захисту — це спосіб позбутися справи без заперечування законності дій уряду.

Але парадоксальність привілею державної таємниці полягає в тому, що уряд може посилатися на неї, не вказуючи причин, і значна кількість федеральних суддів, і, як ми вже відзначали, урядові прокурори, ставляться до таких заяв з повагою, беручи до уваги конституційний поділ влади.

Однак виконавча влада не заслуговує на таку повагу. Генеральний прокурор Грисуолд був введений в оману бюрократами Міністерства оборони. Урядові чиновники неофіційно визнають, що не менше половини — якщо не дев'яносто відсотків — секретної інформації засекречені помилково. Проте, значна кількість федеральних суддів підтримують заяви виконавчої влади, коли вона посилається на національну безпеку. Їм не слід цього робити. Роблячи таким чином, вони, фактично, не виконують своєї ролі, як конституційно рівні виконавчій владі. Вони не перевіряють факти, і не намагаються знайти компроміс. Вони просто відходять убік.

Багато суддів, схоже, вважають, що вони повинні відійти убік, тому що вони не компетентні ухвалювати рішення стосовно питань національної безпеки. Правда полягає в тому, що, насправді, вони, імовірно, більш компетентні, ніж посадові особи органів виконавчої влади, які ухвалюють такі рішення. Судді мають досвід аналізу фактів і їх наслідків, і вони, безумовно, мають повноваження збирати необхідну інформацію. А федеральні судді, що довічно займають цей пост, які ні від кого не залежать і не бояться наслідків своїх дій, можуть бути набагато більш безсторонніми, ніж будь-який представник виконавчої влади. Не дивно, що представники виконавчої влади надмірно використовують таємність, тому що для них це — найбезпечніша лінія поведінки.

Томас Блентон відзначив у своїй статті, що «судді мають у своєму розпорядженні багато інструментів, щоб розслідувати й перевіряти претензії уряду», коли уряд посилається на привілей державної таємниці, у тому числі можуть призначити «спеціального експерта, що має досвід, і перевіреного органами безпеки». (Спеціальний експерт може бути призначений федеральним судом для надання суду звіту при виникненні складних фактичних питань.)

Наприклад, суддя Тейлор може призначити команду спеціальних експертів, таких як колишні співголови Комісії 9/11 Том Кин і Лі Гамильтон, для оцінки тверджень влади про те, що їм доведеться розкрити державні таємниці, щоб пояснити, чому позов не слід розглядати, і чому уряд насправді не порушив FISA — незважаючи на власні публічні визнання уряду, що це насправді так.

Таке рішення мало б зупинити зростаюче зловживання «привілеєм державної таємниці» президентом Бушем і віце-президентом Діком Чейні, які використовують цей привілей більш агресивно, ніж будь-яка адміністрація президента за всю історію США, і останнім часом усе частіше. Хоча точні цифри важко знайти (тому не про всі випадки повідомляється), останні дослідження показали, що «в 2001 році адміністрація Буша використовувала привілей державної таємниці в 23 випадках». Для порівняння, «між 1953 і 1976 роками уряд посилався на цей привілей тільки в чотирьох випадках».

Крайня важливість судового слухання справи

12 липня погляди нації мають бути звернуті до судді Анне Диггс Тейлор. Не буде перебільшенням сказати, що суддя Тейлор, багато в чому, буде ухвалювати рішення щодо долі нації. Ми балансуємо на лезі ножа.

Я згадую слова Мартіна Німеллера, капітана німецької субмарини, а пізніше лютеранського пастора й філософа, якому студент поставив запитання: «Як міг трапитися Холокост?» Наймюллер чудово пояснив, як люди упокорюються з несправедливістю, коли їм здається, що вони тут ні при чому: «Спочатку вони прийшли за комуністами, але я не був комуністом, і я мовчав. Потім вони прийшли за соціалістами й активістами профспілок, але я не відносився до них, і я мовчав. Потім вони прийшли за євреями, але я не був євреєм, і я мовчав. І коли вони прийшли за мною, нікому було заступитися за мене».

Чи вірні ці слова в контексті «державної таємниці»? Запитаєте Махера Арара й Халіда Ель-Масрі — їх катували помилково, незважаючи на відсутність провини з їхнього боку, а потім дозволили уряду уникнути відповідальності в суді на тій підставі, що помилки, які призвели до настільки жахливих страждань, є «державною таємницею». Сподіваємося, що суддя Анна Диггс Тейлор не буде мовчати — заради всіх нас.

У КОНТРОЛІ НАД NSA ПОВИНЕН БРАТИ УЧАСТЬ ВЕРХОВНИЙ СУД

Ендрю Коен

Схоже, Білий Дім і Сенат перебувають на межі складання угоди, яка призведе до того, що конституційність суперечливої національної програми спостереження Агентства національної безпеки оцінюватиметься спеціальними судами, створеними в рамках Закону про контроль над зовнішньою розвідкою (FISA). Це добрий перший крок. Але такий судовий розгляд матиме сенс лише у випадку, якщо остаточне рішення щодо легітимності програми буде ухвалюватися Верховним судом США.

У статті Ерика Ліхтбло, опублікованої сьогодні в ранковому випуску «Нью-Йорк таймс» (я не можу дати посилання), йдеться про таке: «Якщо суд [FISA] визнає програму неконституційною, Генеральний прокурор може уточнити й підтримати це рішення, або, навпаки, оскаржити це рішення в апеляційному суді FISA і врешті-решт, можливо, у Верховному суді...» Але що, якщо суд FISA з самого початку повідомляє, що програма є конституційною? Яким чином ця справа вийде із системи FISA і потрапить на розгляд у регулярному судовому процесі? Це не зовсім зрозуміло, і це — головний недолік пропозиції, перемовини стосовно якої ведуться головою судового комітету Сенату Арленом Спектером.

Програма NSA являє собою масштабне розширення президентських повноважень і широкомасштабне вторгнення в конституційне право на приватність. Подібні дії уряду занадто радикальні й потенційно занадто широко поширені, щоб мати можливість уникнути розгляду у Верховному суді США. Крім того, якщо програма настільки законна, як стверджує Білий Дім, то представники адміністрації (і, у тому числі, п. Спектер), не повинні боятися контролю з боку Верховного суду. Нарешті, тільки схвалення суду зможе задовольнити інтереси мільйонів американців, які зараз ставляться скептично, аж до відрази, до ідеї уряду підслуховувати телефонні розмови без ордеру.

ЧОМУ КОНФІДЕНЦІЙНІ ДАНІ ЗБЕРІГАЮТЬСЯ НА КОМП'ЮТЕРАХ?

Брайан Бергштейн, технічний кореспондент AP

Понеділок, 10 липня 2006 року

(AP) — БОСТОН. Щомісяця виникає новий випадок витоку сугубо конфіденційної інформації через втрату або крадіжку корпоративних або урядових ноутбуків. Зазвичай обговорення стосуються зашифровки таких даних.

Але деякі ключові питання найчастіше залишаються без відповіді. По-перше, чому допускається зберігання на ноутбуках такої кількості конфіденційних даних? Чим займаються весь день ці люди, що змушує їх постійно працювати із записами, скажімо, про 26 мільйонів американців (це приголомшуюче число фігурувало в недавньому випадку з «Veterans Affairs»)?

«Це — проста лінь. І цьому немає виправдання», — сказав Авіва Літан, аналітик з питань безпеки компанії Gartner Inc. «Для цього немає ніяких істотних причин».

Літан пропонує кілька простих заходів: організаціям слід зберігати конфіденційну інформацію тільки на безпечних, централізованих серверах. Працівники можуть одержати доступ до даних з комп'ютерів в офісі або через приватне підключення до Інтернету, але вони не можуть зберігати записи на своїх власних комп'ютерах і працювати з ними в автономному режимі.

Якщо конче необхідно зайнятися аналізом даних поза офісом, співробітник повинен запустити програму, що заміняє реальний номер кредитної карти або соціального страхування випадковими символами скрізь, де це можливо, оскільки фактичні цифри не завжди необхідні.

Дотримання таких правил дозволило б запобігти паніці, що виникла, коли 3 травня з будинку аналітика був украдений ноутбук з даними ветеранів (пізніше він був знайдений, і доступ до інформації, схоже, не здійснювався). Генеральний інспектор VA заявив Конгресу, що цей співробітник носив дані додому для аналізу з 2003 року.

Дійсно, шифрування даних — їх скремблирування приватними кодами — може зробити читання інформації на ноутбуці практично неможливим. Але шифрування часто не викорис-

товується користувачами, які вважають, що це погіршує продуктивність комп'ютера.

Розглянемо випадок з консультантом «ING Financial Services», який зберігав на своєму ноутбуці номери соціального страхування й інші особисті дані 13000 людей, що працюють в Окрузі Колумбія, поки комп'ютер не був викрадений з його будинку минулого місяця. «ING» займається виплатою пенсій на території округу.

Радник «ING» порушив правила, не зашифрувавши дані. Після цього випадку «ING» нагадала всім співробітникам, що програма шифрування повинна бути включена на їхніх ноутбуках, і її не можна відключати. Але сам факт виносу інформації з офісу не є порушенням. Керівники «ING» сказали, що консультант зберігав у себе записи, оскільки вони стосувалися найстарших учасників пенсійного плану, які часто просять його про допомогу. Консультант також прагнув мати дані під рукою для потенційної маркетингової діяльності, наприклад, для ухвалення рішення, кого запросити на фінансовий семінар.

Тепер, у світлі епізоду з ноутбуком, ING переглядає питання, чи можна взагалі виносити конфіденційну інформацію з офісу, навіть якщо вона є зашифрованою. Стів ван Вік, керівник інформаційної служби ING, вважає, що завдяки повсюдно доступним широкосмуговим з'єднанням і безпечному програмному забезпеченню, працівникам не потрібно зберігати конфіденційні дані на портативному обладнанні. Це не тільки являє собою ризик для безпеки даних, але також може призвести до проблем, пов'язаних із синхронізацією даних в офісі й даних на портативному обладнанні, сказав він.

«Контроль і захист інформації легше забезпечувати, якщо вона централізована», — сказав він. — «Навіщо ризикувати?» Значною мірою проблема втрати конфіденційних даних разом з ноутбуками пов'язана з повільністю компаній в оцінці цінності інформації. А якщо ні, то така інформація вже давно розглядалася б як маркетингові відомості й інші таємниці бізнесу, які не можуть залишати безпечні центральні комп'ютери.

Незрозуміло, чи буде коли-небудь усунута ця проблема. Значна кількість співробітників прагнуть зберігати інформацію «локально» на своїх ноутбуках, щоб мати можливість ефективно працювати під час поїздок, зустрічей із клієнтами або в інших місцях, де вони не можуть підключитися до мережі. Тому часто дозволяється брати ноутбуки з даними додому.

Так було й у випадку зі співробітником інвестиційної консультаційної фірми «Ameriprise Financial Inc.», на ноутбуці якого, викраденому в січні, зберігалися відомості про 158000 клієнтів. Представник «Ameriprise» Стівен Конноллі розповів, що цей співробітник був одним з «далеко не всіх людей» у компанії, яким дозволялося зберігати таку конфіденційну інформацію на особистому комп'ютері. Коннолі не зміг пояснити, навіщо цій людині — співробітникові корпоративного рівня, який не працював із клієнтами — був необхідний доступ до таких конфіденційних даних.

У лютому аналогічний випадок відбувся з консультантом компанії «Ernst & Young», який втратив імена, адреси й інформацію про кредитні карти 243000 клієнтів Hotels.com. Представник «Ernst & Young» Чарли Перкинс не пояснив, навіщо консультантові потрібно було зберігати цю інформацію. Однак, за словами Перкинса, компанія певна, що політика зашифровки даних на всіх 30000 ноутбуків її консультантів — захід, який був прийнятий після крадіжки — дозволить не допустити подібних інцидентів у майбутньому, зберігши мобільність співробітників.

Навіть якщо співробітники технічно не повинні виносити комп'ютери з офісу, багато хто таємно переписує файли на свої Ipod, Flash-накопичувачі й інші обладнання зберігання даних, — говорить Суніл Джейн, старший консультант «Sprint Enterprise Mobility Inc.», філії «Sprint Nextel Corp.»

«Набагато швидше завантажити дані, а потім працювати в автономному режимі», — говорить Джейн. — «Це просто людська природа». Джейн каже, що, наскільки йому відомо, центральні сервери його компанії повинні створювати резервні копії основних файлів щоночі, і він, про всяк випадок, робить те ж саме на своєму ноутбуці. Він вважає, що це загальноприйнята практика, тим більше, що багато компаній — у тому числі його — як правило, видають своїм співробітникам усе більш ємні ноутбуки, незалежно від того, чи потребують вони цього чи ні.

«Iron Mountain Inc.», компанія з управління даними, вважає, що вона пропонує оптимальне рішення: програмне забезпечення, яке зможе зробити так, що конфіденційна інформація на ноутбуці буде знищена у випадку втрати або крадіжки комп'ютера. Механізм самознищення спрацьовує, якщо комп'ютер не реєструється в домашньому офісі протягом якогось часу, або якщо злодій намагається підключити комп'ютер до іншої мережі.

ЗАХИСТ ДАНИХ НА УРЯДОВИХ НОУТБУКАХ

Ерік Сінрод

Упродовж останніх двох місяців Міністерство у справах ветеранів, Національна фінансова служба й Федеральна торговельна комісія намагалися розв'язати питання зі зниклими ноутбуками, на яких зберігалася велика кількість конфіденційних даних.

Як наслідок, Адміністрація Президента й Бюро управління й бюджету (OMB) видали нові керівні принципи щодо забезпечення фізичної безпеки й контролю, коли інформація виноситься із приміщень установ і федеральних міністерств, або доступ до неї здійснюється ззовні.

Зокрема, OMB рекомендує всім міністерствам і установам:

1. Зашифровувати всі дані на переносних комп'ютерах/обладнанні, на яких зберігаються урядові дані, за винятком випадків, коли дані визнані не конфіденційними;

2. Дозволяти дистанційний доступ тільки з «двухфакторною» аутентифікацією, коли один з факторів надається обладнанням, який відрізняється від комп'ютера, що одержує доступ;

3. Використовувати функцію «тайм-аут» для дистанційного доступу й мобільного обладнання, коли користувач повинен пройти повторну перевірку після 30 хвилин бездіяльності, а також

4. Реєструвати всі звернення до даних у базах, що містять конфіденційну інформацію, і стежити, щоб усі отримані конфіденційні дані були стерті протягом 90 днів, або перевіряти, що вони усе ще використовуються.

Мета вищевикладеного, як зазначає OMB — «належним чином захистити свої інформаційні активи при використанні інформаційних технологій». Обмежуючись цими вимогами і не даючи жодних докладних рекомендацій, OMB, проте, вимагає, щоб вищезгадані гарантії були створені федеральними міністерствами й відомствами протягом 45 днів.

Будемо сподіватися, що вираз «достатньо гарна робота уряду» найближчим часом буде містити в собі федеральні дії стосовно рекомендацій OMB, і ми перестанемо чути про загублені урядові ноутбуки, що містять легкодоступні конфіденційні дані.

У САН-ФРАНЦИСКО ПЕРЕГЛЯДАЄТЬСЯ КОНТРАКТ ІЗ AT&T У ЗВ'ЯЗКУ З НЕЗАКОННИМ СПОСТЕРЕЖЕННЯМ

Скотт Ліндлоу, Associated Press

Середа, 12 липня 2006 року

(AP) — САН-ФРАНЦИСКО. Міська влада Сан-Франциско переглядає контракт із AT&T Inc. про телекомунікаційні послуги, і вирішують, чи варто вживати заходів проти компанії із приводу її передбачуваного співробітництва з Агентством національної безпеки, заявив мер Гевін Ньюсом.

«Якщо те, що я читаю, є правдою, то я маю серйозні проблеми, як мешканець Сан-Франциско, як платник податків і як мер. І мені це не подобається», — сказав Ньюсом в інтерв'ю Associated Press у вівторок.

Федеральний позов, поданий юридичною компанією із захисту Інтернет-Безпеки «Electronic Frontier Foundation», обвинувачує телекомунікаційного гіганта в незаконному співробітництві з NSA, у рамках якого комунікації в мережах AT&T були доступні для спостереження без ордеру. Згідно з позовом, AT&T дозволила NSA встановити обладнання для аналізу даних у таємних кімнатах в офісах AT&T у Сан-Франциско, а також у декількох інших містах.

Минулого місяця уряд закликав федеральних суддів відхилити цей позов, заявивши, що це загрожує розкриттям державної таємниці. Рішення суду ще не прийняте.

Ньюсом каже, що він просив міського прокурора Денніса Єрреру провести «збір фактів» з цього питання. Мер також сказав, що зібрав разом відомості «про всі існуючі ділові відносини міста з AT&T».

Ці відомості, що містять строки договорів та інші зобов'язання, «можуть бути корисними, якщо ми вирішимо, що це — серйозна проблема, і захочемо не просто символічно заявити протест, але прийняти яке-небудь істотне рішення».

Мер сказав, що йому невідома вартість контрактів AT&T із Сан-Франциско. Також він не буде встановлювати строки для збору даних міським прокурором.

«Я визнаю можливість, з місцевої точки зору, трохи більшого впливу, тому ми маємо міцні відносини з AT&T, і я прагнув би, аби вони тривали», — сказав він.

«Але я також думаю, що це — вулиця із двостороннім рухом», — сказав Ньюсом. — «Якщо ви

збираєтеся працювати з нами, а Сан-Франциско цього прагне, ми говоримо: будь ласка, поважайте цінності людей, які здобувають ці товари й послуги, тобто платників податків нашого міста».

Міський прокурор сказав, що він не розмовляв безпосередньо із представниками NSA про цю програму. Прес-секретар прокурора відмовився дати коментарі про існування або хід розслідування.

Представник офісу AT&T у Сан-Антоніо, Майкл Коу, відмовився від коментарів щодо спостереження за жителями міста або коментарів мера.

«Протягом декількох десятиліть AT&T і місто Сан-Франциско тісно співробітничали», — пише Коу в електронному листі. — «Ми високо цінуємо ці відносини й дуже сподіваємося задовольняти телекомунікаційні потреби міста і його жителів у майбутньому».

Міністерство юстиції заявило, що по всій країні було подано більш ніж 20 позовів, у яких стверджується, що телефонні компанії незаконно співробітничають із NSA. Але перегляд контрактів з AT&T у зв'язку з незаконним спостереженням буде, очевидно, першим у своєму роді позовом, поданим урядовим закладом. Ньюсом говорить, що йому не відомо про інші аналогічні випадки.

17 травня Генеральний прокурор Нью-Джерсі Зуліма Фарбер й інші посадові особи спрямували повістки п'ятьом телекомунікаційним компаніям, вимагаючи надати документи, що пояснюють, чи передавали ці телекомунікаційні компанії, включаючи AT&T, відомості про своїх клієнтів NSA.

Минулого місяця федеральний уряд звернувся до влади Нью-Джерсі із проханням припинити збір інформації про співробітництво телефонних компаній з Агентством національної безпеки.

НЕДАВНІ ВІДКРИТТЯ ЩОДО ДОСТУПУ NSA ДО НАШИХ ТЕЛЕФОННИХ ПЕРЕГОВОРІВ: ЗАКОНИ, ЯКІ, ІМОВІРНО, БУЛИ ПОРУШЕНІ, І МОЖЛИВІ НАСЛІДКИ

Аніта Рамасастрі

Програма несанкціонованого прослуховування NSA телефонних розмов, як і раніше, викликає безліч суперечок. Не далі, як минулого тижня, «USA Today» повідомила, що президент Буш санкціонував ще одну секретну програму спостереження. У рамках цієї програми NSA, зважаючи на все, без будь-яких судових ордерів збирає відомості про телефонні розмови мільйонів американців у гігантську базу даних.

На підставі фактів, які стали відомі громадськості, можна зробити висновок, що телефонні компанії, які співробітничають із NSA, можливо, порушують закон, спеціально прийнятий Конгресом для рішення цієї проблеми — Закон про комунікації, що зберігаються (Stored Communications Act).

Адміністрація наводить ті ж аргументи на свій захист, що й у випадку несанкціонованого прослуховування телефонних розмов: Президент стверджує, що NSA намагається одержати відомості про терористичну діяльність — цього разу не шляхом прослуховування телефонних розмов, а шляхом пошуку у реєстрах телефонних дзвінків для виявлення можливих моделей. За даними «USA Today», у відповідних записах вказується, який номер був набраний, коли був зроблений виклик, а також початкова й кінцева крапка дзвінка (географічно).

Представники Адміністрації Буша підкреслюють, що програма не припускає прослуховування змісту розмов. У той же час, записи про телефонні розмови нібито дозволять уряду відслідковувати дзвінки й виявляти моделі, які можуть допомогти виявити зв'язок між терористами.

Факти про програму, наскільки вони відомі

Про програму контролю телефонних реєстрів ми знаємо мало, але от що відомо на сьогоднішній день: три телекомунікаційні компанії — AT&T, Verizon і Bellsouth, нібито передавали NSA записи про телефонні розмови більш ніж десяти мільйонів американців. Компанії, схоже, не цікавилися, чи мало NSA юридичне право на одержання таких записів, і, звичайно, не зверталися до суду з цього питання.

Компанія Qwest, однак, провела правовий аналіз ситуації. Після цього компанія відмовилася виконати прохання NSA. Qwest відмовилася із двох причин: її представники вважали, що необхідні ордери (або, принаймні, постанови суду) для того, щоб таке прохання було законним, і їх також турбувало, хто матиме доступ до інформації, і яким чином вона може бути використана.

Закон, що діяв з 2001 року по березень 2006 року, забороняє програму

Судячи з того, що нам відомо тепер, компанія Qwest була абсолютно права, відмовившись виконувати прохання NSA. Федеральний закон явно забороняв цій, а також іншим компаніям, виконувати подібні прохання уряду. Хоча цей закон обмежує дії компаній, а не уряду, уряд, безумовно, не повинен натискати на компанії для того, щоб примусити їх порушити закон.

Цей закон — Закон про комунікації, що зберігаються, 1986 року (SCA), який конкретно і ясно забороняє телефонним компаніям передавати уряду свої записи без ордеру або постанови суду. Відповідно до закону провайдери «електронних комунікацій... повинні свідомо не розголошувати... будь-якій державній організації... записи або іншу інформацію, що стосується абонента або клієнта».

Існує лише одне виключення із цього правила: згідно із законом, що діяв до березня 2006 року (коли в SCA були внесені поправки), компанії можуть передавати записи, тільки якщо вони «розумно» вважають, що розкриття інформації може допомогти запобігти «безпосередній загрозі смерті або серйозних тілесних ушкоджень». Так, наприклад, при проведенні конкретного розслідування неминучого терористичного акту, компанія може невідкладно — без рішення суду або ордеру — здійснити передачу записів про підозрюваних.

Схоже, що програма NSA здійснювалася до внесення в березні 2006 року поправок до SCA (що збігся з відновленням «Патріотичного Акту» США). Більше того, програма могла існувати після 11 вересня. Якщо це так, то в ній використовується норма «розумної» віри в «безпосередню небезпеку».

Навряд чи телефонні компанії можуть стверджувати, що вони мали «розумну» віру в «безпосередню небезпеку» протягом усього часу з моменту початку здійснення програми, коли б це не відбулося, до дати внесення змін. Можливо, протягом декількох місяців відразу після атак 11 вересня, або в періоди, коли рівень загрози був найвищим, віра в «безпосередню небезпеку» була виправданою й навіть «розумною». Але навіть уряд стверджує, що безпосередня небезпека існує лише в певних місцях і в певні періоди часу.

Уряд не надав жодних доказів того, що моніторинг телефонних реєстрів з боку NSA був обмежений місцем, часом або рівнем погрози. Замість цього, уряд продовжує реалізовувати програму, що спростовує будь-які заяви про те, що ця діяльність виправдовується «безпосередньою небезпекою».

Крім того, опис програми припускає, що це превентивний захід, а не захід реагування. За даними уряду, NSA сканує величезні бази записів телефонних розмов і намагається знайти моделі, що вказують на майбутні атаки, а не тому, що знає, у певний час, про конкретну загрозу.

Незастосовність виключень «згоди клієнта» і «службової необхідності»

Крім того, очевидно, що програма моніторингу телефонних реєстрів не підпадає під інші виключення закону SCA стосовно розкриття інформації. SCA дозволяє передавати записи згідно із «законною згодою клієнта», але тут такої згоди немає.

Як повідомляється, юристи уряду мають намір заперечити, що у Договорах на надання послуг, що укладаються із компаніями, є набраний дрібним шрифтом пункт, що дозволяє компаніям ділитися інформацією про клієнтів з метою забезпечення правопорядку, що розглядається як «згода». Однак експерти в цій області вважають, що цей пункт не може розглядатися як згода.

Наприклад, професор Орін Керр, колишній федеральний прокурор, що був, і експерт з Четвертої поправки, підкреслює, що, незважаючи на відсутність інтерпретації того, що вважається «згодою» відповідно до SCA, виключення «згоди» у цьому випадку є «точною копією аналогічного виключення в аналогічному SCA федеральному законі про прослуховування» (18 U.S.C. sec. 2510-22). Крім того, Керр стверджує, що згода, відповідно до Закону про прослуховування, вимагає, щоб «користувач фактично погодився на дії, прямо або побічно, прийнявши рішення продовжувати користуватися послугою після фактичного повідомлення».

SCA також дозволяє передавати записи, якщо «виникли проблеми з наданням послуги, із захистом прав або власності постачальника цієї послуги». Наприклад, записи можуть бути передані правоохоронним органам для піймання хакерів, що зламали мережу.

Тут, однак, ні права компаній, ні їх власність не зазнають небезпеки, і передача даних навряд чи пов'язана із проблемами з надання телефонних послуг; вона також не має нічого спільного з наданням телефонних послуг компаніями, а служить лише для цілей уряду.

Чи змінили ситуацію останні поправки, внесені в SCA у березні 2006 року?

У березні 2006 року в SCA були внесені поправки, що стосуються виключень у надзвичайних ситуаціях. Компанії тепер можуть передавати записи до державних органів, якщо вони «сумлінно вважають, що надзвичайна ситуація, пов'язана з небезпекою смерті або нанесення серйозних тілесних ушкоджень будь-якій особі, вимагає негайної передачі даних, пов'язаних з надзвичайною ситуацією».

Як це відрізняється від вихідного виключення в надзвичайних ситуаціях? У принципі, компанія не повинна бути раціональною, вона просто повинна «сумлінно вважати». І немає жодної необхідності в «безпосередній небезпеці» — потрібна просто надзвичайна ситуація, що являє собою небезпеку для життя й здоров'я.

Цілком можливо, що ця остання поправка захищає телефонні компанії, які передавали NSA записи про телефонні розмови після внесення поправки, але не компанії, які робили це в період між початком дії програми й прийняттям поправки.

Наслідки порушення закону

Чи маєте ви вагомі свідчення ймовірного порушення закону, що відбувається далі? SCA передбачає право споживача подати до суду, і кілька позовів уже були подані проти телефонних компаній. SCA встановлює компенсацію збитку в розмірі як мінімум в $1000 за кожне порушення.

Таким чином, один позов вимагає виплати до 5 мільярдів доларів трьома компаніями, які, згідно з повідомленнями, передавали записи — Verizon, AT&T і Bellsouth, якщо ґрунтуватися на тому, що кожний запис, незаконно переданий NSA, вважається окремим порушенням.

SCA передбачає також відшкодування судових витрат, і, якщо рішення буде прийнятий на користь позивачів, телефонні компанії будуть змушені заплатити їхнім адвокатам. Усе це, однак, малоймовірно, оскільки, згідно з опитуваннями, більшість американців влаштовує контроль записів телефонних перемовин з боку уряду — отже, це стосується й деяких присяжних.

Державні службовці, що брати участь у порушеннях, можуть бути піддані дисциплінарному покаранню. І слухання в Конгресі можуть — і повинні — розпочатися.

Чому слухання в Конгресі США є вкрай необхідними

Як було вище зазначено, більшість американців, схоже, не надто переймаються звісткою про таємні передачі NSA телефонних реєстрів. Що робитиме уряд, коли він виявить імовірні телефонні перемовини терористів, завдяки своєму аналізу даних? Чи звернеться він до суду, такий, як суд FISA, щоб одержати більш конкретні повноваження для прослуховування певних телефонних перемовин? Адміністрація не дає відповідей на ці питання.

Слухання можуть підкреслити, наскільки результати таких спостережень можуть бути — і вже були в минулому — неправильними. Я вже писала про небезпеки «цифрових досьє». Телефонні реєстри, які легко можуть бути зіставлені з іменами, дозволять урядові продовжити заповнення цих досьє, складаючи велику картину ділового й особистого життя громадян і моделі повсякденного життя.

Важливо, щоб Конгрес натиснув на адміністрацію, щоб остання більш докладно розповіла про свої плани й наявні гарантії. Чи будуть записи про наші телефонні перемовини зберігатися вічно? Коли уряд збереться глянути на ці записи?

Громадськість повинна знати, чи дійсно програма контролю телефонних реєстрів може ненавмисно привести, наприклад, до расового профілювання або до створення конкретних цільових груп для подальшого спостереження без реальних імовірних причин. Припустимо, існує статистика дзвінків з певного номеру на номери на Близькому Сході або в Афганістані. Потім цей номер зіставляється з іменем. Якщо ім'я «звучить арабською», чи зросте ймовірність того, що за людиною стежитимуть, навіть якщо особа арабського походження, можливо, просто дзвонить родичам, що мешкають за кордоном?

Конгрес має повноваження і засоби для вивчення масштабів і законності дій уряду в цьому випадку (як і у випадку програми прослуховування телефонних розмов без ордеру) без шкоди для національної безпеки. Дійсно, національна безпека вимагає повного розуміння того, яким чином уряд вторгається в приватне життя американців, і чи є це втручання правильним.

Нарешті, навіть якщо врешті-решт буде ухвалене рішення, що програма контролю телефонних реєстрів є законною, вона однаково неправильна й з погляду політики, і з погляду конфіденційності. Слухання можуть, як мінімум, допомогти Конгресу забезпечити введення й виконання належних гарантій при зборі таких даних урядом.

СТАТТЯ 19: ООН ЗМІЦНЮЄ ПРАВО НА СВОБОДУ СЛОВА ТА ІНФОРМАЦІЇ

Сандра Колівер | 28 липня 2011
http://blog.soros.org/author/sandra-coliver/

Комітет ООН з прав людини щойно завершив дворічні консультації і дискусії про те, яким чином інтерпретувати право на «свободу думок і їх вираження», гарантоване статтею 19 Міжнародного пакту про громадянські і політичні права http://www2.ohchr.org/english/law/ccpr.htm.

Думка Комітету, викладена у Загальному коментарі № 34, має серйозний авторитет для судів і трибуналів, й істотно впливатиме на розвиток правових норм у світовому масштабі. Це буде особливо важливо в тих регіонах, де ще немає власних місцевих механізмів судового захисту прав людини (а саме, на Близькому Сході і в Азії). У тих регіонах, де є такі правозахисні механізми (в Америках, Африці та Європі), Міжнародний пакт про громадянські і політичні права відіграє важливу роль у встановленні мінімальних стандартів.

Коментар щодо свободи вираження поглядів заснований на письмових і усних зауваженнях більш ніж 70 неурядових організацій, включаючи організацію «Правова Ініціатива Відкрите Суспільство» http://blog.soros.org/2011/03/article-19-under-the-microscope/, а також урядів, національних правозахисних організацій та вчених. Коментар зачіпає кілька ключових аспектів статті 19, в тому числі:

— значення свободи вираження поглядів та інформації як «мета-права», на якому ґрунтуються інші права;
— зобов'язання урядів захищати свободу слова і забезпечувати доступність інформації;
— право журналістів та інших осіб на поширення інформації, а також право громадян на отримання інформації;
— визнання мінливого характеру сучасних засобів масової інформації, а також розвитку технологій;
— важливість незалежності засобів масової інформації.

Загальний коментар свідчить, що свобода ЗМІ повинна захищатися на найвищому рівні, і що захист, що надається традиційним засобам масової інформації, поширюється в повному обсязі на нові ЗМІ. Коментар закликає держави вжити «всіх необхідних кроків для забезпечення незалежності цих нових засобів масової інформації та забезпечення доступу до них людей».

Одним з найважливіших досягнень, що міститься в коментарі, є твердження, що «заборони прояви неповаги до релігії або іншої системи переконань, включаючи закони про богохульство, несумісні з Пактом», хоча обмеження на такі висловлювання можуть бути виправдані за конкретних обставин, передбачених у статті 20 (2) Пакту, яка забороняє «підбурювання до дискримінації, ворожості або насильства». Хоча «ворожість» — досить невизначений термін, Комісія не може ігнорувати це явне положення Пакту.

Це твердження є особливо важливим в світлі того факту, що чотири з 18 експертів Комітету представляють країни Північної Африки (Алжир, Єгипет, Марокко і Туніс), які є членами Організації Ісламської конференції (ОІК). Протягом останніх декількох років ОІК активно лобіювала Комітет ООН з прав людини, домагаючись прийняття резолюції, що закликає держави встановити кримінальну відповідальність за дифамацію релігії.

Іншим важливим досягненням є чітка вказівка, що стаття 19 «охоплює право на доступ до інформації, що знаходиться в розпорядженні державних органів».

Це право було визнано Міжамериканським та Європейським судами з прав людини (у 2006 і 2009 роках відповідно), а також Африканською комісією з прав людини і народів Африканського союзу (принаймні, з 2002 року). Сам Комітет з прав людини явно визнав це право в травні цього року у справі, що була порушена громадянином Киргизстану, який добивався отримання доступу до інформації про статистику приведення у виконання смертних вироків. На результат цієї справи, безсумнівно, вплинула робота Комітету над загальним коментарем. Вже в березні цього року Комітет затвердив положення коментаря, пов'язані з правом на доступ до інформації.

Загальний коментар № 34 стосується чотирьох важливих компонентів права на доступ до інформації. Держави повинні докласти всіх зусиль для забезпечення швидкого, легкого, ефективного та практичного доступу до контрольованої державою інформації, що є суспільним надбанням. Вони повинні активно надава-

ти громадськості інформацію про роботу уряду, а також іншу інформацію, яка представляє суспільний інтерес. Повинен бути передбачений механізм оскарження у випадках ненадання запитаної інформації, а також у випадках явних відмов. Це право належить до інформації, що знаходиться в розпорядженні всіх державних органів, включаючи законодавчу і судову гілки, і може також поширюватися на приватних осіб, які виконують державні функції.

Коментар, що включає рекомендації «Правової ініціативи», також свідчить, що держави не можуть, відповідно до Пакту, «утримувати або приховувати від громадськості інформацію, що представляє законний суспільний інтерес, якщо вона не завдає шкоди національній безпеці». Це — значний крок вперед. Іншими словами, держави не повинні засекречувати таку інформацію, вони повинні надавати до неї доступ на вимогу, а також активно публікувати її. Більше того, держави не можуть «переслідувати журналістів, дослідників, активістів-екологів, правозахисників або інших осіб за поширення такої інформації». Мається на увазі, що це зобов'язання поширюється навіть на ті дані, які були офіційно засекречені.

Щоб підкреслити інтенсивність дискусії навколо статті 19, слід зазначити, що даний документ складається з 15 сторінок і 54 пунктів, в порівнянні з трьома пунктами, з яких складався попередній загальний коментар щодо свободи вираження поглядів, прийнятий 1983 року.

Майкл О'Флаерті http://www.nottingham.ac.uk/law/staff-lookup/M.Oflaherty, член Комітету з прав людини, відповідальний за розробку коментаря, сказав, що після двох років роботи Комітет склав «максимально потужну заяву».

ПРАВОЗАХИСНИЙ ОРГАН ООН КРИТИКУЄ ОБМЕЖЕННЯ СВОБОДИ СЛОВА

Нью-Йорк, 28 липня 2011 р., 12:05

Управління Верховного комісара з прав людини (УВКПЛ) сьогодні повідомило, що Комітет ООН з прав людини випустив коментар щодо свободи вираження думок, який свідчить, що закони проти богохульства та обмеження на критику уряду несумісні з існуючими нормами, і що свобода вираження поглядів має велике значення для захисту прав людини.

Комітет також зазначив, що антитерористичні заходи, включаючи закони, що криміналізують дії, які «заохочують» або «виправдовують» тероризм, «повинні бути чітко визначені, щоб гарантувати, що вони не призведуть до непотрібного або невідповідного втручання в свободу вираження поглядів», а закони проти дифамації державних посадових осіб і глав держав «не повинні передбачати більш суворе покарання виключно на підставі особистості людини, якій пред'являється обвинувачення».

Доповідь Комітету, озаглавлена «Загальний коментар № 34», є інтерпретацією Міжнародного пакту про громадянські і політичні права 1966 року (МПГПП), до якого приєдналися 167 держав-учасників. Комітет ООН з прав людини є незалежним органом, що здійснює нагляд за дотриманням МПГПП.

«Заборони проявів неповаги до релігії або іншої системі переконань, включаючи закони про богохульство, несумісні з Пактом», за винятком особливих обставин, свідчить коментар, і держави «не повинні забороняти критику таких інститутів, як армія чи адміністрація».

Комітет зазначив, що так звані «закони про пам'ять», які він визначив як «закони, що передбачають покарання за висловлення думок про історичні факти», також є «несумісними з зобов'язаннями, які Пакт накладає на держави-учасників стосовно дотримання свободи думок та їх вираження».

«Загальний коментар являє собою всеосяжну відповідь на численні прохання з боку законодавців, суддів, прокурорів, адвокатів, правозахисників і навіть журналістів щодо роз'яснення багатьох питань, пов'язаних з правом на свободу вираження поглядів і переконань», заявив член комітету Майкл О'Флаерті, головний укладач звіту, http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=11269&LangID=E.

«Цей документ підтверджує центральне значення свободи слова для всіх прав людини і встановлює дуже суворі параметри, в рамках яких це право може обмежуватися державами».

«Свобода вираження поглядів є необхідною умовою для реалізації принципів прозорості та підзвітності, які, в свою чергу, необхідні для стимулювання та захисту прав людини», — йдеться в доповіді.

«Держави-учасники повинні вжити ефективних заходів для захисту від дій, спрямова-

них на переслідування осіб, які здійснюють своє право на свободу вираження поглядів».

Сандра Колівер,
Старший співробітник з правових питань, свободи інформації та вираження думок, Правова Ініціатива «Відкрите Суспільство»
Нью-Йорк
Тел.: +1.212.548.0384
www.right2info.org
www.justiceinitiative.org

Helen Darbishire, *виконавчий директор, «Access Info Europe»*

Pam Bartlett Quintanilla, *координатор проекту, «Access Info Europe»*

РАДА ЄС ПРОТИ ВІДКРИТОГО ПРИЙНЯТТЯ РІШЕНЬ

ГРЕЦІЯ, ВЕЛИКОБРИТАНІЯ Й ІНШІ ДЕРЖАВИ-ЧЛЕНИ ВИСТУПАЮТЬ НА КОРИСТЬ ТАЄМНОСТІ

Мадрид, 27 червня 2011 року. Рада Європейського Союзу оскаржила прийняте в березні 2011 року рішення Генерального Суду, у якому обіцялося відкрити Брюссельський законодавчий процес для належного контролю й участі представників європейської громадськості

Як повідомляється, ряд держав-членів розглядають питання про приєднання до цього протесту, з метою зробити процес прийняття рішень Радою ЄС закритим. Зокрема, Рада прагне позбавити європейських громадян права знати позицію своїх урядів під час обговорення норм і правил ЄС, які сьогодні впливають на дві третини національного законодавства.

Греція й Великобританія вже зайняли позицію проти більшої прозорості Ради: обидві країни встали на сторону Ради, підтримавши первісну справу, яка закінчилася прийняттям Генеральним Судом 22 березня 2011 року рішення на користь суспільного доступу до інформації й участі громадськості.

Ця справа, *Access Info Europe vs. Council* (Справа T-233/09) було розпочата в червні 2009 року. У листопаді 2008 року базована в Мадриді правозахисна організація направила запит про реформування правил ЄС щодо прозорості й одержала документи з вимазаними назвами країн, так що було неможливо довідатися, які країни виступали за, а які проти більш широкого доступу громадськості до інформації.

Генеральний Суд визнав цю відмову незаконною і ухвалив, що Рада «ніяк не продемонструвала», як розголошення назв країн могло «серйозно зашкодити його процесу прийняття рішень».

Суд підкреслив, що «щоб громадяни могли здійснювати свої демократичні права, вони повинні мати можливість докладно простежити процес прийняття рішень», і що вони повинні «мати доступ до всієї необхідної інформації».

ЗАКЛИК ДО ДЕРЖАВ-ЧЛЕНІВ У ПІДТРИМКУ ПРОЗОРОСТІ

Коментуючи новину, що Рада й, можливо, велика кількість країн-учасниць будуть заперечувати згадане рішення, виконавчий директор «Access Info Europe» Хелен Дербишир заявила: «Уся іронія цієї ситуації полягає в тому, що навіть самі правила про прозорість непрозорі. Хоча ЄС стверджує, що намагається стати ближче до громадян, він, насправді, захлопує двері в них перед носом».

Організація «Access Info Europe» призиває держави-члени підтримати визнане на міжнародному рівні право на доступ до інформації й пропонує приєднатися до неї в цій справі.

Ми запрошуємо всі організації громадянського суспільства й окремих осіб, які прагнуть приєднатися до кампанії й переконати свої уряди підтримати прозорість у ЄС, зв'язатися з Памелой Бартлетт за адресою «Access Info Europe» для одержання інформації й агітаційних матеріалів.

Для одержання додаткової інформації — на англійській або французькій мовах — звертайтеся, будь ласка, до нас.

СВОБОДА ВИСЛОВЛЮВАНЬ І ПРИВАТНІСТЬ № 2–3 (34–35)
Квітень–Вересень, 2011

Щоквартальний додаток до інформаційно-аналітичного бюлетеня «Права людини»
Свідоцтво про реєстрацію ХК № 683 від 27 грудня 1999 року
видане обласним комітетом інформації

Видання бюлетеня засновано з благодійною метою для безкоштовного розповсюдження

ЦЕ ВИДАННЯ ЗДІЙСНЕНО ЗА ФІНАНСОВОЇ
SPONSORED BY THE INTERNATIONAL
ТА ЕКСПЕРТНОЇ ПІДТРИМКИ
RENAISSANCE FOUNDATION
МІЖНАРОДНОГО ФОНДУ "ВІДРОДЖЕННЯ"

Обкладинка *Борис Захаров*

Комп'ютерна верстка *Олег Мірошниченко*

Засновник та видавець — ХАРКІВСЬКА ПРАВОЗАХИСНА ГРУПА
Адреса видавця та редакції:
Україна, 61002, Харків-2, вул. Іванова, 27, пом. 4
тел., факс (057) 700-67-71, e-mail: khpg@ukr.net
Електронна версія: http://khpg.org/index.php?r=1.5.3
Адреса для листування: Україна, 61002, Харків-2, а/с 10430
Бюлетень готується та друкується на обладнанні ХПГ за адресою: вул. Іванова, 27, пом. 4.
Наклад — 500 прим.