СВОБОДА ІНФОРМАЦІЇ ТА ПРАВО НА ПРИВАТНІСТЬ В УКРАЇНІ

ТОМ 2

ПРАВО НА ПРИВАТНІСТЬ:

CONDITIO SINE QUA NON

34(75)

ХАРКІВСЬКА ПРАВОЗАХИСНА ГРУПА

ХАРКІВ
«ФОЛІО»
2004

ББК 67
С25

Упорядник
Є. Захаров

Художник-оформлювач
О. Герчук

Ця публікація здійснена за фінансової підтримки
Міністерства іноземних справ Данії (FRESTA)
у співробітництві з Данським інститутом з прав людини

С25 **Свобода інформації та право на приватність в Україні. Том 2. Право на приватність: conditio sine qua non** / Харківська правозахисна група; Худож.-оформлювач О.Герчук – Харків: Фоліо, 2004. – 200 с.

ISBN 966-03-2588-6.

Другий том спеціального випуску №34(75) інформаційно-аналітичного бюлетеня «Права людини» Харківської правозахисної групи містить матеріали, присвячені різним аспектам дотримання права на приватність: захист персональних даних, моніторинг телекомунікацій, недоторканність житла, таємниця листування. Розглядаються також питання доступу до архівів.

Книга містить як переклади зарубіжних фахівців, так і статті вітчизняних дослідників.

ББК 67

ISBN 966-03-2588-6

ПРАВО НА ПРИВАТНІСТЬ

ПРИВАТНІСТЬ І ПРАВА ЛЮДИНИ

Міжнародний огляд законодавства та практики його застосування щодо приватності

Цю доповідь підготовлено Privacy International за рахунок коштів гранту, наданого Інститутом Відкритого Суспільства (Open Society Institute). Основні автори доповіді – Девід Банісар (Electronic Privacy Information Center) та Саймон Девіс (Privacy International). Додаткові дослідження провели Вейн Мадсен, Майкл Касснер, Ронні Брекхеймер, Шауна Ван Донген. Добре обізнаним особам – представникам академічних закладів, урядових структур, правозахисних груп та інших установ було запропоновано підготувати доповіді та надати інформацію. Їхні доповіді було доповнено інформацією з інших джерел, таких як конституції, законодавство, міжнародні й національні офіційні документи, інформаційні повідомлення, доповіді з питань прав людини (список використаних джерел додається).

КОРОТКИЙ ОГЛЯД

Приватність – фундаментальне право людини, визнане в Загальній декларації прав людини ООН, Міжнародному пакті про громадянські й політичні права та в багатьох інших міжнародних і регіональних угодах. Приватність тісно пов'язана з людською гідністю й іншими ключовими цінностями, такими як свобода асоціацій та свобода слова. Вона стала одним із найбільш важливих питань у галузі прав людини новітнього часу. Публікація цієї доповіді демонструє зростаючу важливість, різнобічність та складність цього фундаментального права.

У цій доповіді показано стан приватності в п'ятидесяти країнах світу. Вона окреслює конституційні й законодавчі умови захисту приватності та узагальнює важливі питання й події, що стосуються приватності та стеження.

Майже всі країни світу визнають право на приватність безпосередньо у своїх конституціях. Щонайменше, такі правові норми передбачають право на недоторканність житла та таємницю кореспонденції. Найновіші конституції, наприклад, Південної Африки та Угорщини містять у собі спеціальні норми щодо доступу та контролю за інформацією особистого характеру.

У багатьох країнах, де приватність не визнано безпосередньо у конституції, наприклад, Сполучених Штатах, Ірландії та Індії, для реалі-

зації цього права суди застосовують інші норми. Зокрема, міжнародні договори, де визнається право на приватність, такі як Міжнародний пакт про громадянські й політичні права або Європейська Конвенція про права людини, що є частиною законодавства багатьох країн.

На початку сімдесятих років у різних країнах почали прийматися законодавчі акти з метою захисту приватності. По всьому світі існує загальний рух у напрямку прийняття всеохоплюючого закону, яким встановлювалися б рамки для захисту. Більшість таких законів побудовані на моделях, запроваджених Організацією Економічного Розвитку та Співробітництва й Радою Європи.

У 1995 році, взявши до уваги недоліки законодавства та різний рівень захисту в кожній із держав, Європейський Союз запровадив загальноєвропейську директиву, що має забезпечити громадянам більш широкий обсяг захисту від зловживань їхніми даними[1]. Директива щодо «Захисту осіб у зв'язку з обробкою інформації про особу та відсутністю обмежень на переміщення такої інформації» встановлює основу для національного законодавства. Кожна країна-член Європейського Союзу була зобов'язана внести необхідні зміни в національне законодавство до жовтня 1998 року.

Директивою також накладено зобов'язання на держав-членів забезпечити, щоб інформація особистого характеру, яка стосується громадян держав-членів Євросоюзу, передавалась та оброблялась за межами Європейського Союзу тільки у випадках, передбачених законом. Результатом цієї вимоги стало зростання тиску за межами Євросоюзу щодо ухвалення закону з питань приватності. Більше сорока країн вже мають закони з питань захисту даних або захисту приватності в інформаційному законодавстві. Багато інших започаткували процес розробки подібних законів.

Причини для детальної розробки законодавства

Існує три основних причини для руху в напрямку ухвалення всебічного закону з питань приватності та захисту даних. Багато країн запровадили його з однією метою або кількома.

- **виправити несправедливість, що була допущена у минулому**.

Деякими країнами, особливо у Центральній Європі, Південній Африці та Південній Америці ухвалено законодавчі акти з метою захисту від порушень приватності, що допускалися за часів попередніх авторитарних режимів.

- **розвиток електронної торгівлі**

У багатьох країнах, особливо в Азії, а також у Канаді, існує розвинене або таке, що активно розвивається, законодавство з метою просування електронної торгівлі. У цих країнах визнають складність роботи із персональними даними споживачів, що відправляються з усього світу. Закон щодо приватності вводиться як частина правової бази, що має створити необхідні умови для електронної торгівлі шляхом встановлення загальних правил.

- **уніфікація закону відповідно до норм європейського права**

Більшість країн Центральної та Східної Європи ухвалюють нові законодавчі акти, які грунтуються на Конвенції Ради Європи та Директиві щодо захисту даних Європейського Союзу. Деякі з цих країн сподіваються в найближчому майбутньому набути статусу членів Європейського Союзу. Країни, що належать до інших континентів, як, наприклад, Канада, приймають нові закони з урахуванням того, щоб торгівля не постраждала від вимог, що базуються на положеннях Директиви Євросоюзу.

ІСНУЮЧІ СКЛАДНОСТІ

Порушення права на приватність продовжує викликати стурбованість навіть після запровадження законодавчих та інших засобів захисту. У багатьох країнах законодавство відстає від розвитку технологій, що створює серйозні прогалини в засобах захисту. В інших країнах правозастосовчим органам та розвідувальним службам надано можливість користуватися винятковими правами. Нарешті, в умовах відсутності адекватного нагляду за дотриманням закону та засобами його застосування саме по собі існування законів не може забезпечувати належного захисту.

Навіть у найбільш демократичних країнах дуже поширеним є порушення закону, що стосується знімання інформації з електронних каналів зв'язку. Щорічний звіт Державного департаменту Сполучених Штатів Америки стосовно порушень прав людини містить у собі інформацію про те, що більше ніж у 90 країнах світу відбувається незаконне стеження за політичними опонентами, правозахисниками, журналістами, профспілковими діячами. За підсумками 1996 року у Франції урядовою комісією було встановлено понад 100 000 випадків прослуховування телефонних розмов приватними сторонами, часто в інтересах урядових структур. У Японії поліція нещодавно змушена була сплатити 2,5 мільйони єн за незаконне прослуховування членів комуністичної партії.

Поліцейські служби, навіть у країнах з суворим законом у галузі приватності, і надалі активно збирають інформацію про громадян, які не звинувачуються і навіть не підозрюються у скоєнні злочинів. Зараз продовжуються розслідування таких випадків у Швеції та Норвегії, двох країнах з найбільшою історією захисту приватності стосовно даних, що збираються поліцією. Компанії регулярно нехтують законом, збираючи та поширюючи інформацію особистого характеру. У Сполучених Штатах, навіть в умовах тривалого існування закону щодо інформації про кредитні операції споживачів, компанії активно використовують таку інформацію в ринкових цілях.

ЗАГРОЗИ ДЛЯ ПРИВАТНОСТІ

Зростаюче ускладнення інформаційних технологій з їх можливостями щодо збору, аналізу та поширення інформації стосовно конкретних осіб вимагає невідкладного законодавчого регулювання. Більше того, но-

вий розвиток у галузі медичних досліджень, телекомунікацій, систем транспортування та руху фінансових засобів значно збільшує рівень інформації, що опрацьовується відносно кожної особи. Пов'язані між собою комп'ютери з допомогою високошвидкісних мереж з розвиненими процесорами можуть створювати детальні досьє на будь-яку особу без допомоги єдиної централізованої комп'ютерної системи. Нові технології, що розвиваються в межах військової промисловості, розповсюджуються для використання в правоохоронних органах, цивільних установах та приватних компаніях.

Згідно з опитуваннями громадської думки, стурбованість порушенням приватності зараз більша, ніж будь-коли в новітній історії[2]. Населення різних країн світу висловлює своє занепокоєння стосовно обмеження приватності. У безпрецедентній кількості держав лунають заклики до запровадження закону, що має надати спеціальний захист своїм громадянам. Правозахисні групи стурбовані тим, що велика кількість таких технічних засобів є предметом експорту до країн, що розвиваються, і де не забезпечується належний захист. На цей час існує не так уже й багато бар'єрів для торгівлі технологіями засобів стеження.

Загальнозрозумілим зараз є те, що потужність, місткість та швидкість інформаційних технологій зростає надзвичайно високими темпами. Пропорційно збільшується і рівень втручань у сферу приватності, або принаймні потенційні можливості для цього.

Поза цими очевидними аспектами співвідношення можливостей та ціни існує багато важливих тенденцій, що сприяють обмеженням приватності:

Глобалізація знімає географічні обмеження руху інформації. Розвиток Інтернету є, напевне, найбільш відомим прикладом глобальних технологій.

Конвергенція веде до усунення технологічних бар'єрів між системами. Нові інформаційні системи стають усе більш сумісними з іншими системами і можуть проводити взаємний обмін та обробку різних видів інформації.

Мульті-медіа поєднує багато форм передачі інформації і таким чином інформація, зібрана в одному вигляді, може бути легко переведена в інший.

Передача технологій та політика конвергенції

Наведені вище макротенденції справили специфічний ефект на проведення стеження в країнах, що розвиваються. У сфері інформації та комунікаційних технологій політика швидкої конвергенції інтенсифікується. У спектрі стеження – прослуховування, системи персональної ідентифікації, збір даних, цензура та контроль за криптографією – усе це притаманно Заходу, де неймовірними темпами відбувається невпинний розвиток[3]. Уряди країн, що розвиваються, сподіваються, що країни першого світу забезпечать їх технологіями стеження, такими як цифрове обладнання для підслуховування, дешифратори, сканери, «жучки», засоби стеження та

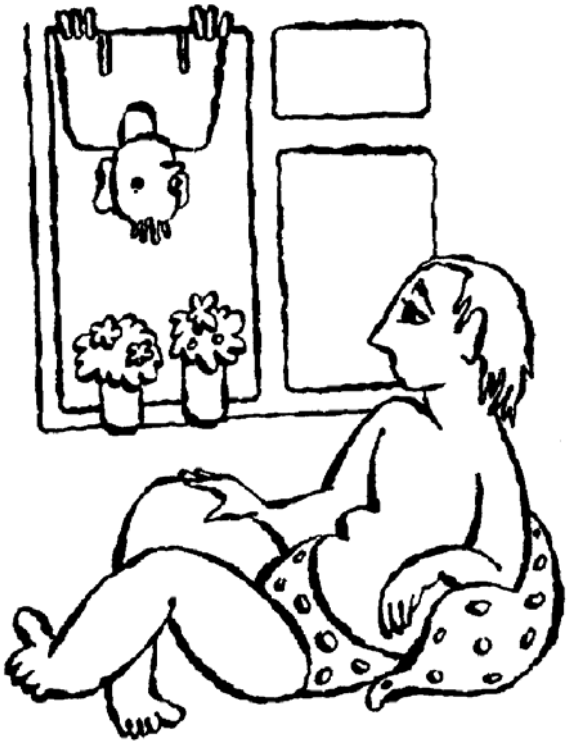
системи комп'ютерного перехоплення. Передача технологій стеження країнами першого світу країнам третього світу є зараз прибутковою складовою військової промисловості[4].

Згідно з даними, викладеними у звіті за 1997 рік «Оцінка технологій політичного контролю», розглянутого Комітетом громадянських свобод Європейського Парламенту і підготовленого службою оцінки науки та технологій (Science and Technology Options Assessment office (STOA) Європейської Комісії[5], більшість технічних засобів використовується для стеження за діяльністю дисидентів, активістів правозахисного руху, журналістів, студентських лідерів, меншин, профспілкових діячів та політичних опонентів. У звіті зроблено висновок, що такі технології (описані як «нові технології стеження») можуть справляти потужний «ефект холодного душу» на тих, хто «може мати бажання дотримуватися особливої точки зору і буде мало охочих для ризику використовувати своє право демократичного протесту». Розмаїття систем ідентифікації є також придатним для контролю за широким сектором населення. За визначенням Privacy International, «в умовах відсутності ефективного законодавчого та конституційного захисту такі технології є шкідливими для демократичних реформ. Це може бути фатальним для кожного, хто «становить інтерес» для правлячого режиму».

Як уряд, так і громадяни можуть мати певні переваги від застосування нових технічних засобів у державному та приватному секторі. Проекти нових «розумних карток» («smart card»), у яких інформація про клієнта розміщується на мікропроцесорі картки, може спростити здійснення складних операцій. Інтернет стане революційним засобом доступу до основної інформації урядових структур. Криптографія може бути засобом безпеки та приватності для всіх сторін. Однак такі ініціативи будуть вимагати створення серйозної далекоглядної правової бази. Чи зможуть уряди створити таку правову основу, залежатиме від їхньої здатності прислухатися до пульсу всесвітньої цифрової економіки та визнавати потребу суворого захисту приватності.

ВИЗНАЧЕННЯ ПРИВАТНОСТІ

Із усіх визнаних на міжнародному рівні прав людини приватність, напевне, визначити найскладніше[6]. Приватність має глибокі історичні корені. Численні посилання на приватність можна знайти в Біблії[7]. Приватність була об'єктом загального захисту за часів давньоєврейської культури, класичної Греції, древнього Китаю[8]. Захист головним чином зводився до права на усамітнення. Визначення приватності дуже різняться між собою і залежать від контексту. У багатьох країнах зроблено прив'язку до захисту даних, інтерпретуючи таким чином приватність з точки зору обробки інформації особистого характеру. За межами цього досить суворого контексту захист приватності часто має вигляд рамок того, наскільки далеко суспільство може втручатися в особисті стосунки[9].



Можна виділити кілька аспектів:

- **інформаційна приватність,** що включає в себе встановлення правил збору та обігу персональних даних, таких як інформація кредитних установ та медичні записи;
- **тілесна приватність,** що стосується захисту від втручань стосовно фізичного стану людей, наприклад, тестування щодо вживання наркотиків та обстеження порожнин;
- **комунікаційна приватність,** тобто безпека та приватність поштових відправлень, телефонних розмов, електронних повідомлень та інших видів комунікацій;
- **територіальна приватність,** що стосується встановлення обмежень на втручання в домашнє та інше навколишнє середовище, наприклад, робоче місце чи громадське оточення.

Відсутність єдиного визначення не повинно створювати враження, що це питання є неважливим. Як зазначив один письменник, «у певному розумінні, усі права людини є аспектами права на приватність»[10].

Декілька поглядів на приватність:

У дев'яностих роках минулого століття майбутній суддя Верховного Суду США Луїз Брандез сформулював концепцію приватності як права

особи «бути залишеною у спокої» («right to be left alone»). Брандез переконував, що приватність – найцінніша із демократичних свобод і виступав за те, щоб це було відображено в Конституції[11].

У преамбулі до австралійської Хартії приватності говориться, що «вільне та демократичне суспільство вимагає поваги до автономії особи та обмеження повноважень державних і приватних організацій порушувати цю автономію.... Приватність є ключовою цінністю, що тісно пов'язана з людською гідністю та іншими ключовими цінностями, як свобода асоціацій, свобода слова... Приватність – фундаментальне право людини, на яке кожна особа може сподіватись»[12].

Алан Вестін, автор праці 1967 року «Приватність та свобода», визначив приватність як прагнення людей вільно вибирати, за яких обставин та до яких меж вони будуть виставляти на показ перед іншими себе, свої переконання та свої дії[13].

На думку Едварда Блоуштейна, приватність – інтерес людини. Вона захищає незалежність та гідність особи[14].

На думку Рута Гавісона, існує три складових елементи приватності: таємність, анонімність, усамітнення. Це стан, який може бути втрачено або за вибором самої особи, або через дії іншої особи[15].

Британський Calcutt Committee визначив, що «нами ніде не було знайдено абсолютно прийнятного правового визначення приватності»[16]. Але комітет задовольнився можливістю знайти правове визначення і дав його у своєму першому звіті з питань приватності:

Право особи бути захищеною від втручання в її особисте життя та стосунки чи її родини безпосередньо фізичним шляхом або через публікацію інформації.

ПРАВО НА ПРИВАТНІСТЬ

Приватність може бути визначено як фундаментальне (проте не абсолютне) право людини. Витоки законодавства в галузі приватності можна знайти вже в 1361 році, коли англійські мирові судді застосовували арешт за підглядання та підслуховування[17]. У 1765 році британський Лорд Кемден, протестуючи проти санкції на доступ до приміщення та виїмки документів, писав: «Ми можемо із задоволенням сказати, що не існує закону в цій країні, яким можна було б виправдати дії підсудних; якби такі існували, це могло б зруйнувати всі суспільні цінності. Що ж стосується документів, то це – найдорожча власність, що належить людині»[18]. Член Парламенту Вільям Пітт писав: «Найбідніша людина може у своєму будинку не підкорятися навіть всій королівській владі. Будинок може бути хитким, його дах може бути ненадійним, його може продувати вітер, всередину може увірватися буря, може забивати дощ, – але Король Англії не може туди увійти, усі його повноваження на дають йому права переступати поріг халупи, що розвалюється».

У різних країнах протягом наступних століть розвивалися специфічні засоби захисту приватності. У 1776 році Парламент Швеції ухвалив Закон «Про доступ до офіційних документів», за яким державні органи були зобов'язані використовувати інформацію у передбачених законом цілях. У 1792 році Декларація про права людини та громадянина проголосила, що приватна власність є недоторканною та священною. У Франції 1858 року було заборонено публікацію фактів із приватного життя та встановлено високі штрафи за це[19]. У 1890 році американські юристи Самуель Воррен та Луїз Брандез дали визначення приватності як «право бути залишеним у спокої»[20].

Сучасну основу приватності можна знайти в Загальній декларації прав людини 1948 року, що в основному захищає територіальну та комунікаційну приватність. Згідно статті 12 декларації «ніхто не може зазнавати безпідставного втручання у його особисте та сімейне життя, безпідставного посягання на недоторканність його житла, таємницю його кореспонденції або на його честь і репутацію. Кожна людина має право на захист законом від подібних втручань чи посягань»[21].

Ціла низка міжнародних угод з прав людини має посилання на приватність як на право. Міжнародний пакт про громадянські й політичні права, Конвенція ООН про працівників-мігрантів[22], Конвенція ООН про права дитини[23] оперують однаковими поняттями[24]. На регіональному рівні ці права наповнюються більшою силою. Стаття 8 Європейської Конвенції з прав людини захищає право на приватність таким чином[25]:

1. Кожна людина має право на повагу до її особистого і сімейного життя, житла і таємниці листування.

2. Держава не може втручатися у здійснення цього права інакше ніж згідно із законом та у випадках, необхідних в демократичному суспільстві в інтересах національної і громадської безпеки або економічного добробуту країни, з метою запобігання заворушенням і злочинам, для захисту здоров’я або моралі чи з метою захисту прав і свобод інших людей.»

На підставі Конвенції з метою нагляду за дотриманням її положень засновано Європейську Комісію з прав людини та Європейський Суд з прав людини. Обидва органи виявляють велику активність у застосуванні права на приватність і послідовно дотримуються широкого тлумачення статті як засобу захисту і вузького тлумачення передбачених статтею обмежень[26]. У своєму першому рішенні щодо приватності Комісія зауважила: «На думку багатьох англосаксонських та французьких авторів право на повагу «приватного життя» є правом на приватність, правом жити за власним бажанням, правом бути захищеним від публічності»... На думку Комісії, однак, право на повагу приватного життя цим не обмежується. Воно включає в себе також певною мірою право встановлювати та розвивати стосунки з іншими людьми, особливо в емоційній сфері для розвитку та становлення особистості[27].

Суд розглянув законодавство держав-членів і наклав санкції на деякі країни за неврегульованість питань прослуховування з боку державних органів та приватних осіб[28]. Він також розглянув випадки, що стосуються доступу осіб до їхніх персональних відомостей у базах даних та реєстрах державних органів з тим, щоб пересвідчитися, що необхідні процедури запроваджено[29]. Ним розповсюджено захист, передбачений статтею 8, за межі діяльності державних органів. На них покладено обов'язок заборонити вчинення таких дій з боку приватних осіб[30]. Можливо, виходячи з таких взаємопов'язаних висновків, Суд міг би зобов'язати застосовувати закон про захист даних у випадках, коли дані оброблялись неналежним чином, завдаючи шкоду суб'єктові цих даних[31]. Стаття 11 Американської Конвенції про права людини в питанні приватності використовує термінологію, близьку до визначень Загальної декларації прав людини[32]. У 1965 році Організація Американських Держав проголосила Американську Декларацію про права та обов'язки людини, що містить у собі заклики до захисту багатьох прав людини, у тому числі права на приватність[33]. Міжамериканський суд з прав людини також почав звертатися у своїх рішеннях до питань приватності.

Еволюція захисту даних

Інтерес до права на приватність зріс в 60-х, 70-х роках XX століття з появою інформаційних технологій. Потенційні можливості для стеження з допомогою потужних комп'ютерних систем ставив на перший план вимоги встановлення спеціальних правил щодо збору та обігу інформації особистого характеру. У багатьох країнах це право було відображено в конституціях. Походження сучасного законодавства в цій сфері було закладено першим у світі законом про захист даних, який було введено в дію на землі Гессе в Німеччині в 1970 році. Наступними були національні законодавчі акти Швеції (1973), Сполучених Штатів (1974), Німеччини (1977) та Франції (1978)[34].

З цих законів виникло два надзвичайно важливих міжнародних інструменти. Це – прийнята в 1981 році Конвенція Ради Європи «Про за-

хист осіб у зв'язку з обробкою інформації про особу та відсутністю обмежень на переміщення такої інформації»[35] та Правила забезпечення захисту приватності у зв'язку із транскордонним переміщенням інформації про особу, встановлені Організацією Економічного Співробітництва та Розвитку (ОЕСР)[36], якими визначено спеціальні вимоги стосовно обігу електронних даних. Правила, встановлені цими двома документами, були покладені в основу законів про захист даних багатьох країн. Ці Правила визначають інформацію особистого характеру як дані, щодо яких встановлюється захист на кожному рівні їх використання від збору, зберігання до надання. Первинним серед цих Правил є право людини на доступ та внесення змін до своїх даних. Стосовно захисту даних немає великих розбіжностей у різних деклараціях та законах. Усі включають вимоги стосовно інформації особистого характеру. Отож, вона має бути:

- отримана чесним та законним шляхом;
- використаною лише із заздалегідь визначеною метою;
- відповідною до поставленої мети, без зайвої інформації, що виходить за межі визначеної мети;
- точною і регулярно оновлюватися;
- знищеною, коли мета досягнута.

Ці два договори мали великий вплив на прийняття законодавчих актів у всьому світі. Більше двадцяти країн дали згоду на дію Конвенції Ради Європи і ще шість її вже підписали, але вона ще не набрала чинності на їх територіях. Принципи ОЕСР також широко застосовуються в національному законодавстві різних країн, навіть тих, що не є членами ОЕСР.

Європейська Директива про телекомунікації та Європейська Директива про захист даних.

Протягом трьох останніх років Європейський Союз ухвалив дві директиви, що забезпечать громадянам більш широкий спектр механізмів захисту від зловживань їхніми даними. Директиви визначають рамковий загальний рівень забезпечення приватності, що не тільки підтверджує принципи, уже передбачені в законодавстві про захист даних, але розширює їх, встановлюючи спектр нових прав. Директива про захист даних визначає загальні принципи для національного законодавства, на підставі яких буде уніфіковано законодавство всіх країн-членів Європейського Союзу[37]. До жовтня 1998 року кожна країна, що є членом ЄС, має внести зміни до свого законодавства, хоча вірогідно, що не всі із них завершать цей процес до початку 1999 року. Директива про телекомунікації[38] встановлює особливий захист користувачів телефонів, цифрового телебачення, мереж мобільного зв'язку та інших систем телекомунікації.

Кілька принципів захисту даних посилено положеннями Директив, а саме: право знати походження даних, право виправлення неточних даних, право на оскарження в суді незаконної обробки даних та право на видачу дозволу на використання даних за певних обставин. Наприклад, особам надається право вільно та безкоштовно, за власним вибором, без повідом-

лення причини відмовлятися від отримання матеріалів, що розповсюджуються шляхом прямого маркетингу. Директивою про захист даних передбачено посилення засобів захисту стосовно використання вразливих персональних даних, наприклад, у сфері охорони здоров'я або фінансового характеру. У майбутньому використання державними та комерційними структурами такої інформації буде можливим лише за умов «чіткої та однозначної» згоди суб'єкта даних.

Основний зміст європейської моделі можна визначити як «забезпечення механізмами виконання». Європейський Союз прагне того, щоб суб'єкти даних мали чітко визначені права і також мали можливість звернутися до посадової особи чи органу, який має вжити певних дій на їх користь. У кожній країні, що є членом ЄС, буде призначено уповноваженого із захисту даних або інший орган, що впроваджуватиме правила стосовно їх захисту. Очікується, що країни, з якими співробітничають держави Євросоюзу, матимуть схожий рівень контролю.

Директива накладає зобов'язання на держави-члени забезпечити, щоб інформація особистого характеру стосовно громадян країн, що входять до Євросоюзу, передавалася та оброблялася за його межами лише на визначених законом підставах[39]. Ця вимога спричинила зростаючий тиск поза Євросоюзом на користь прийняття законів про приватність. Ті країни, що ухиляються від прийняття ефективних законодавчих актів про приватність, можуть бути позбавлені можливості обміну певними видами інформації з країнами-членами Європейського Союзу, особливо якщо вона містить вразливі дані.

Директива про телекомунікації накладає великий обсяг обов'язків на посередників та постачальників послуг щодо гарантій приватності користувачів засобів комунікацій. Нові правила заповнять прогалини існуючого законодавства про захист даних. Доступ до даних про фінансові розрахунки буде суворо обмежено, як і до даних про ринкову діяльність взагалі. Замовники засобів ідентифікації зобов'язані передбачити можливості для блокування кожної лінії передачі даних. Інформація про виконання комунікаційних послуг має знищуватися одразу ж після завершення сеансу зв'язку.

Моделі захисту приватності

Зараз існує кілька загальних моделей захисту приватності. У деяких країнах одночасно використовується кілька моделей.

Модель регулювання, що застосовується у Європі, Австралії, Гонконзі, Новій Зеландії, Центральній і Східній Європі та Канаді полягає в тому, що існує посадова особа, яка забезпечує виконання положень детально розробленого закону про приватність. Ця посадова особа (вона може називатися по-різному, наприклад: Уповноважений, Омбудсмен, Реєстратор) здійснює нагляд за дотриманням законності та проводить розслідування щодо виявлених порушень. У деяких випадках посадова особа може приймати певні рішення стосовно правопорушника. Посадова особа

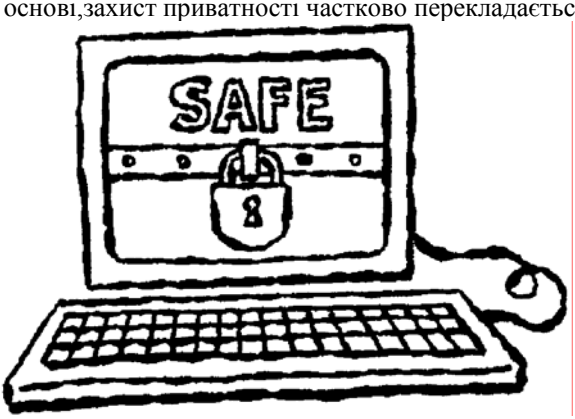
також відповідає за громадянську освіту та міжнародні стосунки щодо захисту даних та їх передачі. Такої моделі дотримуються більшість країн, де існують закони про захист даних. Цю модель також обрано Європою для створення нового режиму захисту даних. Однак коло повноважень таких органів дуже різниться, часто надходять повідомлення про серйозну нестачу засобів, що призводить до невиконання положень діючого законодавства.

Деякі країни, наприклад, Сполучені Штати уникають схвалення загальних принципів захисту даних, надаючи перевагу спеціальним секторальним законодавчим актам, таким як відеозаписи при укладенні договорів оренди та збереження приватності у фінансових питаннях. У подібних випадках виконання норм законодавства забезпечується з допомогою цілого комплексу засобів. Проблема цього підходу полягає в тому, що при появі нових технічних засобів виникає потреба в прийнятті нових законів, таким чином не завжди можна забезпечити надійний захист. Відсутність засобів правового захисту генетичної інформації в Сполучених Штатах є кричущим прикладом таких недоліків. В інших країнах вузькоспеціалізоване законодавство використовується як засіб посилення законів з широкою сферою правового регулювання, встановлюючи деталі захисту певних категорій інформації, таких, як поліцейські досьє або дані про користувачів кредитних установ.

Захист даних може забезпечуватися, принаймні теоретично, через різні форми саморегулювання, коли компанії та промислові підприємства встановлюють свої внутрішні правила. Однак аналіз таких зусиль підводить до невтішних висновків. Дуже небагато є свідчень того, що вдається досягти поставленої мети шляхом таких правил.

Адекватність та забезпечення виконання є головними проблемами в цьому підході. У багатьох країнах внутрішні правила мають тенденцію до забезпечення захисту в дуже обмеженому обсязі при наявності механізмів виконання. Така політика зараз здійснюється в Сполучених Штатах, Сінгапурі, Австралії.

У зв'язку з тим, що різні технічні засоби стають більш доступними на комерційній основі,захист приватності частково перекладається



і на індивідуальних користувачів. Так користувачі Інтернету можуть застосовувати різні програми та системи, що забезпечують різні ступені захисту приватності та безпеки засобів комунікацій. Але залишаються відкритими питання щодо безпеки та надійності таких систем. Нещодавно Європейська Комісія вивчила деякі з цих технологій та дійшла висновку, що вони не можуть замінити собою засоби правового захисту[40].

МЕХАНІЗМИ ПОРУШЕННЯ ПРИВАТНОСТІ

У цій доповіді наведено приклади технічних засобів, що викликають стурбованість стосовно захисту приватності. Багато з них застосовуються поза сферою правового захисту.

СИСТЕМИ ІДЕНТИФІКАЦІЇ

Ідентифікаційні картки

Ідентифікаційні картки в тій чи іншій формі використовуються практично в усіх країнах світу. Їх форма, призначення та зміст різняться між собою. У більшості країн існує офіційна національна ідентифікаційна картка встановленого зразку, однак у багатьох розвинених країнах такої картки не існує. Серед них Сполучені Штати, Канада, Нова Зеландія, Австралія, Сполучене Королівство, Ірландія та країни Півночі. Такі картки існують у Німеччині, Франції, Бельгії, Греції, Люксембурзі, Португалії та Іспанії.

Ідентифікаційні картки вводяться з різною метою. Старі ідентифікаційні системи були побудовані на даних стосовно раси, релігії, політичних переконань. Загроза повстань, релігійної дискримінації або політичного екстремізму використовувалася як спільне обгрунтування для введення систем ідентифікації, що має привести до визначення ворогів держави або зробити їх вразливими без необхідних документів. У Пакистані картки використовуються для реалізації системи квотування.

За останні роки ідентифікаційні картки пов'язують з національними системами реєстрації, що в свою чергу формують основу для державного управління. У таких системах, наприклад, Іспанії, Португалії, Таїланду та Сінгапуру ідентифікаційні картки стають лише одним видимим компонентом набагато більшої системи. З появою магнітних стрічок та мікропроцесорів такі картки можуть використовуватися для отримання послуг з боку державних органів. Таким чином картки стають поєднанням засобів ідентифікації та доступу до послуг. В основі цих планів є також паралельне розширення повноважень поліції. Навіть у демократичних країнах поліція має право вимагати посвідчення особи під загрозою затримання. У деяких країнах таку практику було успішно оскаржено на підставі конституційних гарантій приватності. У 1998 році Верховний Суд Філіппін ухвалив рішення про те, що національна система ідентифікації є порушенням конституційного права на приватність. У 1991 році Конституційний суд Угорщини дійшов висновку, що закон про введення багатоцільо-

вих особистих ідентифікаційних номерів порушує конституційне право на приватність[41].

Біометрія

Біометрія – це процес збору, обробки та зберігання персональних фізичних характеристик з метою ідентифікації та встановлення автентичності. Найбільш популярними видами біометричних систем є сканування сітківки ока, геометрія долоні, сканування великого пальця, відбитки пальців, розпізнавання голосу та відцифровані (що зберігаються в електронному вигляді) фотографічні зображення. Такі технології викликають інтерес як з боку державних органів, так і приватних компаній, оскільки на відміну від інших засобів ідентифікації, таких, як картки чи паперові документи, вони здатні гарантувати точну та глибоку ідентифікацію.

Засоби біометричної ідентифікації застосовуються у всьому світі. Іспанія почала застосовувати національну систему відбитків пальців для встановлення права на отримання виплат безробітнім та надання медичних послуг. Росія оголосила плани введення в банківській сфері національної системи електронних відбитків пальців. Жителі Ямайки зобов'язані пройти сканування великого пальця перед тим, як скористатися правом голосу. У Франції та Німеччині проходить випробування обладнання, що заносить на кредитну картку інформацію про відбитки пальців. Такі технології використовуються крамницями роздрібної торгівлі, державними органами, центрами догляду за дітьми, поліцейськими структурами, у засобах автоматичного підрахунку. Автоматизована імміграційна система, створена Службою імміграції та натуралізації Сполучених Штатів використовує геометрію долоні. Геометричні дані долоні осіб, що часто здійснюють подорожі, зберігаються на мікропроцесорних платах «розумних» карток. Подорожуючі кладуть свою долоню на сканер і вставляють картку в паз. У зв’язку з цим понад 70 000 осіб стали перед судом. Ця система може в результаті перерости у всесвітню систему ідентифікації подорожуючих.

Найбільш спірна форма біометрії – ідентифікація ДНК – має переваги при застосуванні з новими засобами сканування, що здатні протягом хвилин автоматично встановлювати відповідність ДНК зразкам, занесеним до великої бази даних. Поліцейські структури в деяких країнах, наприклад, Сполучених Штатах, Німеччині і Канаді створюють національні бази даних ДНК. У Сполученому Королівстві та Сполучених Штатах поліція вимагає, щоб особи в певних регіонах добровільно надали зразки, інакше їх будуть підозрювати.

Контроль за комунікаціями

Майже всі країни мають певні засоби, здатні знімати інформацію з каналів телефонного, факсимільного, телексного зв'язку. У більшості випадків такі перехоплення ініціюються та здійснюються правозастосовчими органами. Відомо про зловживання в сфері знімання інформації в бі-

льшості країн, іноді дуже масштабні, коли відбуваються тисячі випадків незаконного прослуховування. Зловживання незмінно стосуються осіб, що представляють «інтерес» для уряду. Об'єктами стають політичні опоненти, студентські лідери, правозахисники[42]. Правозастосовчі органи традиційно тісно співпрацюють з телекомунікаційними компаніями для створення можливостей, щоб телефонні системи добре прослуховувалися. Такі заходи є різними: від надання поліції фізичного доступу до телефонних станцій до встановлення обладнання для автоматичного перехоплення інформації.

Сполучені Штати є світовим лідером у докладанні зусиль для обмеження індивідуальної приватності і збільшенні можливостей своєї поліції та спеціальних служб підслуховувати особисте спілкування. Кампанія має два юридичних аспекти. Перший – зобов'язати всіх, хто забезпечує зв'язок з допомогою цифрових, мобільних, супутникових телефонів, та хто займається розвитком комунікаційних технологій, передбачити можливості для контролю; другий – обмежити розповсюдження програмного забезпечення для криптографії, технічних засобів, що надають людям можливості захисту своїх засобів комунікації та баз даних від доступу до них з боку інших осіб[43].

Водночас Сполучені Штати утримують лідерство в застосуванні електронного контролю та послабленні законодавства про банківську таємницю. Директор ФБР Луїз Фріх активно здійснював всесвітні вояжі з метою розширення застосування засобів зняття інформації в нових країнах вільного світу, таких, як Угорщина та Чеська Республіка.

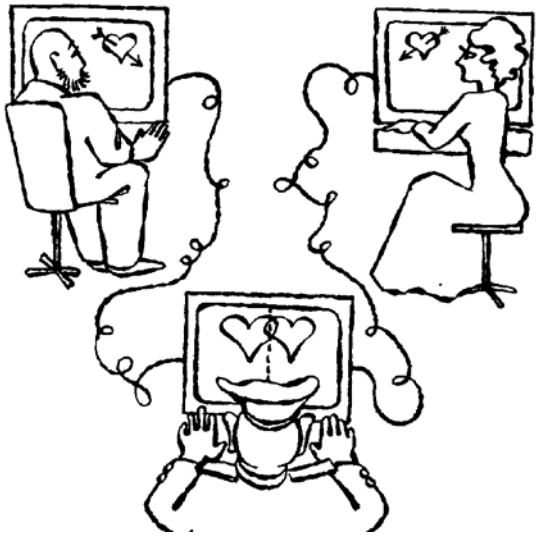
Контроль за Інтернетом та електронною поштою

За останнє десятиліття Інтернет став важливим засобом зв'язку та проведення досліджень. Технологічний розвиток відбувається дуже високими темпами, щороку з'являються мільйони нових користувачів. Усе більше зростає використання Інтернету з комерційною метою. Місткість, спроможність, швидкість та надійність Інтернету постійно зростають, що призводить до постійного розвитку та нового використання середовища.

Проте Інтернет не захищений від перехоплення інформації та контролю з боку органів влади.

Оскільки середовище є новим, йому часто бракує захисту, зокрема такого, що мають телефонні системи загального користування. Правозастосовчі органи та служби національної безпеки по всьому світу швидко почали нарощувати можливості для перехоплення й оцінки повідомлень електронної пошти та руху інформації через мережу Інтернет. Правоохоронні органи Сполученого Королівства намагаються переконувати, що перехоплення повідомлень електронної пошти має бути дозволено через укладення угоди між поліцією та провайдерами послуг Інтернету. Це викликало занепокоєння з боку правозахисних груп, які вимагають, щоб перехоплення повідомлень електронної пошти не відрізнялося від проце-

дур, встановлених для прослуховування телефонних розмов. У Сінгапурі доступ до Інтернету здійснюють організації, що самі є під контролем, або пов'язані з державними органами і, згідно з повідомленнями, регулярно надають інформацію урядовим структурам. У Росії обговорюється пропозиція про те, що всі провайдери послуг Інтернету мають встановити «чорну скриньку» та забезпечити високошвидкісну лінію для Федеральної



Служби Безпеки. «Анонімні ремейлери», які знімають встановлену інформацію з електронної пошти, можуть зупинити аналіз руху інформації. Вони є відповідниками абонентських скриньок в Інтернеті. Їх застосування також викликало спротив з боку поліції та служб розвідки. У Фінляндії популярний анонімний ремейлер припинив своє існування, через те що, використовуючи правові заходи, оператора змусили назвати одного із своїх користувачів.

Найбільш важливим засобом захисту від контролю стає криптографія. Повідомлення кодується таким чином, що лише та особа, для якої воно призначено, зможе розкодувати його і потім прочитати. Найбільш відомою програмою криптографії є «Досить добра приватність» (Pretty Good Privacy, PGP), якою користуються понад 100 000 користувачів, включаючи правозахисні групи, такі, як Міжнародна Амністія.

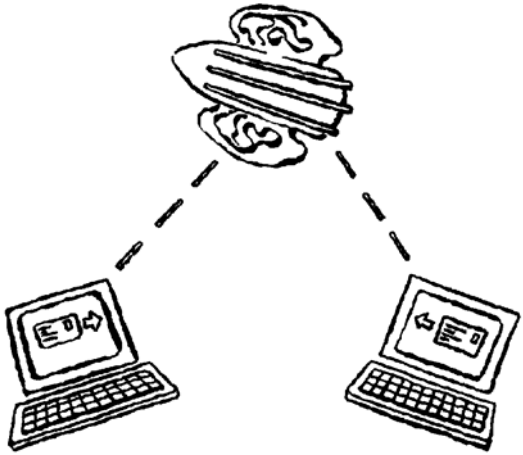
Однією з найбільших загроз для приватності в Інтернеті стає запис інформації про певну діяльність в Інтернеті. Кожного разу при відвідуванні веб-сторінки сервер, на якому розміщено сторінку, реєструє звернення користувача, при цьому фіксується час і дата звертання. Деякі сайти розміщують у машинах користувачів «cookies», що допомагає більш

детально спостерігати за діяльністю людей в Інтернеті. Інші запитують імена користувачів, адреси, іншу персональну інформацію перед тим, як надати можливість доступу. Купівля товарів через Інтернет контролюється таким же чином. Он-лайнівські крамниці дуже високо цінують таку інформацію, не в останню чергу за те, що її можна продати торгівцям та іншим організаціям. Уже винайдено деякі технічні засоби для запобігання таким діям. Програмне забезпечення, що гарантує анонімність, дозволяє користувачам відвідувати веб-сторінки, не повідомляючи своєї адреси в Інтернеті. Програми знищення cookies, що зараз передбачені в більшості браузерів, не дають можливості сайту розмістити cookies у машині користувача. Анонімний цифровий готівковий розрахунок дозволяє споживачам здійснювати платежі не називаючи себе.

Національна безпека і система Echelon

Одразу після закінчення Другої світової війни у 1947 році уряди Сполучених Штатів, Сполученого Королівства, Канади, Австралії та Нової Зеландії підписали пакт, відомий як «Quadripartite», або угода «Сполучене Королівство – Сполучені Штати « (UKUSA). Їхніми намірами було – встановити домовленості про те, яким чином можна досягнути спільних інтересів у галузі національної безпеки. Цією угодою п'ять держав поділили планету на п'ять сфер впливу, і для кожної країни було визначено спеціальні цілі. Угодою UKUSA передбачена стандартизація термінології, кодованих слів, процедур перехоплення інформації, заходи співробітництва, обмін інформацією і доступ до засобів обслуговування. Важливою частиною угоди був обмін інформацією та персоналом. Завдяки цьому оперативні працівники спеціальних служб зв'язку Нової Зеландії GCSD мають можливість використовувати в Канберрі засоби Австралійського Директорату захисту зв'язку для контролю за місцевими засобами комунікацій і передавати результати роботи спецслужбам Австралії. І жодна з цих держав не зобов'язана формально давати згоду чи повідомляти про перехоплення інформації[44].

Найбільш тісні зв'язки в межах стосунків UKUSA встановлено між Агентством національної безпеки США (NSA) та Британським штабом урядового зв'язку (GCHQ). Найбільш важливі засоби цього альянсу розташовані в Менвіс Хілл (Menwith Hill) на півночі Англії. База з двома дюжинами антен та широкими можливостями комп'ютерних засобів має умови для підслуховування широкого спектра засобів комунікації. З появою системи INTELSAT та цифрового телезв'язку в Менвісі та на інших станціях розвинено можливості для зняття інформації з широкого спектру засобів комунікацій: факсимільний телексний зв'язок, звукові повідомлення. Дуже поширеним припущенням є те, що Менвіс Хілл має 40 000 каналів, через це може забезпечуватися доступ до більшості європейських та радянських мереж комунікацій.



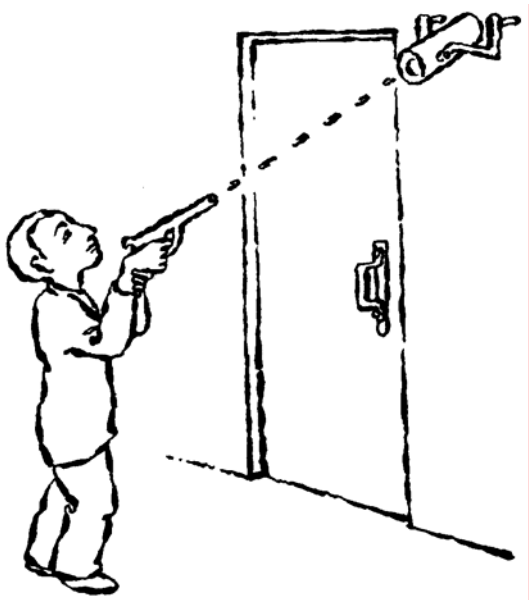
У звіті Європейського парламенту, опублікованому наприкінці 1997 року, підтверджується, що «Проект «Echelon» надає можливість NSA здійснювати пошук майже в усіх інформаційних мережах із допомогою «ключових слів». Зміст повідомлень не аналізується постійно і не переглядається в режимі реального часу, однак щоденні доповіді надають інформацію, яка допомагає спецслужбам визначати цілі для своєї подальшої діяльності. Автоматичний контроль звукових засобів комунікації може бути не за горами. Система голосового розпізнавання «Oratory» вже кілька років використовується для перехоплення та аналізу дипломатичних телефонних розмов[45]. У звіті «Оцінка технологій політичного контролю» сказано: «По всій Європі всі засоби комунікацій телефонного, факсимільного зв'язку, а також повідомлення електронної пошти регулярно перехоплюються Агентством національної безпеки Сполучених Штатів, при цьому визначена інформація передається з Європейського материка через стратегічний вузол у Лондоні, потім з допомогою супутника в Форт Мед (Fort Meade) в Меріленді через важливий вузол в Менвіс Хілл, що поблизу Північного Йорку в Сполученому Королівстві». Звіт викликав хвилю стурбованості, що спричинило обговорення цієї проблеми в Європейському парламенті 14 вересня 1998 року. У «компромісному рішенні», виробленому того дня чотирма головними сторонами, міститься заклик до більшої звітності та використання «засобів захисту» стосовно діяльності спеціальних служб.

ВІДЕОСТЕЖЕННЯ

За останні роки використання камер відеостеження – Приховане кругове телебачення – ПКТБ (Closed Circuit Television, CCTV) досягло в усьому світі безпрецедентного рівня. Лише у Сполученому Королівстві витрачається щороку від 150 до 300 мільйонів фунтів стерлінгів на індус-

трію стеження, що включає близько 200 000 камер для контролю за громадськими місцями[46]. Більшість міст та містечок починають користуватися ПКТБ для стеженням за такими місцями, об'єктами нерухомості та автостоянками. Зростання ринку таких засобів оцінюється приблизно в 15-20 відсотків щороку. Багато центральних ділових кварталів Великобританії контролюються зараз при допомозі систем відеостеження , включаючи системи пов'язаних між собою камер для створення повної панорами, можливостями зміни положення камер у просторі, зміни масштабу зображення, використання інфрачервоного випромінювання. Їхнє використання у приватній власності також стає популярним[47].

Такі системи мають складну технологію. Використовується також нічне бачення, комп'ютерна обробка і можливості визначення рухливих об'єктів. Це дозволяє операторові передбачити можливості, щоб система подавала сигнал тривоги, коли що-небудь рухається перед об'єктивом камери.



Системи відеокамер усе більше виконують функцію куленепробивного жилета та засобів автоматичного самозахисту. Якість зображення, як правило, є досить високою. З допомогою багатьох систем можна прочитати назву сигарет на коробці, маючи відстань сто метрів. Часто такі системи можуть працювати в суцільній темряві, при цьому забезпечуючи зображення як при денному світлі. Технічні засоби будуть врешті пов'язані із складним програмним забезпеченням, що дозволить автоматично розпізнавати обличчя, аналізувати поведінку натовпу і (в певному середовищі) досить близько спостерігати, що відбувається між поверхнею

шкіри людини та її одягом. Можливості камер будуть і надалі зростати, у той час як вартість і розміри будуть зменшуватися. Слід узяти до уваги, що таємне візуальне стеження в певних місцях буде повсюдним.

Тенденції щодо використання ПКТБ не обмежуються лише Великобританією. Швеція, що колись була опозиційно налаштована до такого стеження, зараз розглядає можливість послаблення законодавства про приватність, щоб розширити громадське стеження, у той час як у Норвегії використання ПКТБ спричинило введення до закону про захист даних спеціальних положень про такий вид стеження. Тим часом використання ПКТБ для контролю за публічними місцями помітно зросло в Північній Америці та Австралії. У Сінгапурі вони широко використовуються для контролю за дотриманням правил дорожнього руху та для запобігання засмічуванню.

На думку деяких спостерігачів, це явище драматичним чином змінює природу міст. Ці технічні засоби здобули назву «п'ятої послуги». ПКТБ інтегрується в міське середовище таким же чином, як електроприлади та телефонні мережі в першій половині цього століття. ПКТБ спричинює глибокі зміни міського середовища, і зараз це є важливою частиною міського управління. Візуальне стеження стає встановленим компонентом при плануванні нових міських центрів, житлових районів, громадських будівель і навіть систем дорожнього сполучення. Зображення, отримані з допомогою ПКТБ, можуть у майбутньому розглядатися як ще один тип необхідної інформації і визначатися як продукт, що складає «додану вартість».

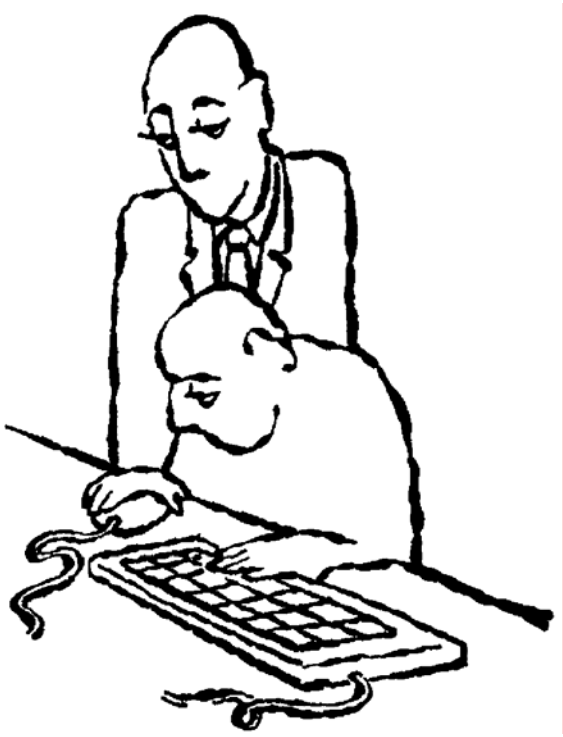
Стеження на робочому місці

Майже в кожній країні службовці є вразливими стосовно всебічного контролю з боку своїх керівників. Правовий захист за таких обставин більш слабкий, оскільки такий контроль часто включається в умови працевлаштування. У багатьох країнах роботодавці можуть прослуховувати телефонні розмови, читати повідомлення електронної пошти та інформацію на моніторі комп'ютера своїх працівників. Вони можуть підслуховувати розмови, аналізувати роботу комп'ютера і клавіатури, спостерігати за допомогою камер ПКТБ, використовувати обладнання для стеження та контролю за діями осіб, робити аналіз сечі, щоб виявити вживання наркотиків і вимагати інформацію інтимного характеру.

Засоби, що використовуються для контролю за працівниками, є надзвичайно потужними. Вони можуть аналізувати «ключові елементи» для визначення, чи ефективно працівники використовують свій час між телефонними розмовами. Компанії-виробники програмного забезпечення називають цей процес «контролем за виконанням». Навіть на робочих місцях, які займають висококваліфіковані спеціалісти у галузі інформаційних технологій, керівники вимагають права на стеження за кожною деталлю роботи працівників. Сучасні системи мереж можуть допитувати комп'ютери, щоб визначити, яке програмне забезпечення використовується, наскільки часто і для чого. Всебічне стеження з метою ревізії до-

зволяє менеджерам складати образ кожного користувача і робити огляд того, як працівники взаємодіють із своїми машинами. Програмне забезпечення надає також менеджерам можливість повного централізованого контролю за програмним забезпеченням кожного персонального комп'ютера. Менеджер може зараз на відстані змінювати або припиняти роботу програм на будь-якій машині.

Такі технології поширюють свою дію на всі аспекти життя працівників. Мініатюрні камери контролюють поведінку. «Розумні» ідентифікаційні значки стежать за пересуванням працівників навколо будівлі. Системи телефонного управління (Telephone Management Systems (TMS) аналізують використання телефонів та місця, куди спрямовуються телефонні виклики. Психологічне тестування, загальнорозумове тестування, тестування спроможності, тестування виконавських якостей, тестування на визначення професійного інтересу, особистісні тестування та тестування на чесність – усі вони оцінюються електронним шляхом. Стеження та контроль стають запланованими частинами сучасних інформаційних систем.



У той час, коли компанії стверджують, що таке стеження – виправдане, є цілком зрозумілим, що не всі здійснюють контроль на законних підставах. Після певної організаційної діяльності місцевої спілки один

роботодавець у США встановив відеокамери, щоб стежити за кожним працівником та його робочим місцем. Хоча керівництво заявило, що ці технічні засоби встановлювалися виключно для контролю безпеки, двох службовців тимчасово усунули від роботи за те, що вони залишили робочі місця, не запитавши дозволу піти в туалет. Згідно з доповіддю відділу міжнародної праці (International Labour Office), діяльність представників профспілки було значно обмежено «ефектом залякування» працівників, які знали, що їхнє спілкування контролюється.

Цілий потік широко розголошених випадків про схожі зловживання візуальним стеженням спричинив стурбованість на робочих місцях. У 1991 році опитування працівників, проведене по всій території Сполучених Штатів виявило, що 62 відсотки не згодні з використанням відеостеження (включаючи 38 відсотків, що «абсолютно не згодні»). Однак, нещодавній звіт Американської асоціації управління (American Management Association) показує, що дві третини американських керівників шпигують за своїми працівниками, часто використовуючи перехоплення повідомлень електронної пошти та телефонних розмов[48].

У звіті, що має назву «Робочий стрес» сказано, що хворобою XX століття Міжнародна Організація Праці «вважає зростання прикладів проблем по всьому світу, включаючи країни, що розвиваються, коли … компанії роблять надто мало, щоб допомогти працівникам подолати напруження сучасної індустріалізації». У звіті також сказано, що «оскільки використання комп'ютерів поширюється в усьому світі, працівники в багатьох країнах стають об'єктами нових утисків, включаючи електронне підслуховування керівниками…». Проведене в 1990 році опитування працівників засобів телекомунікацій, частково профінансоване об'єднанням американських працівників засобів телекомунікацій, виявило, що 84 відсотки працівників, які знаходилися під контролем, скаржились на високе напруження, у той час як серед тих, хто не знаходився під контролем – лише 67 відсотків. У дослідженні, проведеному пізніше Управлінням США з питань оцінки технологій (US Office of Technology Assessment), також зазначено, що контроль за робочим місцем «сприяє виникненню стресів та захворювань, пов'язаних із стресом»[49].

У Великобританії та Сполучених Штатах існують деякі законодавчі обмеження для використання відеостеження, на відміну від законів Австрії, Німеччини, Норвегії та Швеції, відповідно до яких роботодавець зобов'язаний дійти згоди з працівниками в цих питаннях.

Така ситуація розглядалась у Європейському Суді з прав людини. Колишній британський помічник начальника поліції Елісон Хелфорд скаржилась, що після подання нею скарги на поліцію стосовно статевої дискримінації, її робочий телефон почали прослуховувати. У той час, як уряд Великобританії стверджував, що це були законні і правильні дії, Хелфорд стверджувала, що це є порушенням права на приватність, передбаченого Європейською Конвенцією про права людини. Суд із цим погоди-

вся і визнав, що поліція вчинила невірно, прослуховуючи телефон пані Хелфорд[50].

На практиці ж, очевидно, закони, що вироблені на підставі Європейської Директиви про телекомунікації, будуть порушуватися. У цей час, однак, рішення Суду, здається, робить трохи більше, ніж зобов'язує керівників повідомляти працівників, що вони не повинні очікувати на приватність при користуванні телефоном. І, відповідно, більшість справ рухаються в напрямку встановленого контролю над телефонними викликами.

Посилання

1. Directive 95/ /EC of the European Parliament and of the Council of On the Protection of Individuals with regard to the processing of personal data and on the free movement of such data.

2. Simon Davies «Re-engineering the right to privacy : how privacy has been transformed from a right to a commodity», in Agre and Rotenberg (ed) «Technology and Privacy : the new landscape», MIT Press, 1997 p.143.

3. Simon Davies and Ian Hosein, «Liberty on the Line» in Liberating Cyberspace, Pluto Press, London, 1998.

4. Big Brother Incorporated, Privacy International site: <http:// www.privacy.org/pi/reports/>.

5. Published by Science and Technology Options Assessment (STOA). Ref : project no. IV/STOA/ RSCH/LP/politicon.1

6. James Michael, Privacy and Human Rights, UNESCO 1994 p.1.

7. Richard Hixson, Privacy in a Public Society: Human Rights in Conflict 3 (1987). See Barrington Moore, Privacy: Studies in Social and Cultural History (1984).

8. Ibid. at 5.

9. Simon Davies «Big Brother : Britain's web of surveillance and the new technological order», Pan, London, 1996 p. 23

10. Volio, Fernando. «Legal personality, privacy and the family» in Henkin (ed) The International Bill of Rights, New York : Columbia University Press, 1981.

11. Samuel Warren and Louis Brandeis, «The right to privacy», Harvard Law Review 4, 1890 pp 193-220.

12. «The Australian Privacy Charter», published by the Australian Privacy Charter Group, Law School, University of New South Wales, Sydney 1994.

13. Alan F Westin, Privacy and Freedom, Atheneum, New York p. 7.

14. Privacy as an Aspect of Human Dignity, [1964] 39 New York U. L.R. 962 at 971.

15. 9 Privacy and the Limits of Law, [1980] 89 Yale L.J. 421, at 428.

16. Report of the Committee on Privacy and Related Matters, Chairman David Calcutt QC, 1990, Cmnd. 1102, London: HMSO, page 7.

17. James Michael, p.15

18. Entick v. Carrington, 1558-1774 All E.R. Rep. 45.

19. The Rachel affaire. Judgment of June 16, 1858, Trib. pr. inst. de la Seine, 1858 D.P. III 62. See Jeanne M. Hauch, Protecting Private Facts in France: The Warren & Brandeis Tort is Alive and Well and Flourishing in Paris, 68 Tul. L. Rev. 1219 (May 1994).

20. Warren and Brandeis, The Right to Privacy, 4 Harvard L.R. 193 (1890).

21. Universal Declaration of Human Rights, <http://www.hrweb.org /legal/udhr.html>

22. A/RES/45/158 25 February 1991, Article 14.

23. UNGA Doc A/RES/44/25 (12 December 1989) with Annex, Article 16.

24. International Covenant on Civil and Political Rights, <http:// www.hrweb.org/legal/cpr.html>

25. Convention for the Protection of Human Rights and Fundamental Freedoms Rome, 4.XI.1950. <http://www.coe.fr/eng/legaltxt/5e.htm>.

26. Nadine Strossen, Recent US and Intl. Judicial Protection of Individual Rights: A comparative Legal Process Analysis and Proposed Synthesis, 41 Hastings L.J. 805 (1990).

27. X v. Iceland, 5 Eur. Commнn H.R. 86.87 (1976).

28. European Court of Human Rights, Case of Klass and Others: Judgement of 6 September 1978, Series A No. 28 (1979). Malone v. Commissioner of Police, 2 All E.R. 620 (1979). See Note, Secret Surveillance and the European Convention on Human Rights, 33 Stanford Law Review 1113, 1122 (1981).

29. Judgement of 26 March 1987 (Leander Case).

30. Id at 848, 849.

31. Rolv Ryssdal, Data Protection and the European Convention on Human Rights in Council of Europe. Data protection, human rights and democratic values, XIII Conference of the Data Commissioners 2-4 October 1991, 41-43. (1992).

32. Signed Nov. 22, 1969, entered into force July 18, 1978, O.A.S. Treaty Series No. 36, at 1, O.A.S. Off. Rec. OEA/Ser. L/V/II.23 dec rev. 2.

33. O.A.S. Res XXX, adopted by the Ninth Conference of American States, 1948 OEA/Ser/. L./V/I.4 Rev (1965).

34. An excellent analysis of these laws is found in David Flaherty, «Protecting Privacy in surveillance societies», University of North Carolina Press, 1989.

35. Convention fn the Protection of Individuals with regard to the Automatic Processing of Personal Data Convention , ETS No. 108, Strasbourg, 1981. <http://www.coe.fr/eng/legaltxt/108e.htm>.

36. OECD, Guidelines governing the Protection of Privacy and Transborder Data Flows of Personal Data , Paris, 1981.

37. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.<http://www.odpr.org/-restofit/Legislation/Directive/Directive_Contents.html>.

38. Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector (Directive 97/66/EC of the European Parliament and of the Council of Europe of 15 December 1997). <http://www2.echo.lu/legal/en/dataprot/protection.html>.

39. Article 25 of the Directive stipulates that in many circumstances, the level of protection in the receiving country must be «adequate» – an expression which is widely accepted to mean «equivalent». Article 26 lays out certain options for transferring data out of Europe in circumstances where the level of protection is not deemed adequate. These include consent and contracts.

40. Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS).

<http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/wp11en.htm>.

41. Constitutional Court Decision No. 15-AB of 13 April 1991.

<http://www.privacy.org/pi/countries/hungary/hungarian_id_decision_1991.html>.

42. U.S. Department of State Singapore Country Report on Human Rights Practices for 1997, January 30, 1998.

43. See Banisar and Davies, The Code War, Index on Censorship, January 1998.

44. James Bamford, The Puzzle Palace, Penguin Books, 1981.

45. European Parliament, Scientific and Technological Options Assessment (STOA), An Appraisal of Technologies of Political Control, 6 January 1998. <http://jya.com/stoa-atpc.htm>.

46. House of Lords, Science and Technology Committee, Fifth report, «Digital images as evidence», 3 February 1998, London.

47. Stepehen Graham, John Brooks, and Dan Heery мTowns on the Television : Closed Circuit TV in British Towns and Citieso; Centre for Urban Technology, University of Newcastle upon Tyne.

48. American Management Association, Report on Electronic Monitoring & Surveillance, 1997.

<http://www.amanet.org/survey/elec97.htm>.

49. Office of Technology Assessment, New Technology, New Tensions, September 1987.

50. Halford v United Kingdom (Application No 20605/92), 24 EHRR 523, 25 June 1997.

Переклад з англійської Романа Романова

Саймон Девіс, генеральний директор Privacy International

ЧАС ДЛЯ БАЙТУ ПРИВАТНОСТІ

(друкується із незначними скороченнями)

ЗАМІСТЬ ПЕРЕДМОВИ

Переклад статті Саймона Девіса (джерело – INDEX Online, електрона версія журналу INDEX on Censorship) мусить бути дуже цікавим для читача – як в теоретичній площині, так і в практичній. Цей матеріал присвячено такій гострій проблемі як повага до приватного та сімейного життя з боку засобів масової інформації. І якщо скептики можуть сказати, що різні там «електронні штучки» не становлять великої загрози для приватності громадян в «недорозвинутих країнах», а лише для «постіндустріального суспільства», то актуальність проблеми балансу між приватністю та відкритістю (privacy and trancparency) саме для нас навряд чи хтось поставить під сумнів. Відсутність гострих конфліктів навколо цієї проблеми не означає, що в Україні її не існує. Яскравим прикладом може служити сусідня Російська Федерація, де активний розвиток ринку засобів масової інформації, потужні фінансові вливання від так званих «олігархів» та совєтські правові традиції, які взагалі не враховували таку категорію як приватність, призвели до цілої низки крупномаштабних скандалів. Згадайте фотоплівку з колишнім міністром юстиції Валентином Ковальовим, відеофільм з Генеральним прокурором Юрієм Скуратовим, публікацію в пресі стенограм телефонних розмов Тетяни Д'яченко, порушену кримінальну справу проти Сергія Лісовського (його підозрюють саме у порушенні недоторканності приватного життя)...

Отже, виникає дуже складне і суперечливе питання, відповідь на яке не є очевидною. Чи варто вводити обмеження свободи слова, якщо пройшло не більше 10 років, як ми маємо хоча б відносно вільну пресу? Чи не будуть будь-які обмеження використані владою в своїх інтересах? Дуже широка дискусія іде зараз з цього приводу знову ж таки в Росії. Обидві палати Федеральних Зборів підтримали ідею створення органу, який стежив би за дотриманням «моральності», проте, президент Росії Борис Єльцин наклав вето на відповідний законопроект, ставши на захист свободи слова.

Проте, насправді стаття пана Девіса зачіпає більш широке коло питань, ніж лише захист приватності від втручання з боку преси. Чи можете Ви собі уявити активне громадянське суспільство, здатне підкорити державу своїм інтересам в умовах, коли державні органи мають можливості для тотального контролю за будь-якою інституцією цього

самого громадянського суспільства? Чи не становить це загрозу для держав, що побудовані на таких принципах? А чи не становить це ще більшу загрозу для тих держав, де громадянське суспільство знаходиться лише на початку свого розвитку і поки що не може нав'язувати свою волю державним органам? Тож яким буде баланс між державою та суспільством в недалекому майбутньому?

На моє тверде переконання, теза про невелику актуальність подібних загроз для бідних держав на кшталт України не є переконливою. Безперечно, пенсіонерові, що кілька місяців не може отримати встановлену державою пенсію у розмірі близько 12 доларів США, навряд чи видається такою вже важливою проблема стеження за користувачами мобільних телефонів, кредитних карток та контролю за відвідувачами певних сайтів в Інтернеті. Однак в тих державах, які ставлять своїх громадян в умови на межі виживання, де вплив громадянського суспільства не є співвимірним із владою державних органів, шкода від посилення контролюючих можливостей держави може бути особливо великою. Відсутність коштів також не є сильним аргументом, адже ціни на мерседеси також є дуже високими, проте, українські чиновники полюбляють їздити на дорогих автомобілях. Незважаючи на постійне зменшення ВВП, починаючи від Адміністрації Президента і закінчуючи Верховним Судом, скрізь проведено так званий «євроремонт». Таких прикладів можна наводити безліч (чого варта лише суперечка з використанням ЗМІ та прокуратури між паном Кучмою та паном Лазаренко про те, хто більше дачних будинків побудував та відремонтував за рахунок українських платників податків!). Отже, чи може наш чиновник відмовитися від соблазну запровадити ефективну систему збору компромату, навіть якщо витрати на неї будуть дуже високими? Маю побоювання, що ні.

Роман Романов

Уряди із задоволенням переконують, що права не є статичними. Часи змінюються. Громадська непокора, кажуть вони, потребує обмеження права на свободу об'єднань. Інтернет вимагає нового погляду на свободу висловлювань. Через організовану злочинність виникла необхідність фундаментального перегляду прав власності.

З таким же задоволенням засоби масової інформації поширюють ці аргументи. З точки зору багатьох засобів інформації, баланс між правами, що задовільняв наших батьків, має небагато спільного з пригноблюючими загрозливими реаліями сьогодення. Зміни – як технологічного характеру, так і в поведінці людей – вимагають від нас постійного перегляду обсягу індивідуальних свобод.

Такий погляд є справедливим лише за окремих умов. Права людини мають спиратися на міцну змістовну основу, інакше вони будуть поховані. Перегляд часто призводить до ерозії. Якщо існує переконливий аргумент за зменшення прав заради суспільних інтересів, то водночас є ще

більш переконливий аргумент на користь посилення прав, коли існує загроза індивідуальним свободам. Велика кількість прав потребує посилення і в першу чергу, як жодне інше – право на приватність.

Кожного разу коли захисники громадянських прав обговорюють знищення приватності, головну їх стурбованість викликає проблема розвитку різних форм стеження. В наші дні це залежить перш за все від інформаційних технологій.

Діапазон нових технологій і майже необмежений спектр їхніх функцій створюють плаваючу економіку, побудовану на стеженні. Стрімкий розвиток обладнання для аудіо- та відеостеження, ідентифікаційні технології та системи збору даних створили безпрецедентні можливості для поліції та спецслужб. Стеження все більше стає невід'ємним компонентом інформаційно забезпеченої економіки. Дані кожної повнолітньої людини в розвинутому світі вміщено в середньому до 200 комп'ютерних баз данних.

Технології наступного покоління будуть використовувати зростаюче злиття між людьми та технологіями. Сфери життя, що традиційно визнавалися приватними, будуть в значній мірі виставлені напоказ. Технологічна конвергенція підтвердить, що всі машини зможуть вчасно контактувати між собою.

Зараз іде створення глобальної інформаційної інфраструктури – потенційно найбільшої потужності з часів народження автомобіля. Масове стеження швидко розвивається від Аргентини до Замбії не лише за допомогою відеокамер, дослідження ДНК, сателітарного стеження, поліцейських систем та кредитних установ, але й через неймовірно широкі можливості комп'ютерних систем контролю. Навіть зараз мобільні телефони та банківські машини створюють механізми, які можна застосовувати для географічного стеження в режимі реального часу. Пошукові системи Інтернету детально відображають діяльність та інтереси конкретних людей. Це дозволяє владним структурам збирати дані як суспільного, так і приватного характеру. І поява цього контрольованого суспільства приведе нас в нову еру соціального контролю. Ці дві речі ідуть поруч.

Нещодавно в своїй статті, опублікованій в «Гардіан», газетний магнат Девід Берклі, власник газети «Єуропін», застеріг: «Ніколи раніше ми, як індивіди, так не потребували захисту як тепер». Він запропронував, щоби «право на приватність охоплювало всі форми втручання у... «внутрішнє коло», всередині якого будь-хто може жити приватним життям за його власним вибором».

Отже, йдеться про відносини приватності та засобів інформації. Це покоління бачило значне збільшення втручання засобів інформації в приватне життя. Нові технології створюють умови для втручань в приватне життя в такому масштабі, що навряд чи хтось міг би уявити собі навіть 20 років тому. Дійсно, загроза з боку засобів інформації для приватності ко-

жного зростає щодня. Цифрування, тобто перетворення слів в електронні біти означає, що дані від засобів інформації швидко стають доступними в багатьох «машинозчитувальних» формах, які можуть бути проаналізовані, дубльовані, збережені і передані. Глобалізація гарантує розвиток цього процесу в усесвіті. У поєднанні з потужними засобами пошуку даних вплив на життя людей, їх добробут та репутацію може бути руйнуючим. Засоби інформації, що використовують такі технології, не повинні застосовувати одні правила для державних структур, а інші для себе.

Аргументом на користь кращого захисту приватності проти такого поєднання сил має бути вимушеність. Але смерть принцеси Діани висунула на перший план рідкісну єдність серед засобів інформации всього розвинутого світу: закони про приватність шкідливі для вільного суспільства. Комісія з питань скарг щодо преси (The Press Complaints Commission), якою встановлено існуючий режим саморегулювання в Англії, також виступає проти законодавства щодо приватності. Голова Комисії Лорд Вокхем, всупереч своїм попереднім виступам, зазначає: «Деякі люди намагаються випустити приватність із її пляшки».

В своїй статті Девід Берклі яскраво висвітлив зв'язок між сферою традиційного стеження з боку поліції та інших державних органів і сучасною практикою засобів інформації, але обмежився підтримкою прав, встановлених діючим законодавством. «Зловживання владою преси», підсумував він, є неприйнятним. Я вважаю, що набагато гірше, однак, було би прийняття нового законодавчого акту Британії, який би обмежував свободу преси. Берклі вважає, що такий закон посилив би зловживання владою з боку держави, і загроза диктатури могла би стати реальною.

Права на приватність не повинні бути продані так дешево. Питання захисту приватності стосується не тільки рарагаzzі та відомих людей. Вони є не менш важливими і для звичайних людей в екстраординарних ситуаціях. Хворі на СНІД, сім'ї потерпілих від нещасних випадків та глобальних катастроф, члени політичних партій – всі вони мають право на життя без переслідування. Ті, хто, провів якийсь час у в'язниці... мають право на приватність. Прийомні діти, вагітні жінки, любителі тварин і тренери-ентузіасти за певних обставин, можуть відчути себе жертвами небажаного втручання з боку засобів інформації, незалежно від намірів останніх. Життя цих людей і мільйонів до них подібних не можуть використовуватися для захисту будь-яких суспільних інтересів, проти права на приватність.

Враховуючи все це, яким міг би бути практичний вплив права на приватність? Можливо, так звані журналістські розслідування, багато в чому мають змінитися. Але, головним чином, закон просто відбив би вже існуючі кодекси поведінки асоціацій журналістів. Аргументи, висловлені Лордом Вакхемом, Рупертом Мурдахом та іншими, що багаті і впливові люди будуть використовувати новий закон, щоби «заткнути рота» пресі –

безпідставні. Засоби інформації, здається, звертають мало уваги на внутрішні загрози, типу монополізації преси, конфліктів інтересів, грошових винагород, самоцензури, редакційної звітності... Загроза контролю через частину законодавства, здається, викликає більший інтерес засобів інформації, ніж загроза заборони чи судового процесу.

Європейська Конвенція з прав людини, що скоро стане частиною внутрішнього права Великобританії, визнає приватність і свободу слова як рівні права. У нашому сучасному суспільстві вони є сумісними, а не конфліктуючими. Ті, хто намагається протиставляти ці поняття, обслуговують свої власні інтереси, ставлячи їх вище суспільного блага. Я вважаю, що ця проблема має законодавче рішення, яке відповідає двадцять першому століттю, і що ми маємо прагнути його знайти. Всі ми – захисники приватності і професійні працівники засобів інформації – працюємо, щоб наше суспільство стало більш справедливим, щоб керівництво ним здійснювалося більш відкрито та відповідально.

Переклад з англійської Романа Романова

Андрій Пазюк, Privacy Ukraine

ПРИВАТНІСТЬ ТА ІНТЕРНЕТ

Право на приватність та Інтернет – два явища, які з'явилися у двадцятому столітті і зобов'язані йому своїм народженням. Перше з'явилося раніше, на початку століття. Друге – на півстоліття пізніше, і, як молодше, спробувало похитнути старше, звести приватність мешканців кібернетичного простору – користувачів Інтернет – нанівець.

Як відзначив один з авторів в журналі «Економіст» за травень 1999 року, за назвою «Кінець приватності»[1]:

Обсяг даних, що записуються про людей буде продовжуватися розширюватися драматично. Диспути про приватність стають все більш різкими. Спроби стримати суспільство суцільного спостереження через нові закони будуть посилюватися.

Ось стрімкий прогноз: всі ці спроби стримати поширення хвилі електронного втручання в приватність будуть провалені … люди почнуть відчувати, що вони просто не мають приватності. Це буде знаменувати одну з найбільших соціальних змін сучасного часу…

Однак, напевно, автор цих песимістичних строк перебільшує. Ідея приватності, яка нерозривно пов'язана із категорією свободи особистості, здатна суттєво впливати на самий розвиток інформаційного суспільства. Здатна об'єднувати людей, які цінують власну інформаційну свободу. Є непоодинокі випадки, коли завдяки наполегливості користувачів у відстоюванні своїх інтересів, вдалося запобігти або припинити порушення приватності в Інтернет.

Так, у 1996 році, компанія Yahoo зазнала публічний протест через застосування систему пошуку людей. Можливості системи дозволяли відсортирувати 175 мільйонів людей, відібравши їх із списків прямої розсилки реклами. Після отримання претензій, Yahoo вирішила знищити 85 мільйонів даних з адресами користувачів, що не було включено до цих списків. У 1997 році, компанія American Online (AOL) оприлюднила плани стосовно розкриття даних про телефоні номери дописувачів своїм партнерам по телемаркетингу. Дописувачі виступили проти цього і зазначили, що це суттєво порушувало б умови угоди про надання послуги. У відповідь, компанія відмовилася від своїх планів[2].

---

[1] «The End of Privacy», The Economist, 1 May 1999, 11.

[2] Jerry Berman, Deirdre Mulligan. Privacy in the Digital Age: Work in Progress // Nova Law Review. – Vol. 23. – #2. – Winter 1999.

Це дає сподівання, що проблема забезпечення приватності в Інтернет буде вирішуватися. Однак постійний розвиток існуючих і поява нових технологій вимагають прийняття адекватних заходів для забезпечення право на повагу до приватного життя користувачів глобальної інфраструктури Інтернет.

ПРАВО НА ПРИВАТНІСТЬ

Для визнання того факту, що приватне життя людини має правову цінність знадобився певний розвиток цивілізації. Своє світове визнання право на приватність (right to privacy) отримало саме у двадцятому столітті, що пов'язано із появою нових технологій, завдяки яким втручання у приватну сферу життя людину значно спростилося.

У своїй статті, в 1890 році, американські юристи Луїс Д. Брендіс та Самуел Д. Варрен писали: «сучасні винаходи і бізнес методи вимагають уваги до наступних кроків, що мають бути зроблені для захисту індивідів»[3]. Автори зробили першу спробу дати визначення праву на приватність. На їх думку, це право «бути залишеним на самоті»(let to be alone), яке несе в собі ідею захисту результатів інтелектуальної і емоційної активності особи в суспільстві.

З розвитком телекомунікаційних технологій, появою комп'ютерів і поширенням автоматизованої обробки персональних даних, концепція приватності набуває більше інформаційного змісту. У відомому рішенні Федерального Конституційного Суду Німеччині 1983 року воно сформульовано як право індивіда на інформаційне самовизначення.

Концепція (інформаційної) приватності, яка виросла з фундаментального права на повагу до приватного життя[4], на сучасному етапі перетворила цю категорію в окрему галузь права із своїми інститутами, суб'єктами і правовідносинами. В її основі система прав осіб, що є суб'єктами даних, яким кореспондують відповідні обов'язки інших суб'єктів стосовно дотримання правил роботи з персональними даними[5].

Права суб'єкта даних:

– знати про ціль збору і правомірні підстави для цього, майбутніх отримувачів, і свої права під час збору даних;

– отримати копію даних, що було зібрано, включаючи інформацію про їх використання; вносити корективи, знищувати або блокувати (забо-

---

[3] Louis D. Brandeis, Samuel D. Warren The Right To Privacy, 4 Harv.L.Rev. 193-220 (1890).

[4] Це право проголошується в Ст. 12 Загальної Декларації з прав людини, Ст. 8 Європейської Конвенції про захист прав і основних свобод людини та ін.

[5] Далі наводяться принципи і правила, що встановлені в Директиві Європейського Союзу 1995 року. Стандарти цієї Директиви є найбільш жорсткими у порівнянні з відповідними вимогами Конвенції Ради Європи 1981 року та Керівними Принципами Організації Економічної Співпраці і Розвитку 1980 року.

роняти використання) даних, що обробляються в порушення закону; а також вимагати повідомлення про це сторонам, яким ці дані було розкрито;

– заперечувати проти обробки на безсумнівних законних підставах, і використання даних з метою прямої реклами (шляхом відмови від участі в розсилці рекламних матеріалів тощо);

– право не бути предметом рішень, що суттєво зачіпають права особи, які базуються виключно на автоматизовано прийнятих рішеннях спрямованих на оцінку особистих якостей цієї особи (з виключеннями, якщо при цьому гарантується врахування правомірних інтересів особи); а також право знати логіку дії механізму прийняття рішень такою автоматизованою системою.

Правила обробки даних:

Якість даних

Принцип якості даних вимагає того, щоб персональна інформація:

(а) оброблялась на правомірних і законних підставах;

(б) збиралася для спеціальних, визначених і правомірних цілей, і використовувалася у спосіб сумісний з такими цілями;

(в) була точної і не була застарілою;

(г) не зберігалася у формі, що дозволяє ідентифікацію особи, триваліше, ніж це потрібно для таких цілей.

Правомірність обробки

Обробка персональних даних (збір, записування, використання і передача) для того, щоб бути правомірною, має відбуватися на одній із умов, що перелічені нижче:

(а) за прямою згодою суб'єкта даних (особи, якої стосуються дані). Згода є чинною лише тоді, коли суб'єкт даних отримує попереднє повідомлення про ціль збору і майбутніх її отримувачів, і може бути відкликана;

(б) коли це потрібно для виконання контракту з суб'єктом даних або для вчинення дій, що замовляє суб'єкт даних до контракту;

(в) коли це потрібно для дотримання контролером даних зобов'язань за законом;

(г) коли це потрібно для захисту життєвих інтересів суб'єкта даних;

(д) коли це потрібно для виконання завдань в суспільних інтересах або здійснюється під час виконання владних повноважень, що наділено контролера або третю особу, якій ці дані розкриваються;

(е) коли це потрібно для правомірних цілей, яким слідують контролер або третя особа, або сторони, яким дані розкриваються, за виключенням, коли ці інтереси переважуються інтересами або фундаментальними правами і свободами суб'єкта даних.

Обмеження обробки даних

Обмеження обробки даних передбачено двома принципами, – принципом «обмеження ціллю», за яким використання і обробка персональної інформації обмежені попередньо визначеною ціллю збору даних (вищезазначені принципи правомірності обробки є законними виключенням з цього принципу), і принципом обмеження чутливих даних.

За другим принципом, обробка персональних даних, що розкривають расове або етнічне походження, політичні погляди або філософські переконання, членство у профспілках, сексуальне життя, стан здоров'я, – заборонена (з великою кількістю виключень). Дані про вчинення правопорушень або застосування секретних засобів можуть оброблятися лише під наглядом відповідної інстанції.

Безпека

Вимогою до систем, що обробляють будь-які дані є забезпечення безпеки (під цим розуміється комплекс організаційних і технічних засобів).

Вказані права суб'єктів даних і правила роботи з персональними даними вимагають здійснення контролю і вжиття заходів примушення за необхідністю. Такі функції на національному рівні виконують уповноважені державні органи. Однак глобальна і децентралізована інфраструктура Інтернет робить це проблематичним.

РИЗИКИ ПРИВАТНОСТІ В ІНТЕРНЕТ

Теорія передачі інформації між комп'ютерами з'явилась у 1961 році. А вже у 1969 році перші вузли (host) академічних установ США з'єднались в одній мережі.

Починаючи з 80-х років двадцятого віку, Інтернет поступово стає тим, що зараз називають «мережа мереж»[6]. Він починає використовуватися на повсякденній основі і стрімко поширюватися у всьому світі, завдяки концепції відкритої архітектури побудови мережі (open architecture networking)[7].

У порівняні із вже ставшими звичайними засобами передачі інформації, такими як теле-, радіомовлення, Інтернет являє собою новий вид медіуму з унікальними характеристиками. Його унікальність полягає в тому, що він функціонує не тільки як звичайний транслятор, тобто поширювач інформації, але до того ж є комунікаційним засобом[8].

---

[6] A Brief History of the Internet. – Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff.

[7] Концепція базується на технічній ідеї, завдяки якій до мережі можуть вільно приєднуватися вузли на федеративній основі.

[8] За визначенням, даним Федеральною Радою з питань Побудови Мережі (Federal Networking Council), термін «Інтернет» має застосовуватися до глобальної інформаційної системи, яка – (i) логічно зв'язана глобально унікальним адресним простором, який базується на Протоколі Интернету (Internet Protocol) або наступних розширеннях/модифікаціях; (ii) здатна підтримувати комунікаційний зв'язок через застосування програмного набору Протоколу Управління Передачею /Інтернет Протоколу (Transmission Control Protocol/ Internet Protocol) або наступних розширень/модифікацій та/або інші IP-сполучені протоколи; та (iii) забезпечує, використовує або робить доступними, публічно чи конфіденційно, послуги високого рівня, покладені на зв'язок та відповідну інфраструктуру, що описана вище. Цит. по: зноска 1.

Інформація про людину є джерелом можливої небезпеки для його приватності. Через відкритість Інтернет і його особливість як системи, що може накопичувати і обробляти інформацію про людину, надзвичайно актуальним є питання забезпечення приватності при користуванні трансляційно-комунікативними можливостями цієї глобальної мережі.

Обмін повідомленнями за допомогою Інтернет принципово інший ніж при передачі інформації звичайними комунікаційними засобами. Більшість користувачів не мають прямого доступу до ресурсів глобальної мережі. Цей доступ вони отримують через його постачальників, які фактично є посередниками між користувачами і мережею. Електронне повідомлення, рухаючись у мережі, проходить крок за кроком, від одного оператора до іншого, вибираючи найоптимальнійший з шляхів[9].

Кожний з операторів виступає як проміжна ланка і має можливість втручання у цей процес. Оператори можуть не тільки узнати про зміст повідомлення, а і додаткову інформацію. Стандартне повідомлення електронною поштою містить заголовок з інформацією про відправника та отримувача, яка включає в себе ім'я, інтернет адресу, назву вузла, час листування. Це вимагає від користувачів вжиття відповідних заходів для забезпечення приватності процесу обміну електронними повідомленнями[10].

Інтернет несе в собі ризики не тільки для комунікаційної приватності. Із появою унікального адресного простору у вигляді веб-сторінок, право на повагу до приватного життя користувача доповнюється новим змістом. Йдеться про приватність інформаційної активності (інформаційного життя) користувача в мережі.

Кожна веб-публікація має свою унікальну адресу, за якою вона знаходиться. Щоб дістати потрібні Інтернет-публікації чи послуги «онлайн», користувач має вступити у контакт з постачальниками цих публікацій чи послуг.

Рухаючись рівень за рівнем в інформаційній «павутині» Інтернет, користувач залишає за собою інформаційний слід у вигляді операційних даних (transactional data). Ці дані включають в себе Інтернет-адресу комп'ютера користувача, інформацію про програмне забезпечення, тип комп'ютера, відвідувані веб-сторінки, а також про попередні візити до цієї сторінки[11].

---

[9] В середньому електронне повідомлення проходить приблизно через 50 операторів доки не досягне адресата. Виходячи з інтересів національної безпеки, деякі розвинуті країни, серед яких Канада і Сполучене Королівство Великої Британії, вжили комплекс технічних і організаційних заходів для того, щоб електронні повідомлення, які мають відправника і отримувача на їх територіях, не виходили за національні кордони під час свого шляху.

[10] Серед таких засобів найбільш ефективним є криптографічний захист інформації.

[11] Така інформація автоматично записується на комп'ютері користувача завдяки використанню технології «cookies».

Такі дані є багатим джерелом інформації про поведінку користувача в мережі, що, в свою чергу, може бути використано і використовується для створення профілю користувача, – сукупності характеристик, якими охоплюються його смаки, звички, мотивації при користуванні Інтернет. А співставлення цієї інформації з іншими даними дозволяє ідентифікувати людину. При цьому, в більшості випадків, людина і гадки не має про те, яка персональна інформація, і з якою метою збирається і опрацьовується[12].

Ризик приватності людини існує і при користуванні людиною такою можливістю Інтернет як послуги «он-лайн». За визначенням, послуги «он-лайн» – це електроні комунікаційні системи, які пропонують за попередньою оплатою своїм підписчикам перелік послуг (електрона пошта, інформаційні послуги, ігри, участь у дискусійних групах за інтересами або спілкування в режимі реального часу), які є доступними через телефону мережу з використанням модему і комп'ютера[13].

Як для функціювання будь-якої з традиційних електронних систем, для послуг «он-лайн» потрібна інформація про користувача. Ця інформація використовується в різних процесах, що відбуваються при роботі в електронних системах[14]. Постачальники послуг «он-лайн» збирають і опрацьовують персональні дані про особу користувача, оскільки це потрібно для роботи таких систем.

Ризики приватності людини в мережі посилюються тим, що Інтернет дає можливість порушення її прав не тільки операторам, які безпосередньо збирають дані про користувача. Програмне забезпечення на сучасному етапі розвитку дозволяє здійснювати цілеспрямований пошук, співставлення і систематизацію всієї доступної в мережі інформації про визначеного користувача. Це включає в себе адресу і телефоні номери, місце народження, навчання, професію, місця роботи, його смаки і звички, погляди і переконання. Більше того, в США існують організації, які пропонують так звані «пошукові послуги» («look-up services») на комерційній основі.

---

[12] Recommendation No. 1/99 On Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware Adopted by the Working Party on 23 February 1999.

[13] Таке визначення послуг он-лайн дано у документі Комісії ЕС від 16.10.96 р. Green Paper «On the Protection of Minors and Human Dignity in Audiovisual and Information Services». – COM (96) 487.

[14] При використані інформаційних систем відбуваються процеси авторизації, ідентифікації і посвідчення, контролю права доступу, ревізії і розрахунку. – Джерело: Доповідь «Privacy Enhancing Technologies: the Path to Anonimity». – ed.: Ronald Hes, John Borking. – 1998. The Hague.

ШЛЯХИ ВИРІШЕННЯ ПРОБЛЕМИ

Вирішити питання захисту приватності користувачів Інтернет можливо за умов вжиття комплексу заходів, організаційних і технічних.

Перш за все, на організаційному рівні пропонується створити міжнародний наглядовий механізм за дотриманням приватності користувачів Інтернет в рамках існуючої системи регулювання Інтернет. Така система зараз існує у формі стандартизації. «Стандарти це не тільки технічне питання. Вони обумовлюють технологію, яка буде застосовуватися в інформаційному суспільстві, і відповідно, шлях, яким промисловість, користувачі, споживачі і адміністратори будуть здобувати зиск від цього»[15]. Через це, організації, що займаються стандартизацією Інтернет, мають можливість визначати пріоритети і напрямки розвитку Інтернет.

Разом з тим, стандартизація це процес суб'єктивний. Він відображає динаміку ринку і сам є комерційною діяльністю. Внаслідок спрямованості процесу стандартизації на потреби ринку, публічні інтереси і права користувачів не завжди отримували належного нормативно-технічного втілення.

На сучасному етапі ситуація починає змінюватися. Так з'являються концепції і технічні розробки, які надають можливість користування телекомунікаційними послугами без ідентифікації особи користувача[16].

Анонімність користування Інтернет визнається як один із суттєвих принципів, що дозволяє гарантувати певний рівень приватності при користуванні Інтернет[17]. З іншої сторони, справедливо відзначається, що принцип анонімності, завдяки якому можна уникнути ідентифікації, не завжди відповідає іншим публічним інтересам. Таким, як боротьба з незаконним і згубним змістом в Інтернет, фінансовим шахрайством або порушенням авторських прав.

На думку автора, вірний підхід – це балансування, яке має відбуватися за принципом пропорційності задіяних інтересів, як особи так і всього суспільства. Цей принцип знайшов своє відображення в практиці Європейського Суду з прав людини по статті 8 Європейської Конвенції про захист прав і основних свобод людини, яка проголошує право на повагу до приватного життя людини[18].

---

[15] Standardization and the Global Information Society: The European Approach Communication from the Commission to the Council and the Parliament.- Brussels, 24 July 1996 COM (96) 359.

[16] Серед них, концепція «Захисник Ідентичності»(Identity Protector). Див. Зноску 13.

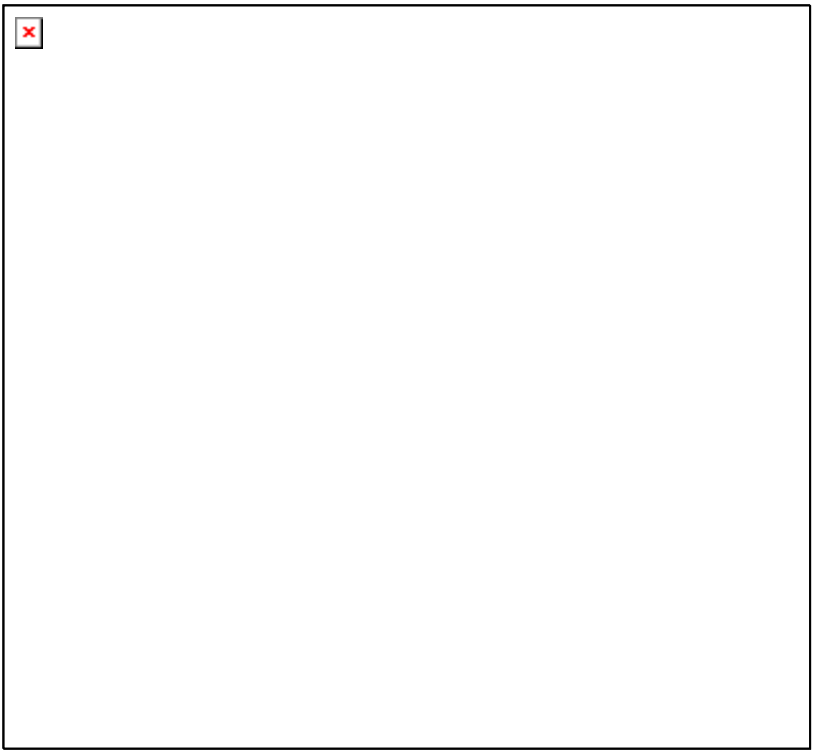
[17] Recommendation 3/97 EU. Anonymity on the Internet, adopted by Working Party on 3 December 1997.

[18] Пазюк А. Захист приватного життя людини в діяльності Ради Європи.// Вісник Українського Центру прав людини, Число 1-2/ 1999, Стор. 9-12.

Слід звернути увагу і на такий механізм, як саморегуляція телекомунікаційного сектора через прийняття кодексів «чесної інформаційної практики» (fair information practice). Хоча, так зване, «м'яке законодавство» (soft law), під яким і розуміються ці кодекси, не є достатнім для гарантування прав користувачів. Вирішальну роль мають відігравати міжнародні інструменти в галузі захисту приватності. Оскільки цю глобальну, як сам Інтернет, проблему на національному рівні вирішити не можливо.

Закріплені в існуючих міжнародно-правових актах, таких як Конвенція Ради Європи 1981 року, Керівні Принципи Організації Економічної Співпраці і Розвитку 1980 року, Директива Європейського Союзу 1995 року, принципи приватності потребують їх адаптації для застосування у новому інформаційному середовищі.

Феномен Інтернет, якому ми зобов'язані появою такого поняття як інтерактивна приватність, вимагає вжиття адекватних заходів, аби «кінець приватності» не наступив.



ТЕРИТОРІАЛЬНА ПРИВАТНІСТЬ ТА ПРИВАТНІСТЬ КОМУНІКАЦІЙ

Євген Захаров, Харківська правозахисна група

ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ ТА ПРИВАТНІСТЬ КОМУНІКАЦІЙ

КОНСТИТУЦІЙНІ ГАРАНТІЇ ТА ОБМЕЖЕННЯ

Частина 1 статті 30 Конституції України проголошує: «Кожному гарантується недоторканність житла. Не допускається проникнення до житла чи до іншого володіння особи, проведення в них огляду чи обшуку інакше як за вмотивованим рішенням суду»[19]. Стаття 31 Конституції гарантує таємницю листування, телефонних розмов, телеграфної чи іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, «з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо».

Порядок здійснення таких виключних заходів регулюється Законом України «Про оперативно-розшукову-діяльність» (далі ОРД), який був прийнятий 18 лютого 1992 р. (з численними змінами та доповненнями в 1992-2003 рр.) та статтею 187 Кримінально-процесуального кодексу (далі КПК) в редакції 21.06.2001.

ОРГАНИ, ЯКІ МАЮТЬ ПРАВО НА ОРД, І ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ ОРД

Право проводити оперативно-розшукові заходи (далі ОРЗ) надано відповідно до статті 5 Закону про ОРД підрозділам Міністерства внутрішніх справ України (кримінальна, транспортна та спеціальна міліція, спецпідрозділи по боротьбі з організованою злочинністю, судова міліція); підрозділи СБУ (розвідка, контррозвідка, військова контррозвідка, захисту національної державності, внутрішньої безпеки, по боротьбі з корупці-

[19] Тут й далі в цьому розділі уривки з нормативних актів наводяться з комп'ютерної правової системи «Ліга-Закон».

єю та організованою злочинністю, оперативно-технічні, оперативного документування, боротьби з тероризмом і захисту учасників кримінального судочинства та працівників правоохоронних органів); Державної прикордонної служби України; управління державної охорони; органів державної податкової служби (оперативні підрозділи податкової міліції); органів і установ Державного департаменту України з питань виконання покарань (оперативні підрозділи); розвідувального органу Міністерства оборони України.

Підстави для проведення оперативно-розшукової діяльності визначені в статті 6 Закону про ОРД:

«1) наявність достатньої інформації, одержаної в установленому законом порядку, що потребує перевірки за допомогою ОРЗ, про

– злочини, що готуються або вчинені невстановленими особами;

– осіб, які готують або вчинили злочин;

– осіб, які переховуються від органів розслідування, суду або ухиляються від відбування кримінального покарання;

– осіб безвісно відсутніх;

– розвідувально-підривну діяльність спецслужб іноземних держав, організацій та окремих осіб проти України;

– реальну загрозу життю, здоров'ю, житлу, майну працівників суду і правоохоронних органів у зв'язку з їх службовою діяльністю, а також особам, які беруть участь у кримінальному судочинстві, членам їх сімей та близьким родичам, з метою створення необхідних умов для належного відправлення правосуддя; співробітників розвідувальних органів України у зв'язку із службовою діяльністю цих осіб, їх близьких родичів, а також осіб, які конфіденційно співробітничають або співробітничали з розвідувальними органами України, та членів їх сімей з метою належного здійснення розвідувальної діяльності;

2) запити повноважних державних органів, установ та організацій про перевірку осіб у зв'язку з їх допуском до державної таємниці і до роботи з ядерними матеріалами та на ядерних установках;

3) потреба в отриманні розвідувальної інформації в інтересах безпеки суспільства і держави.»

За відсутності перелічених підстав ОРД забороняється.

Стаття 8 цього Закону перераховує права підрозділів, що здійснюють ОРД. Згідно з п.7 вони мають право «негласно виявляти та фіксувати сліди тяжкого або особливо тяжкого злочину, документи та інші предмети, що можуть бути доказами підготовки або вчинення такого злочину, чи одержувати розвідувальну інформацію, у тому числі шляхом проникнення оперативного працівника в приміщення, транспортні засоби, на земельні ділянки», а відповідно до п.9 та 10 – «знімати інформацію з каналів зв'язку, застосовувати інші технічні засоби отримання інформації» та

«контролювати шляхом відбору за окремими ознаками телеграфно-поштові відправлення».

Окрім Закону про ОРД зняття інформації з каналів зв'язку згадується також у Законі «Про організаційно-правові засади боротьби з організованою злочинністю». У відповідності до статті 15 цього Закону спецпідрозділам МВС та СБУ по боротьбі з організованою злочинністю надане право:

«1. У боротьбі з організованою злочинністю спеціальним підрозділам органів внутрішніх справ і Служби безпеки України надається право за попередньою санкцією прокурора додатково використовувати спеціальні технічні засоби у випадках:

а) контролю, фіксації і документування розмов та інших дій осіб за наявності підстав вважати їх причетними до організованої злочинної діяльності;

б) фіксації та документування факту телефонної розмови між громадянами, надсилання листа або телеграфного повідомлення, без порушення таємниці змісту телефонної розмови, листа або телеграфного повідомлення;

в) забезпечення особистої безпеки і безпеки житла, майна співробітників спеціальних підрозділів органів внутрішніх справ і Служби безпеки України, учасників кримінального судочинства, їх близьких родичів, за їх згодою, в разі загрози заподіяння їм шкоди у зв'язку з їх участю в боротьбі з організованою злочинністю.

2. В інших випадках спеціальні підрозділи по боротьбі з організованою злочинністю органів внутрішніх справ і Служби безпеки України застосовують технічні засоби в порядку, що визначається Законом України «Про оперативно-розшукову діяльність». Фактичні дані, що отримані і зафіксовані співробітниками вказаних спецпідрозділів з використанням вказаних технічних засобів, можуть бути використані як докази в суді.»

Очевидно, ці ОРЗ порушують право на приватність, гарантоване статтями 30 та 31 Конституції, і тому повинні застосовуватися як виняткові засоби у випадках, передбачених законом. Частина 5 статті 9 Закону про ОРД говорить, що «під час здійснення ОРД не допускається порушення прав і свобод людини і юридичних осіб. Окремі обмеження цих прав і свобод мають винятковий і тимчасовий характер і можуть застосовуватись лише за рішенням суду щодо особи, в діях якої є ознаки тяжкого або особливо тяжкого злочину, та у випадках, передбачених законодавством України, з метою захисту прав і свобод інших осіб, безпеки суспільства.» Частина 14 статті 9 формулює теж саме дещо по-іншому: «оперативно-розшукові заходи, пов'язані з тимчасовим обмеженням прав людини, проводяться з метою запобігання тяжким або особливо тяжким злочинам, їх припинення і розкриття, розшуку осіб, які ухиляються від відбування кримінального покарання або безвісти зникли, захисту життя, здоров'я, житла і майна працівників суду і правоохоронних органів та осіб, які бе-

руть участь у кримінальному судочинстві, припинення розвідувально-підривної діяльності проти України. У разі оперативної необхідності невідкладного здійснення цих заходів оперативно-розшукові підрозділи зобов'язані протягом 24 годин повідомити суд або прокурора про застосування та підстави для їх проведення». Зауважимо, що у частині 5 йдеться тільки про ОРЗ щодо конкретної особи, тоді як у частині 14 – про ОРЗ, які не обов'язково прив'язані до конкретної особи. Як зазначає шведський професор Денніс Телльборг[20], сьогодні головною функцією негласного нагляду є не викриття злочинця, а встановлення самої наявності злочину. Коли спецпідрозділи провадять розшукову діяльність проти організованної злочинності, торговців наркотиками тощо, вони працюють до вчинення злочину, і мета цих ОРЗ – зібрати інформацію про особу, злочинну групу або можливі насильницькі дії (терористичний акт, наприклад). Іншими словами, те, що хочуть з'ясувати на етапі, коли подається заява до суду про отримання дозволу на негласне стеження, часто неможливо конкретизувати. У таких випадках отримання судової санкції втрачає сенс, а спецпідрозділи фактично можуть організовувати негласне стеження на власний розсуд без застосування судового контролю. Отже, процедура отримання судової санкції повинна чітко визначатися законом, бути ясною і детальною, а формулювання гарантій проти зловживань стає центральним питанням.

СУДОВИЙ ДОЗВІЛ НА ОРЗ, ЯКІ ПОРУШУЮТЬ ПРАВО НА ПРИВАТНІСТЬ

До прийняття Конституції оперативно-розшукові заходи, які порушують право на приватність, здійснювалися як виняткові за санкцією Генерального прокурора України або його заступників, прокурора республіки Крим, прокурорів Києва, областей або прирівнених до них прокурорів. Ця норма статті 8 Закону «Про оперативно-розшукову діяльність» (далі ОРД) залишалася незмінною до початку 2001 року, хоча в п.22 Постанови Пленуму Верховного Суду України (далі ВСУ) №9 від 1 листопада 1996 року «Про використання Конституції України при відправленні правосуддя» ясно вказувалося, що «дозвіл на проникнення до житла чи іншого володіння особи, накладення арешту на кореспонденцію і виїмку поштово-телеграфних установ та зняття інформації з каналів зв'язку (телефонних розмов, телеграфної та іншої кореспонденції) надається тільки судом». В редакції Закону про ОРД від 18.01.2001 частина друга статті 8 була змінена наступним чином: «Негласне проникнення до житла чи до іншого володіння особи, зняття інформації з каналів зв'язку, контроль за листуванням, телефонними розмовами, телеграфною та іншою кореспон-

[20] Прослушивание телефонных разговоров в международном праве и законодательстве одиннадцати европейских стран. – Харьков: Фолио, 1999. – 152 с.

денцією, застосування інших технічних засобів одержання інформації проводяться за рішенням суду, прийнятим за поданням керівника відповідного оперативного підрозділу або його заступника. Про отримання такого дозволу суду або про відмову в ньому зазначені особи повідомляють прокурору протягом доби. Застосування цих заходів проводиться виключно з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншим способом одержати інформацію неможливо. За результатами здійснення зазначених оперативно-розшукових заходів складається протокол з відповідними додатками, який підлягає використанню як джерело доказів у кримінальному судочинстві». Проте процедура судового розгляду подання про отримання дозволу так і не була врегульована законодавцем, що, безсумнівно, є суттєвою вадою Закону про ОРД з огляду на його відповідність міжнародним стандартам. Крім того, «виключно з метою отримання розвідувальної інформації для забезпечення зовнішньої безпеки України, запобігання і припинення терористичних актів, розвідувально-підривних посягань спеціальних служб іноземних держав та іноземних організацій зазначені заходи можуть здійснюватись в порядку, узгодженому з Генеральним прокурором України та Головою Верховного Суду України» (частина 3 статті 8). Що це за узгодження, Закон не визначає.

Як зазначено І.М.Козьяковим[21], процедура надання судового дозволу здійснюється на підставі листа ВСУ від 19 листопада 1996 р. № 16/6 «Про тимчасовий порядок розгляду матеріалів про дачу дозволу на проникнення до житла чи іншого володіння особи, накладення арешту на кореспонденцію і виїмку поштово-телеграфних установ та зняття інформації з каналів зв'язку (телефонних розмов, телеграфної та іншої кореспонденції)». При цьому автор посилався на монографію І.В.Сервецького[22], видану у 2000 р. Звісно, я став шукати вказаний лист ВСУ, оскільки процедура прийняття рішення про застосування виняткових заходів, що обмежують фундаментальне право людини на приватність, за всіма канонами, має бути ясно і чітко виписана. Але виявилося, що цей лист відсутній у комп'ютерних правових системах, таких, як «Ліга-Закон» та інші. Довелося повернутися до старого засобу: пошуку монографії І.В.Сервецького в бібліотеці. На щастя, книжка знайшлася, і я отримав доступ до довгоочікуваного листа ВСУ.

Проте, як може переконатися читач, очікування виявилися марними. У листі наведені тільки загальні принципи порядку надання дозволу на

---

[21] Козьяков І.М. Судовий контроль за отриманням інформації приватного характеру //Вісник Верховного Суду України, №4, 2003. – С. 54-56.

[22] Сервецький І.В. Науково-практичний коментар Закону України «Про оперативно-розшукову діяльність». – Київ, Парламентське видавництво, 2000. – С.183-184.

здійснювання оперативно-розшукових заходів. Не вказаний максимальний термін дії дозволу, не вказано, на який термін може бути продовжено дозвіл. Законами інших країн чітко обумовлена максимальна тривалість зняття інформації з каналів зв'язку, яку може дозволити суд: у Франції – 4 місяці, Німеччині – 3 місяці, Фінляндії та Швеції – 1 місяць, Угорщині – 1.5 місяця, Росії – 6 місяців, тощо. Лише в Україні максимальний термін дії дозволу на негласні ОРД взагалі не визначений. Раніше тривалість обмежувалася опосередковано терміном 6 місяців (і тільки в випадках, коли підозри не підтвердилися), оскільки діяла норма про знищення оперативно-розшукової справи, якщо протягом шести місяців не встановлені дані, що вказують на ознаки злочину, скоєного особою, щодо якої здійснювалися ОРЗ. Але ця норма з Закону про ОРД була виключена. Сумнівними виглядають й п.6,7 листа ВСУ. Проте ми не будемо аналізувати положення цього листа. Можна зрозуміти керівництво ВСУ, яке у вкрай стислий проміжок часу видало терміновий документ для праці судів відповідно до щойно прийнятої Конституції. А от зрозуміти законодавця, який так і не врегулював процедуру надання та продовження санкції на застосування оперативно-розшукових заходів, які у виняткових випадках обмежують конституційні права людини, ніяк не можна. Тим більше, що Закон про ОРД з 1996 року змінювався 11 разів! Зауважимо, що процедура надання дозволу на накладення арешту на кореспонденцію та зняття інформації з каналів зв'язку під час розслідування кримінальної справи детально розписана у статті 187 Кримінально-процесуального кодексу, проте і вона не містить максимальний термін дії дозволу і положення про періодичний судовий контроль. А от процедура надання дозволу на негласне проникнення до житла чи до іншого володіння особи КПК не врегульована.

Отже, суди досі мають керуватися листом ВСУ від 19 листопада 1996 р. № 16/6, юридична чинність якого дуже сумнівна. Адже він не відноситься до нормативно-правових актів, і його не можна назвати навіть квазіджерелом права, як наприклад, керівні роз'яснення Пленуму Верховного Суду України. Дуже дивує відсутність цього листа в системі «Ліга-Закон», оскільки вона повинна містити усі нормативні акти, зареєстровані Міністерством юстиції. Я звернувся з проханням розмістити лист ВСУ в системі, проте отримав відповідь наступного змісту[23]: «Разместить в системе запрашиваемый Вами документ Верховного Суда Украины от 19.11.96 г. не представляется возможным, поскольку он не был обнародован. Кроме того, судя из названия, можно предположить, что этот документ является внутренним, а значит, и получить его будет невозможно». Таким чином, зазначений лист не був зареєстрований в Єдиному

[23] Наводиться мовою оригіналу.

реєстрі нормативних актів України. А звідси випливає, що цей лист не може вважатися чинним, адже відповідно до статті 57 Конституції «закони та інші нормативно-правові акти, що визначають права і обов'язки громадян, не доведені до відома населення у порядку, встановленому законом, є нечинними». На мою думку, ця ситуація яскраво ілюструє реальне, а не декларативне, ставлення органів державної влади України до прав людини. При цьому масштаби таємного стеження в Україні вражають: за повідомленням одного з суддів Верховного Суду України на недавній конференції, у 2002 році було надано більше 40 000 дозволів на зняття інформації з каналів зв'язку, з них найбільше – приблизно 4000 – в Харківській області (це дуже багато, в європейських країнах надають сотні дозволів за рік, а в такій країні, як США, де рівень злочинності значно більше, ніж в Україні – кількість дозволів коливається на рівні 1000-1300 на рік). Цікаво порівняти кількість дозволів з кількістю засуджених судами України у 2002 р. до позбавлення волі на певний строк за вчинення тяжких і особливо тяжких злочинів: 41211[24]. Логічно припустити, що оперативно-розшукова діяльність була насамперед спрямована на розкриття організованих груп та злочинних організацій. У 2002 році було виявлено 722 групи, у складі яких діяло 3205 осіб, які скоїли 6467 злочинів. При цьому за вчинення злочинів організованою групою до позбавлення волі засуджено 653 особи. У 2002 році в Харківській області було виявлено 51 організовану групу та злочинну організацію і 237 осіб, які діяли в їх складі. До позбавлення волі загалом було засуджено 3793 особи. У зв'язку ж з чим були надані 4000 санкції на зняття інформації з каналів зв'язку? Як на мене, ці дані важко зіставити. Отже, вкрай необхідна публікація річних звітів, де були б вказані кількість санкцій, кількість відмов, види злочинів, у випадку яких надавалися санкції, середня тривалість зняття інформації з каналів зв'язку, кількість порушених за результатами ОРД кримінальних справ, тощо.

Враховуючи, що вищевказаний лист ВСУ практично недоступний для широкого загалу, ми вирішили надрукувати його в нашому виданні (див. нижче).

ІМУНІТЕТИ

Законом встановлені певні обмеження на проведення ОРЗ у відношенні деяких категорій громадян. Так, відповідно до ч.2 ст.10 Закону «Про адвокатуру» забороняється прослуховування телефонних розмов адвокатів у зв'язку з ОРД без санкції Генерального прокурора, його заступників, прокурорів Республіки Крим, м.м. Києва і Севастополя. Об-

[24] Ці та наступні статистичні дані наводяться за виданнями: Вісник Верховного Суду України, 2003, №3, 2003, с. - та №4, с.36-41.

шук, огляд особистих речей і багажу, транспорту, житлового чи службового приміщення, а також порушення таємниці листування, телефонних розмов, телеграфної та іншої кореспонденції депутата Верховної Ради України допускаються лише у разі, коли Верховною Радою України надано згоду на притягнення його до кримінальної відповідальності (ч.2 ст.27 Закону «Про статус народного депутата України»). Крім того, ч.4 ст. 11 Закону про ОРД забороняється залучати до виконання оперативно-розшукових задач медичних працівників, священнослужителів, адвокатів, якщо об'єкт ОРД є їхнім клієнтом чи пацієнтом.

Ч.4 ст.13 Закону України «Про статус суддів» встановлювала, що проникнення в житло чи службове приміщення судді, в його особистий чи службовий транспорт, проведення там огляду, обшуку чи виїмки, прослуховування його телефонних розмов, особистий обшук судді, а також огляд, виїмка його кореспонденції, речей і документів можуть проводитися тільки із санкції Генерального прокурора України при наявності порушеної кримінальної справи. Але в червні 2001 року ці обмеження було зняті: для перерахованих ОРЗ щодо суддів достатньо вмотивованого рішення суду.

ГАРАНТІЇ ЗАКОННОСТІ ТА ВІДПОВІДАЛЬНІСТЬ

Гарантії законності при здійсненні ОРД сформульовані в статті 9 Закону про ОРД. У кожному випадку наявності підстав для проведення ОРД заводиться оперативно-розшукова справа (за виключенням перевірки осіб у зв'язку з допуском їх до державної таємниці). Без заведення цієї справи ОРЗ забороняються. При цьому виноситься постанова, у якій вказується місце та час її складання, посада й прізвище особи, яка її підписала, підстава і мета заведення оперативно-розшукової справи. У випадках порушення прав і свобод людини або юридичних осіб в процесі здійснення ОРД, а також у випадку, коли причетність до правопорушення особи, щодо якої здійснювалися ОРЗ, не підтвердилась, підрозділи, що проводили ОРЗ, повинні невідкладно поновити порушені права і відшкодувати заподіяні моральні і матеріальні збитки (проте незрозуміло, як об'єкт ОРД дізнається про проведення відносно нього оперативно-розшукових заходів, оскільки Закон не містить зобов'язання інформувати особу в таких випадках, отже, ця норма видається цілком декларативною). Громадяни України й інші особи мають право у встановленому законом порядку одержати від органів, що проводили ОРЗ, письмове пояснення з приводу обмеження своїх прав і свобод та оскаржити ці дії (у випадку негласного стеження це можливо тільки у випадку розголошення інформації, що міститься у справі, отже, можливість ефективного оскарження є дуже сумнівною). Відомості, отримані внаслідок ОРЗ, що стосуються особистого життя, честі і гідності особи, якщо вони не містять ін-

формації про вчинення заборонених законом дій, зберіганню не підлягають і повинні бути знищені (частини 1,8,10 і 12 статті 9). На жаль, з частини 3 статті 9 видалена норма про знищення оперативно-розшукової справи, якщо протягом шести місяців не встановлені дані, що вказують на ознаки злочину, скоєного особою, щодо якої здійснювалися ОРЗ.

Контроль за проведенням оперативно-розшукової діяльності згідно із статтею 9 покладений на ті самі органи, які і здійснюють цю діяльність (МВС, СБУ, Державна прикордонна служба, податкова міліція, тощо). Нагляд за дотриманням законності під час проведення ОРД здійснюється Генеральним прокурором України, його заступниками, прокурорами АРК, областей, міст Києва і Севастополя (стаття 14 Закону про ОРД). Законодавством передбачений також парламентський контроль за діяльністю СБУ (він здійснюється Комітетом з питань оборони і національної безпеки) та за виконанням законів у сфері боротьби з корупцією та організованою злочинністю (його здійснює Комітет з питань законодавчого забезпечення правоохоронної діяльності та боротьби з організованою злочинністю та корупцією), проте, на мій погляд, парламентський контроль невідчутний або, принаймні, про цей контроль громадськості нічого невідомо.

Покарання за порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер передбачене статтею 163 Кримінального кодексу України. Ці дії караються штрафом від 50 до 100 неоподаткованих мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі до трьох років. Ті самі дії, вчинені щодо державних чи громадських діячів або вчинені службовою особою, або з використанням спеціальних засобів, призначених для негласного зняття інформації, караються позбавленням волі на строк від трьох до семи років.

Очевидно, гарантії законності в законі про ОРД слабко захищають від зловживань, особливо якщо їх порівнювати з гарантіями законності в німецькому чи угорському законах, які передбачають парламентський нагляд за законністю перехоплення повідомлень за допомогою роботи спеціальних органів. У ці органи може звернутися зі скаргою кожний, хто вважає, що його кореспонденція контролюється спецслужбами незаконно. Цікаво, що німецький Комітет G-10 інформується міністром про всі дозволені ним обмежувальні заходи **до того,** як перехоплення почали здійснювати. Комітет має право скасувати наказ міністра, після чого перехоплення негайно припиняється, якщо, через терміновість, воно було розпочате до одержання дозволу. Після закінчення перехоплення особа, чиї повідомлення перехоплювалися, повідомляється про це, «якщо це не ставить під загрозу мету розслідування». Уся непотрібна надалі документація повинна бути знищена.

На мій погляд, Закон про оперативно-розшукову діяльність незадовільний з точки зору гарантій права на приватність і суперечить міжнародним стандартам у цій галузі, оскільки приховує у собі потенційні порушення статті 8 Європейської конвенції про захист прав людини й основних свобод.

ПРИНЦИПИ ЗАКОНОДАВСТВА З ПЕРЕХОПЛЕННЯ ПОВІДОМЛЕНЬ, СФОРМУЛЬОВАНІ ЄВРОПЕЙСЬКИМ СУДОМ З ПРАВ ЛЮДИНИ

Перша частина статті 8 Конвенції встановлює, що «кожен має право на повагу до його приватного і сімейного життя, до житла і до таємниці кореспонденції». Друга частина статті 8 вказує на обмеження цього права: «Держава не може втручатися у здійснення цього права інакше ніж згідно із законом та у випадках, необхідних в демократичному суспільстві в інтересах національної і громадської безпеки або економічного добробуту країни, з метою запобігання заворушенням і злочинам, для захисту здоров'я або моралі чи з метою захисту прав і свобод інших осіб».

Виходячи з аналізу практики Європейського суду з прав людини по статті 8 у частині перехоплення повідомлень (справи **Класс проти Німеччини, Малоун проти Об'єднаного Королівства, Ювіг проти Франції, Крюслен проти Франції** й інші), були сформульовані принципи[25], яким мусить відповідати закон, що регулює контроль комунікацій, щоб він не порушував статтю 8. Перехоплення повідомлень повинне здійснюватися **на підставі закону**, який має бути **доступним** (тобто щоб людина мала можливість переконатися, що перехоплення відповідає законодавчим нормам, які використані в даному конкретному випадку), **передбачуваним** (тобто людина повинна бути здатна передбачити наслідки своїх можливих дій) і задовольняти необхідному критерію **якості.** Зокрема, це означає, що закон має вказувати:

– список злочинів, здійснення яких може привести до перехоплення повідомлень;

– обмежуватися випадками, коли фактичні підстави підозрювати особу в здійсненні тяжкого злочину уже виявлені іншими засобами (Класс);

– санкціонувати перехоплення тільки на підставі мотивованої письмової заяви визначеної високої посадової особи (Класс);

---

[25] Прослушивание телефонных разговоров в международном праве и законодательстве одиннадцати европейских стран. – Харьков: Фолио, 1999. – 152 с. Слід відзначити, що усі вказані справи були пов’язані з прослуховуванням телефонних розмов. На наш погляд, сформульовані принципи відносяться до будь-яких видів зняття інформації з каналів зв’язку.

– дозволяти перехоплення повідомлень тільки після одержання санкції посадової особи або органу, що не належить до виконавчої влади, бажано, судді (Класс);

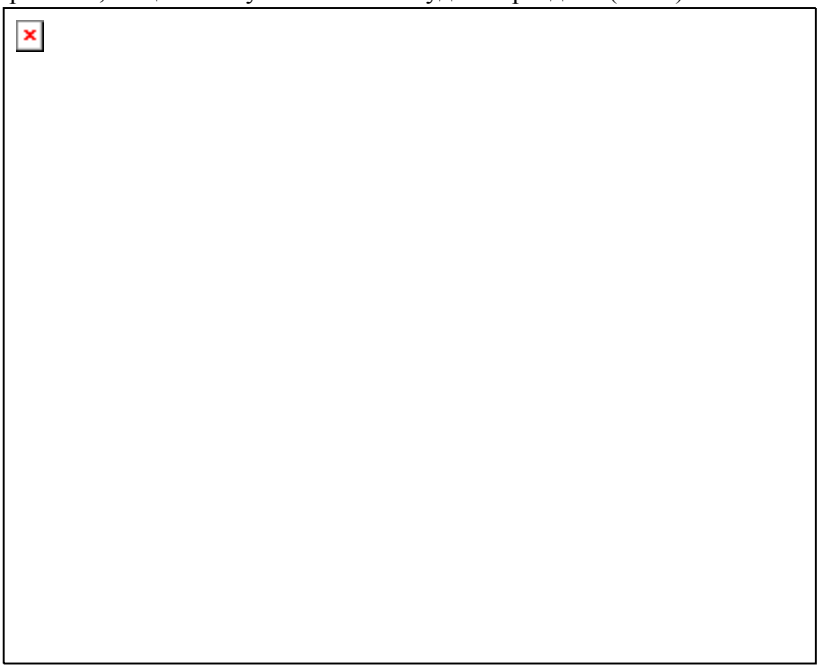
– встановлювати обмеження на тривалість перехоплення: повинний бути зазначений період, протягом якого санкція на перехоплення дійсна (Ювіг, Крюслен);

– визначати правила, що стосуються звітів, які містять матеріали перехоплених повідомлень (Ювіг, Крюслен);

– передбачати запобіжні заходи проти обміну цими матеріалами між різними державними органами (Ювіг, Крюслен);

– визначати обставини, за якими записи можна чи необхідно знищити (Ювіг);

– встановлювати, що треба робити з копіями або переписаними матеріалами, якщо обвинувачена особа буде виправдана (Ювіг).



Перехоплення повідомлень повинне також здійснюватися як **необхідне в демократичному суспільстві**, тобто «тільки в такій мірі, що необхідна для безпеки демократичних інститутів», і «за виняткових умов, що необхідні у демократичному суспільстві в інтересах національної безпеки і/або попередження заворушень чи злочину» (Класс).

Нарешті, будь-яка особа в країні, де діє закон про таємне перехоплення повідомлень, може вимагати визнання себе жертвою без будь-яко-

го обов'язку наводити докази чи навіть на підставі голослівного твердження, що спостереження дійсно велося.

ЧИ ЗАДОВОЛЬНЯЄ УКРАЇНСЬКЕ ЗАКОНОДАВСТВО ПРО ОПЕРАТИВНО-РОЗШУКОВУ ДІЯЛЬНІСТЬ ПРИНЦИПАМ, ВСТАНОВЛЕНИМ ЄВРОПЕЙСЬКИМ СУДОМ З ПРАВ ЛЮДИНИ?

Позитивні моменти, що будуть схвалені Судом: процедура має основу в національному законодавстві, вона передбачувана, санкція на зняття інформації з каналів зв'язку дається судом і тільки «з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншим способом одержати інформацію неможливо» (ч.2 статті 8 Закону про ОРД), існує вказівка про знищення отриманих у результаті ОРД відомостей, які стосуються особистого життя, честі та гідності людини. Проте, Суд навряд чи визначить процедуру задовільною:

а) Суд навряд чи визнає, що втручання держави в приватне життя «необхідне в демократичному суспільстві», оскільки перелік злочинів, за яких воно допускається, – тяжкі й особливо тяжкі – надмірно широкий. Як відзначив Суд у справі Класса, право на секретне спостереження за громадянами є характерним для поліцейських держав, а в демократичних державах, відповідно до Конвенції, таке спостереження може бути терпимим тільки у випадку крайньої необхідності для збереження демократичних інститутів. Крім того, на стадії ОРД досить часто важко визначити, чи йдеться саме про тяжкий чи особливо тяжкий злочин. Отже, слід було б дати чіткий перелік злочинів, у випадку скоєння чи підготовки яких дозволено використовувати зняття інформації з каналів зв'язку.

б) Суд, очевидно, визнає законодавство недоступним через те, що процедура одержання санкції на зняття інформації з каналів зв'язку регулюється малодоступними відомчими інструкціями. Ця процедура повинна бути чітко описана в законі про ОРД при проведенні ОРЗ у вигляді зняття інформації з каналів зв'язку з метою запобігання і припинення тяжких і особливо тяжких злочинів, і в Кримінально-процесуальному кодексі при проведенні слідства після порушення кримінальної справи (зауважимо, що стаття 187 Кримінально-процесуального кодексу потребує доопрацювання, щоб відповідати критеріям доступності і передбачуваності).

в) українське законодавство є явно недостатнім для того, щоб задовольнити критерію «якості закону», воно не містить досить ефективних гарантій проти зловживань. По-перше, відсутні чіткі вказівки про тривалість процедур негласного стеження, по-друге, майже нічого не сказано про передачу, використання і збереження зібраних матеріалів, про складання підсумкових доповідей, по-третє, незалежний нагляд за законністю

явно недостатній, особливо якщо порівнювати його з німецькою чи угорською процедурою парламентського контролю.

Отже, Закон про ОРД потребує суттєвих змін.

ПЕРСПЕКТИВИ

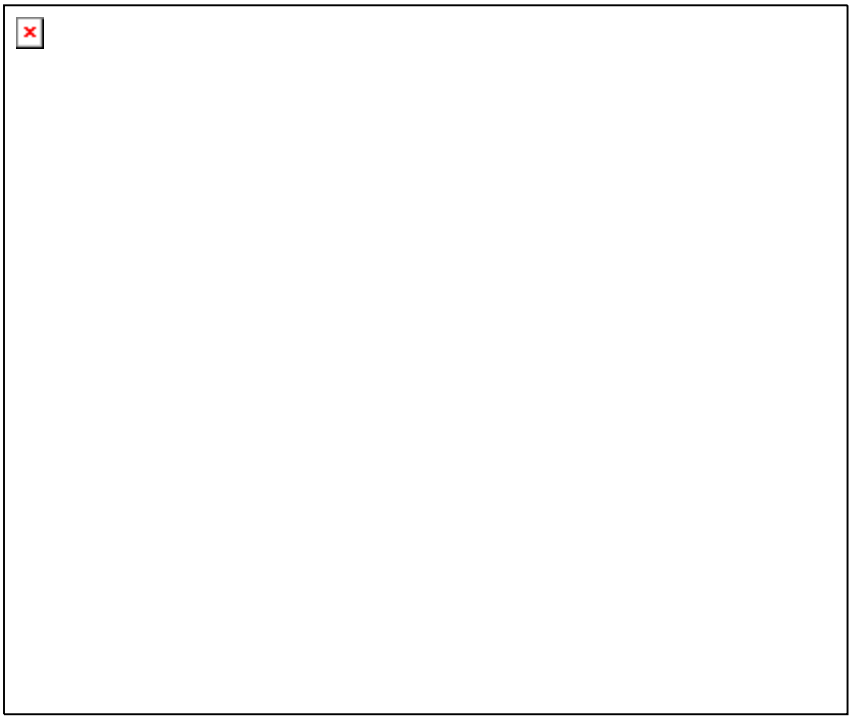
Стрімкий розвиток Інтернет докорінно змінив світ. Нові інформаційні технології несуть не тільки небачені можливості для інтелектуального і технічного прогресу, але й несподівані засоби і способи здійснення злочинів. Злочинність стала набагато більш витонченою з використанням інформаційних технологій. Шантаж, переслідування, загрози життю помітно спростилися, адже зловмиснику технічно легко залишитися непізнаним. У Мережі поширені різні схеми шахрайства. З'явилися і чисто комп'ютерні злочини: атаки хакерів на сайти великих кампаній та державних органів, розкрадання фінансових засобів через Інтернет. Як показало недавнє дослідження, проведене кампанією Gartner Group, число фінансових махінацій в Інтернет у 12 разів більше, ніж у «реальній» банківській системі США. За даними Європейської Комісії в 2000 році з кредитних карток європейців було украдено 553 млн. доларів, причому біля половини злочинців діяло через Інтернет[26]. Звісно, спецслужби повинні володіти адекватними можливостями для попередження і розслідування таких злочинів. Ріст організованої злочинності, тероризму, наркобізнесу вимагає неординарних дій спецслужб у припиненні і розкритті злочинів, а для цього необхідні дедалі більш досконалі методи і засоби отримання інформації. Унаслідок цього і з'являються такі системи контролю комунікацій, як міжконтинентальний проект Echelon (США, Великобританія, Канада, Австралія і Нова Зеландія), проект Європейського Союзу Enfopol, російський СОРМ та інші. Створена подібна система і в Україні.

Ще в лютому 2001 року на сайті СБУ було розміщено текст під назвою «Щодо моніторингу мережі Інтернет»[27], де СБУ визнавало, що здійснює моніторинг інформації, яка передається або отримується з використанням систем і засобів зв'язку. Моніторинг було визначено як процедуру, «яка здійснюється уповноваженими державними органами з метою виявлення на законних підставах інформації в телекомунікаційному просторі нашої країни, зміст якої становить безпосередню або опосередковану загрозу політичній, економічній, військовій або іншій безпеці держави». Незрозуміло, правда, що саме вважається телекомунікаційним простором нашої країни, оскільки Інтернет не має кордонів. І хоча у повідомленні стверджувалося, що моніторинг здійснюється «у суворій відповідності з законом», інший фрагмент того ж тексту це спростовував: «Прин-

[26] Сергей Смирнов. Прив@тность. – М.: Права человека, 2002. – С.23.

[27] www.sbu.gov.ua

ципово нові можливості формування інтегрального телекомунікаційного середовища у глобальному масштабі об'єктивно виключають можливість застосування національних законів, що ґрунтуються на географічних кордонах і традиційних поняттях державного суверенітету». Проте легалізувати моніторинг було необхідно, і СБУ підготувала законопроект «Про моніторинг телекомунікацій», у якому фактично закріплювала функціонування існуючої системи і технічні вимоги до неї. Він був внесений до парламенту 7 серпня 2003 р. під номером 4042.



У законопроекті описані правові та організаційні основи моніторингу телекомунікацій під час проведення оперативно-розшукової, контрозвідувальної і розвідувальної діяльності з метою забезпечення безпеки громадян, суспільства і держави. Під моніторингом телекомунікацій законопроект розуміє спостереження, відбір за визначеними ознаками, оброблення та реєстрацію сеансу зв'язку в мережах телекомунікацій із застосуванням системи моніторингу мережі телекомунікацій. Він здійснюється виключно як засіб оперативно-розшукової, контррозвідувальної і розвідувальної діяльності. Технічні засоби системи моніторингу і засоби доступу до неї розміщують провайдери – оператори систем телекомунікацій, а засоби управління системою моніторингу розміщує спеціально уповноважений орган – СБУ, який і здійснює моніторинг. У цілому до

системи моніторингу висуваються досить високі вимоги, зокрема, вона повинна забезпечити можливість гарантованого доступу в режимі реального часу до сеансу зв'язку користувача мережі, що є об'єктом моніторингу, ідентифікувати, копіювати та оформляти зміст сеансу його зв'язку і надати скопійованим повідомленням вигляду, у якому вони були послані. Система моніторингу повинна впроваджуватися практично на всіх мережах телекомунікацій загального користування, і після впровадження процес моніторингу є прерогативою СБУ і цілком відокремлюється від провайдера. При цьому передбачається, що провайдер придбає чи забезпечить розробку системи моніторингу за власні кошти. Питання гарантій від зловживань в законопроекті майже не розглядається, він містить тільки декілька відсилочних норм до закону про ОРД.

Однак в усіх без винятку країнах відсутність реального нагляду за діями спецслужб неминуче призводить до зловживань і до стеження за тими, хто здається владі небезпечними. Сьогодні більше 90 країн практикують незаконний контроль за інформацією опозиції, правозахисників, журналістів, профспілкових діячів та просто людей, що нешаблонно мислять. Тому проекти контролю комунікацій усюди зустрічають опір. Наприклад, Сенат США відмовився недавно фінансувати проект, що припускав створення електронної системи для збору всіляких даних про американців: від їхніх електронних листів до результатів медичних обстежень і банківських транзакцій. У країнах колишнього СРСР, де стеження за інакодумцями в минулому було нормою життя і де контроль за діями спецслужб сьогодні вкрай слабкий чи взагалі відсутній, побоювання за недоторканність своєї кореспонденції видаються цілком природними. Не став винятком і законопроект СБУ про моніторинг телекомунікацій. Проблема тут у площині довіри або недовіри до спецслужб. Оскільки СБУ не виявила свою принципову відмінність від колишнього «караючого меча», а скоріше навпаки, характер її дій часто нагадував про стиль сумної пам'яті 5-го управління КДБ, то і ставлення українців до ідеї моніторингу комунікацій відповідне. Ну, не вірять вони, що СБУ буде діяти законно. І або протестують проти прийняття закону взагалі, або, визнаючи, що моніторинг необхідний для успішної боротьби зі злочинністю, вимагають передбачити в законі надійні гарантії проти зловживань. А в цьому сенсі законопроект ще гірший, ніж закон про ОРД. Незалежний нагляд за законністю відсутній. Ст.10 наказує знищувати інформаційні повідомлення, відібрані помилково, інших повідомлень про збереження знятої інформації немає, а є тільки вказівка, що порядок ведення, зберігання та використання протоколу моніторингу визначається Кабінетом Міністрів України. У статті 12 зазначено, що не підлягає розголошенню інформація стосовно особистого життя, честі та гідності особи, що стала відома в процесі здійснення моніторингу. І все.

Панує думка, що система моніторингу зводить нанівець необхідність одержання санкції в суді перед кожним зняттям інформації – мовляв, на-

віщо: усе підготовлено, підключайся і знімай. Як на мене, ці побоювання є наслідком відсутності довіри до правоохоронних органів. На мій погляд, вони якраз будуть звертатися до суду за санкцією, і важко уявити ситуацію, коли український суддя їм відмовить. Цю проблему можливо вирішити суто технічно, якщо автоматично ініціювати доступ до сеансу зв'язку винятково за санкцією, переданою з комп'ютера судді, який прийняв рішення про проведення моніторингу. Але отут виникає інше питання. Інтернет не знає державних кордонів, і, перехоплюючи повідомлення якого-небудь громадянина України, правоохоронні органи з неминучістю будуть втручатися в процес його інформаційного обміну з громадянами інших держав, на перехоплення повідомлень яких вони, узагалі говорячи, права не мають. Цей момент ані законопроект, ані закон про ОРД ніяк не враховують. Далі, очевидно, що поняття моніторингу не укладається в рамки «зняття інформації з каналу зв'язку» щодо певної особи, яке розглядається в законі про ОРД. З вимог до системи моніторингу можна побачити, що в процесі моніторингу буде досліджуватися трафік без прив'язки до конкретної особи, відносно якої є дані про причетність до скоєного злочину чи злочину, що готується. Це схоже на дії рибалки, що закидає невід і сподівається піймати яку-небудь рибу. Не виникає сумнівів у тім, що істинна мета моніторингу – не викрити конкретного злочинця, а знайти його, одержати інформацію про підготовку до здійснення злочину чи вже скоєний злочин. Але одержання судової санкції в цьому випадку втрачає сенс, а можливості для сваволі нескінченні. Ані законопроект про моніторинг, ані закон про ОРД узагалі не розглядають трафік як об'єкт правового регулювання і, відповідно, навіть не постає питання про гарантії дотримання законності. Але ж це питання стає ключовим при дослідженні трафіку в контексті дотримання права на приватність. Отже, закон не прописує гарантій від зловживань у випадку дослідження трафіку.

Реакція суспільства на появу законопроекту №4042 не забарилася. Спільними зусиллями депутатів, недержавних організацій і операторів зв'язку був створений законопроект «Про перехоплення телекомунікацій», який був внесений в парламент народним депутатом Валерієм Лебедівським 1 червня 2004 р. під номером 4042-1. На мою думку, в цілому законопроект заслуговує на високу оцінку, в центрі уваги його – дотримання права на приватність в поєднанні із створенням ефективного механізму перехоплення. Як можна переконатися, автори врахували європейські угоди щодо захисту приватності в подібних системах, передбачили незалежний контроль за законністю перехоплення та гарантії проти зловживань. Проте поза межами законопроекту залишився пошук невизначених осіб шляхом дослідження трафіку – процедур, якими широко користуються спецслужби (наприклад, пошук по ключовим словам). Отже, проблема правового регулювання моніторингу у цьому випадку залишається відкритою.

ЛИСТ ВЕРХОВНОГО СУДУ УКРАЇНИ №16/6 ВІД 19. 11. 1996Р.

Головам Верховного Суду Автономної Республіки Крим, обласних, міжобласного. Київського і Севастопольського міських судів, військових судів регіонів і Військово-морських сил

Про тимчасовий порядок розгляду матеріалів про **дачу дозволу на проникнення до житла чи іншого володіння особи, накладення арешту на кореспонденцію і виїмку поштово-телеграфних установ та зняття інформації з каналів зв'язку (телефонних розмов, телеграфної та іншої кореспонденції)**

У зв'язку із запитами про порядок дачі дозволу на проникнення до житла чи до іншого володіння особи (стаття 30 Конституції), накладення арешту на кореспонденцію і виїмку її в поштово-телеграфних установах та зняття інформації з каналів зв'язку (стаття 31 Конституції, стаття 8 Закону України "Про оперативно-розшукову діяльність") Верховний Суд України звертає увагу судів на таке:

Згідно зі статтею Конституції кожному гарантується недоторканність житла.

Проникнення до житла чи іншого володіння особи може мати місце не інакше, як за вмотивованим рішенням суду.

У невідкладних випадках, пов'язаних із врятуванням життя людей та майна чи з безпосереднім переслідуванням осіб, які підозрюються у вчиненні злочину, можливий інший, встановлений законом, порядок проникнення до житла чи іншого володіння особи.

Відповідно до статті 31 Конституції України кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо.

Перехідні положення Конституції на дію Статті 30 Конституції в частині дачі дозволу на проникнення до житлового приміщення чи до іншого володіння особи та на дію статті 31 Конституції не поширюються.

Оскільки норми Конституції України є нормами прямої дії, дозвіл на проникнення до житла чи до іншого володіння особи, накладення арешту на кореспонденцію, її виїмку та зняття інформації з каналів зв'язку здійснюється тільки судом. До прийняття відповідних законів розгляд таких матеріалів має здійснюватися судом відповідно до норм законодавства

про оперативно-розшукову діяльність, боротьбу з корупцією, організованою злочинністю в частині, що не суперечить Конституції України, та з обов'язковим дотриманням таємниці інформації, що знаходиться в матеріалах оперативно-розшукової або кримінальної справи.

При цьому слід мати на увазі:

1. За поданням відповідного органу, який здійснює оперативно-розшукову діяльність, дізнання чи досудове слідство, розгляд матеріалів здійснюється невідкладно Верховним Судом, обласними та прирівняними до них судами в порядку, що визначається керівництвом цих судів.

2. Для розгляду подання суддя може витребувати від відповідного органу для ознайомлення матеріали, якими обґрунтовується необхідність обмеження конституційних прав особи.

3. Розглянувши подання суддя виносить постанову про:

а) дачу дозволу на проникнення до житла чи до іншого володіння особи, накладення арешту на кореспонденцію, її виїмку в поштово-телеграфних установах чи зняття інформації з каналів зв'язку — телефонних розмов, телеграфної та іншої кореспонденції. В постанові зазначається термін дії дозволу.

б) відмову в застосуванні таких заходів.

4. Рішення обласного та прирівняного до нього суду про відмову в застосуванні заходів може бути переглянуте Верховним Судом України, рішення якого є остаточним.

5. Постановою судді, який дав дозвіл на застосування заходів, може бути продовжено термін його дії.

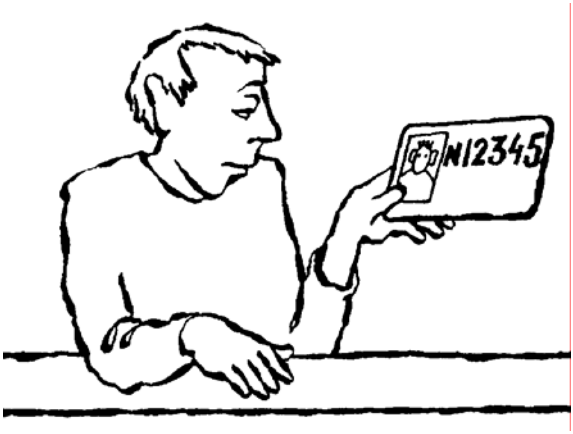
6. Скасування застосованих заходів здійснюється відповідним органом або судом у разі, коли необхідність цього заходу відпала.

7. Дані, одержані в результаті застосування зазначених заходів, долучаються до справи лише у разі, коли визнані доказами у справі. В такому разі до справи долучається і копія постанови судді про застосування заходів.

8. Матеріали провадження (оригінали подання і постанови судді) зберігаються у відповідному суді за правилами таємного діловодства.

9. Лист Верховного Суду України 5-6н 122 від 1 жовтня 1996 року з цього питання відкликається.

Голова Верховного Суду України В. Ф. Бойко


N12345

ПРАВО НА ПРИВАТНІСТЬ ТА ІДЕНТИФІКАЦІЯ ОСОБИ

Саймон Девіс, Privacy International

ІДЕНТИФІКАЦІЙНІ КАРТКИ

Питання, що виникають найчастіше

У цій доповіді досліджуються ключові аспекти, пов'язані з використанням ідентифікаційних карток та технологій, на основі яких вони створені. Privacy International підготувала цю доповідь, зважаючи на зростання в усьому світі стурбованості з приводу застосування сучасних систем ідентифікації. В наші наміри входить обговорення на міжнародному рівні реальних фактів та поширення обміну інформацією щодо проблем, створених такими картковими системами.

Основний автор цієї доповіді – Саймон Девіс, генеральний директор Privacy International і науковий співробітник Лондонської Школи економіки. Свій внесок та допомогу у підготовку доповіді надали члени Privacy International по всій Північній Америці, Європі та Азії.

1. Скільки країн використовують ID картки?

У тому чи іншому вигляді ідентифікаційні картки використовуються в багатьох країнах світу. Типи карток, їх зміст та функції дуже різняться. Близько 100 країн мають офіційні обов'язкові ідентифікаційні картки, що використовуються для різних цілей. Однак у багатьох розвинених країнах таких карток не існує. Серед них: США, Канада, Нова Зеландія, Ірландія, країни півночі і Швеція. Не мають таких карток зокрема Німеччина, Франція, Бельгія, Греція, Люксембург, Португалія та Іспанія.

Використання спеціалізованих карток у сфері охорони здоров'я та соціального забезпечення є дуже поширеним. Більшість країн, де не існує універсальної державної картки, мають медичну картку або картку соціального забезпечення (Medicare в Австралії, номер соціального забезпечення в Сполучених Штатах), або традиційні паперові ідентифікаційні документи. І навпаки, у Швеції, де існують національні номери з широкою сферою застосування, немає єдиної офіційної ідентифікаційної картки.

Загалом, особливо в розвинених країнах, ключовим елементом карток є їх номер. Він використовується як адміністративний механізм для різних цілей. У багатьох країнах номер є загальним засобом, що забезпечує доступ до інформації про діяльність власника картки в різних сферах життя.

Дослідження ідентифікаційних карток по всьому світові виявляє багато цікавих фактів. Найбільш важливим серед них є фактична відсутність карток у країнах загального права. Ні економічний, ні політичний

розвиток країни не визначає наявність карток. Ні Мексика, ні Бангладеш їх не мають. Дотепер не було карток і в Індії (навіть зараз, насправді, ідентифікаційна картка є скоріше реєстраційною карткою виборця, ніж державною ідентифікаційною карткою. Однак абсолютна більшість розвинених країн мають або систему ідентифікаційних карток, або використовують паперові документи, що частіше передбачають скоріше регіональну авторизацію, ніж загальнодержавну.

У багатьох державах ідентифікаційні документи замінюються пластиковими картками, які є більш довговічними і надійними з точки зору складностей для підробки. Компанії, що займаються виготовленням карток, мають добре розвинену систему розповсюдження своєї продукції, включаючи навіть найбільш віддалені райони світу. Деякі країни Азії та Африки замінюють старі документи на аналогічні з магнітною стрічкою або маркіровкою. У 1996 році документи водія автотранспортного засобу в Сполученому Королівстві були замінені на фотографічні ідентифікаційні картки. Зміна форми картки на іншу завжди супроводжується зміною характеру та змісту інформаційної структури документа.

2. Які головні цілі запровадження ідентифікаційних карток?

Існує багато причин запровадження ідентифікаційних карток. Расові, політичні й релігійні ознаки часто були підставою для старих систем ідентифікації. Небезпека повстання або політичний екстремізм, дискримінація за релігійними ознаками часто є мотивацією введення систем ідентифікації, що повинно було б змусити ворогів держави зареєструватися, або зробити їх становище вразливим за відсутності необхідних документів. У Пакистані картки використовуються для встановлення системи квотування, в Китаї вони є засобом побудови суспільства.

У Сполученому Королівстві поточні пропозиції щодо національної ідентифікаційної картки обумовлені необхідністю розвитку документа, прийнятного для інших європейських країн, а також вірою в те, що такі плани можуть сприяти боротьбі із злочинністю. В Австралії метою запропонованого запровадження картки була боротьба проти ухилення від сплати податків, а в Новій Зеландії – реалізація права на соціальне забезпечення. В Голландії картка введена з подвійною метою – як засіб підвищення ефективності державного управління і водночас вона є ключовим елементом для спрощення процедури прикордонного контролю.

В основі таких планів лежить посилення влади поліції. Навіть у демократичних країнах у поліції залишається право вимагати документи, що засвідчують особу, під загрозою затримання.

За останні роки ідентифікаційні картки почали пов'язуватися із системою реєстрації, яка, у свою чергу, лежить в основі державного управління. В таких системах, наприклад, в Іспанії, Португалії, Таїланді та Сінгапурі, ідентифікаційні картки стали лише одним помітним компонентом набагато більшої системи. З появою магнітних стрічок та мікропроцесорних технологій ці картки стали також засобом для доступу до державних

послуг. Таким чином, картки стали поєднанням засобів обслуговування та ідентифікації.

Про цю подвійну функцію було добре сказано сенатором із Філіппін у передмові до розробленого нею законопроекту 1991 року про ідентифікаційні картки як інтегрованого засобу зв'язку між громадянином та його урядом

3. Які основні типи ідентифікаційних систем існують?

Узагальнюючи, можна виділити три різних системи ідентифікаційних карток:

1. Окремі документи
2. Реєстраційна система
3. Інтегрована система

Окремі документи виготовляються в примітивних умовах або за обставин, коли існує загроза неочікуваних економічних і політичних змін. Часто на територіях, де владу здійснює військове керівництво або діють закони надзвичайного стану, в обіг вводяться місцеві ідентифікаційні картки, які по суті є внутрішніми паспортами. Їх головна мета – встановлення права проживання особи на певній території.

Більшість ідентифікаційних систем включають у себе допоміжний реєстр, де знаходиться паралельно така ж інформація, що міститься на картці. Як правило, цей реєстр створюється органами місцевої влади. В меншості країн це є національною системою. Навіть в таких країнах як Франція та Німеччина немає національного реєстру ідентифікаційних карток. У Німеччині існує конституційне обмеження на введення державного ідентифікаційного номера.

По суті всі системи карток, що були запроваджені за останні 10 років, є інтегрованими системами. Вони створені таким чином, щоб стати основою для загального державного управління. В результаті номер картки став державним реєстраційним номером, що використовується як загальний ідентифікатор багатьма державними установами.

Цікаво, що жителі країн, де використовуються паперові документи, часто називають їх англійською ICs або Identity cards. Афганська Tazkira – це 16-сторінковий буклет, але його часто називають карткою, так само як і в Польщі, де посвідчення особи – це схожий на паспорт буклет, що має назву «Dowod osobisty» (або, дослівно, посвідчення особи), але частіше перекладається як картка.

4. інформацію містять ідентифікаційні картки?

Більшість карток, що використовуються в розвинених країнах, містять у собі таку інформацію: ім'я, стать, дата народження та вихідні дані випуску самої картки. Також вказується термін дії, номер картки, залишається вільне місце для підпису. Меншість вузькоспеціалізованих (секторальних) карток ще мають фотокартку. Картки, що офіційно видаються поліцією або міністерством внутрішніх справ, містять фотокартку а також, у багатьох випадках, відбитки пальців.

У Бразилії, наприклад, усі жителі зобов'язані постійно мати при собі пластикові гнучкі картки, що за розмірами схожі на кредитну картку і містять фотокартку, відбиток великого пальця, повне ім'я, по батькові, державну приналежність (бразилець чи іноземець) і серійний номер.

У Чилі це – маленька пластикова картка з фото, іменем, датою та місцем народження, підписом та особистим номером. Корейська «Державна Реєстраційна Картка» вказує ім'я, дату народження, постійну адресу, тимчасову адресу, запис про військовий обов'язок, назву органу, що її видав, дату видачі, фото, державний ідентифікаційний номер і відбитки великих пальців обох рук.

Малайзійська ідентифікаційна картка вказує ім'я, дату народження, імена батьків, релігійну та етнічну приналежність, стать, фізичні характеристики, місце народження та деякі інші ідентифікаційні відмітки на зворотному боці. На лицевій стороні знаходяться фото, відбитки пальців і номер ідентифікаційної картки.

Пакистанська картка містить у собі великий обсяг інформації, включаючи фото, підпис, серійний номер картки, підпис представника влади, дату видачі, номер поштового відділення, номер ідентифікаційної картки, ім'я, по батькові, тимчасову адресу, постійну адресу, ідентифікаційні відмітки і дату народження.

Німецька «Personalausweis» – це пластикова картка, на лицевій стороні якої знаходяться ім'я, дата і місце народження, національність, термін закінчення дії, підпис і фото. Ім'я, дата народження і номер картки зчитуються автоматично. На зворотній стороні – адреса, зріст, колір очей, назва державного органу, що видав картку і дата видачі. Зміна адреси на картці відбувається шляхом наклеювання нового на старий.

Італійські картки відрізняються більшим розміром (три чверті дюйма) і містять у собі ідентифікаційний номер, ім'я, фото, підпис, відбиток пальця, дату і місце народження, громадянство, місце проживання, адресу, сімейний стан, фах і фізичні характеристики.

В окремих випадках, зокрема в Сінгапурі і деяких країнах Азії, на картках ставиться маркіровка, яку державні органи вважають більш надійною за магнітну стрічку. Французи також переходять до карток, що зчитуються автоматично.

5. Яка фінансова вартість системи ідентифікаційних карток?

На Філіппінах, у Сполученому Королівстві і в Австралії вартість запровадження системи ідентифікації стала головною причиною політичного та громадського спротиву на загальнонаціональному рівні. Наміри Філіппін щодо запровадження системи ідентифікації грунтувалися на урядових розрахунках, підготовлених, як це часто буває, фахівцями в галузі комп'ютерної техніки. Потім з'ясувалося, що очікувані витрати були нижчими реально необхідних. Протягом семи років треба було витратити додатково вісім мільярдів песо. Це стало головною причиною відхилення пропозиції.

В Австралії вартість запровадження ідентифікаційної картки вплинула на те, що довелося виключити з попередніх планів витрати на проведення навчання, адміністративний нагляд, плинність кадрів, оплату роботи у вихідні дні та лікарняних листів, витрати на узгодження та закордонний випуск карток. Інші витрати, що рідко включають у загальну суму витрат (як це було, наприклад, в Австралії) пов'язані з підробкою, непередбачений заздалегідь додатковий випуск карток і витрати на приватний сектор. Як результат – офіційна вартість Австралійської картки в період з 1986 по 1987 роки збільшилась майже вдвічі.

Витрати на введення ідентифікаційної картки у приватному секторі є надзвичайно високими. Австралійська Асоціація Банкірів очікує, що така система потребує вкладення понад ста мільйонів доларів протягом 10 років. Загальна вартість запровадження карток у приватному секторі може скласти близько одного мільярда доларів на рік.

Офіційний кошторис витрат на введення Австралійської картки складав 820 мільйонів доларів протягом семи років. Доопрацьований бюджет, що включав у себе витрати на приватний сектор, а також інші фактори, збільшився в кілька разів.

Державний центр інформаційних технологій Великобританії (Information Technology Center) повідомив, що державна «розумна» картка може коштувати від п'яти до восьми фунтів стерлінгів на одну особу. Але ці цифри не враховують управлінські витрати, різні узгодження й т.ін. У серпні 1996 Міністр у справах Королівства Майкл Говард повідомив про запровадження державної ідентифікаційної картки і заявив, що її вартість імовірніше за все вдвічі перевищить розрахунки центру інформаційних технологій (від десяти до п'ятнадцяти фунтів).

6. Чи можуть ідентифікаційні картки допомогти в роботі правозастосовчих органів?

Хоча дотримання правопорядку є основною мотивацією запровадження ідентифікаційних карток у багатьох країнах, для поліції ці переваги виявились незначними. У Великобританії Міністр у справах Королівства Майкл Говард на конференції Консервативної партії в 1994 році заявив, що, за його переконанням, ідентифікаційна картка може стати безцінним засобом боротьби із злочинністю. Це твердження дещо втратило свою вагу під час розробки проекту.

Воно також отримало незначну підтримку з боку академічних та правозастосовчих органів. Асоціація Начальників Поліції (Association of Chief Police Officers) повідомила, що її члени більше схиляються до добровільної системи, а в разі запровадження обов'язкової картки вважають, що вона може зашкодити стосункам з громадськістю. Керівництво Голландської поліції не підтримало пропозицію щодо введення аналогічної системи за схожими мотивами.

На думку представників поліції обох країн головною проблемою, з якою вони стикаються у боротьбі із злочинністю є не відсутність ідентифікаційних процедур, а збір доказів та переслідування правопорушників. Однак деякі співробітники поліції і фахівці в галузі кримінології наводять свідчення того, що наявність картки могла б вплинути на зменшення злочинності та успішне переслідування злочинців. У доповіді Асоціації Начальників Поліції Великобританії за 1993 рік, говориться, що кількість вуличних злочинів, крадіжок та злочинів, скоєних із використанням фальшивих документів могла б зменшитись завдяки введенню ідентифікаційної картки, хоча ці твердження суперечать позиції Асоціації про те, що картки мають бути добровільними.

Насправді лише національна база даних ДНК (таку нещодавно створено у Великобританії) або база даних біометричної інформації (як було запропоновано в Онтаріо) можуть допомогти поліції у встановленні зв'язку між злочинами та особами, що їх скоїли.

Один з аргументів на підтримку введення карток полягає в передбаченні того, що вони будуть сприяти дотриманню правопорядку внаслідок розуміння людьми наявності постійного контролю над ними. Іноді картки пропонуються як засіб, що зменшує можливості для злочинної діяльності. В 1989 році уряд Сполученого Королівства схилявся до запровадження машинозчитувальних ідентифікаційних карток для боротьби з насиллям та хуліганством під час футбольних матчів. Загалом ідея полягала в тому, що картки дозволяли б їх власникам пройти на певну територію і зайняти визначене місце. В разі, якщо власник картки був втягнений у будь-який конфлікт на цій території, картка могла бути анульована. Пропозицію було відхилено після доповіді Лорда Головного Судді (Lord Chief Justice), де говорилося, що така ідея збільшує небезпеку виникнення безпорядків і складає загрозу для життя людей, якщо виникне катастрофа або інші надзвичайні обставини.

Одним із непередбачуваних наслідків запровадження ідентифікаційних карток може бути зростання кількості злочинів у сфері підробки документів. Здолавши один раз перешкоди при ідентифікації, злочинці можуть користуватися картками в інших випадках. Порожні бланки навіть банківських карток з високим рівнем захисту в таких країнах як Сінгапур можна придбати всього за кілька фунтів. Уже через два місяці після випуску в Австралії Банком Співдружності нових голографічних карток з високим ступенем захисту в обігу знаходилися добре виготовлені підробки.

Це питання обговорювалося в Австралії, Сполученому Королівстві і Нідерландах. Усе побудовано на простій логіці: чим вища цінність карток, тим ширша сфера їх застосування, а це, безумовно, робить їх більш привабливими для злочинних елементів.

Такі чинники дуже суперечать аргументам на користь дотримання правопорядку. Багато людей стурбовані тим, що вони бачать, як система правосуддя не може справитися з правопорушниками, і цінність ідентифікаційної картки в цьому сенсі видається сумнівною.

7. Як впливають ідентифікаційні картки на ухилення від сплати податків, отримання прибутків обманним шляхом?

Необхідність вдосконалення засобів боротьби з шахрайством стала причиною введення інтегрованих інформаційних систем з широкою сферою застосування в більшості розвинених країн. Іноді така стратегія включає в себе запровадження ідентифікаційних карток.

Збитки від шахрайства можуть бути досить значними, однак корені цього явища часто мають людські або організаційні аспекти, де технології не можуть повністю бути засобом вирішення проблем.

Службами соціального забезпечення по всьому світу визначені основні чинники шахрайства. Часто називають три основних рівні шахрайства. За ступенем важливості їх можна класифікувати наступним чином:

- Неправдиве декларування або недекларування доходів та витрат (проблема головним чином стосується ухилення від сплати податків)
- Отримання прибутків злочинним шляхом, використовуючи фальшиві документи, що посвідчують особу
- Крадіжка та підробка платіжних документів.

Ці чинники слід враховувати разом з багатьма іншими факторами, які призводять до непорозумінь у цій сфері, включаючи зокрема помилки з боку службовців і недостатність знань щодо умов сплати.

Говорячи про шахрайство, однією з центральних проблем є загальна складність визначення природи шахрайства і його впливу. Фактично не існує етнографічних досліджень у цій сфері й та інформація що існує, отримана шляхом внутрішнього і зовнішнього аудиту, із звітів відповідних управлінців та ретроспективних досліджень. Багато методик пов'язані лише з оцінкою загрози, а не з визначенням реальних масштабів шахрайства. До цього часу не розроблено певних стандартних правил для оцінки інформаційних технологій, створених для контролю за шахрайст-

вом та ідентифікації. Додаткові проблеми стосуються визначення шахрайства й умов здійснення контролю, що часто не збігаються у внутрішніх дослідженнях, які проводять податкові служби.

Оцінки поширення фальсифікації даних, що подаються в податкові заклади, дуже різняться. Департамент соціальних служб Торонто, наприклад, офіційно визначив шкоду, спричинену шляхом обману при ідентифікації менше ніж в одну десяту відсотка від загальної суми прибутку. Водночас Департамент соціального забезпечення Австралії називає цифри в десять разів більші. Взагалі такі оцінки розходяться від однієї десятої відсотка до більше чотирьох відсотків від загальної суми соціальних виплат. У Британії ці суми оцінюються в межах від одного до двох мільярдів фунтів стерлінгів, що є, за міжнародними мірками, верхньою межею у визначеному спектрі.

Парламентський комітет з питання Австралійської картки попередив, що обіцяні переваги від запровадження картки є лише здогадками. Департамент фінансів відмовився підтримувати фінансові пропозиції Комісії з питань медичного страхування (Комісія була організацією, включеною до планів запровадження картки). Очікувані прибутки постійно переглядались і зменшувалися, у той час як витрати продовжували зростати. Департамент соціального забезпечення запевнив, що ідентифікаційні картки мало в чому можуть допомогти для зменшення шахрайства у сфері соціального забезпечення. Розглядаючи пропозиції й посилаючись на висновки, зроблені Парламентським комітетом, Департамент заявив, що менше одного відсотка від суми перевитрат становили випадки, пов'язані з невірною ідентифікацією. Департамент дійшов висновку, що карткова система може спричинити нові види шахрайства.

Департамент соціального забезпечення Сполученого Королівства висловився проти карткової системи з тих же причин.

Австралійський Департамент соціального забезпечення визначив цифру вимушених витрат через невірну ідентифікацію в межах 0,6 відсотка від загальної суми збитків, у той час як розміри прихованих прибутків сягали 61%. Головний інтерес податкових служб полягає у створенні єдиної системи нумерації, що може використовуватися для працевлаштування, і яка могла б зменшити масштаби чорного ринку.

8. Чи можуть ідентифікаційні картки сприяти контролю за незаконною імміграцією?

І так, і ні водночас. Хоча питання, пов'язані з імміграцією, є важливим мотивом в усіх пропозиціях щодо запровадження ідентифікаційних карток у континентальній Європі, Сполучених Штатах і деяких менш розвинених країнах, однак вплив карток на проблему нелегальної імміграції не є однозначним.

Скасування внутрішніх кордонів стало першочерговою турботою Європейського Союзу. Шенгенська угода, укладена між країнами Бенілюксу, Францією, Іспанією й Німеччиною, передбачає ліквідацію пунктів

прикордонного контролю при одночасному посиленні внутрішніх процедур нагляду. Франція та Нідерланди вже ухвалили законодавчі акти, що дозволяють ширше здійснювати ідентифікаційні перевірки, решта країн, очевидно, йтимуть за ними.

Введення особистих ідентифікаційних документів у новій Європі без внутрішніх кордонів – процес, що сприймається неоднозначно, але саме він видається для багатьох зручним з огляду на більшу свободу пересування в межах Союзу.

Використання карток з метою перевірки статусу жителів віднесено до функцій поліції та інших чиновників, що мають широкі владні повноваження в питанні встановлення особи. З точки зору громадянських прав успіх цих заходів знаходиться в залежності від двох факторів: або значно підвищиться рівень постійного контролю за всім населенням, або це означатиме дискримінаційні перевірки, що будуть сфокусовані на меншинах.

Є два основних аргументи, що найчастіше використовуються для виправдання необхідності пошуку нелегальних іммігрантів в усіх країнах:

1) ці люди отримують робочі місця, що мають належати громадянам і особам, які мають постійне місце проживання;

2) вони часто незаконним шляхом отримують виплати по безробіттю і т. ін.

Образ нелегальних іммігрантів, які живуть за рахунок держави є дуже сильним. Його дуже ефективно використовують прихильники ідентифікаційних карток. Однак потім були зібрані науково обгрунтовані свідчення того, що насправді таке твердження не відповідає дійсності. Об'єднаний Парламентський Комітет з питання Австралійської картки розглядав це і дійшов висновку, що справжня кількість іммігрантів, які отримують певні виплати з боку держави, є незначною. Доповідь описує загальну ситуацію, а також окремо розглядає конкретні випадки з метою визначення їх точного числа. У Новому Південному Уельсі з понад 57 тисяч іноземців, дозволений термін перебування яких у країні закінчився, було виявлено тільки 22, що отримували державні виплати по безробіттю. Тобто 22 особи із п'ятимільйонного населення. Департамент імміграції та етнічних стосунків заявив, що ця цифра насправді в тридцять разів вища і складає не 0,4%, а 12,4% від загального числа іноземців, які незаконно залишилися на території країни.

Насправді більшість імміграційних служб світу в основу своїх висновків закладають якісні характеристики. Знову ж таки, повертаючись до Австралійської картки, стає зрозуміло, що очікувана кількість нелегальних іммігрантів грунтувалась на здогадках, відсоток працевлаштованих нелегальних іммігрантів був побудований на здогадках, відсоток приїжджих, хто нелегально отримав роботу, визначений у доповіді Департаменту, є також здогадкою… У Комітету не було забагато складностей, щоб відхилити дані Департаменту імміграції та етнічних стосунків як такі, що є явно перебільшеними.

9. Чи сприяють ідентифікаційні картки посиленню влади поліції?

Загалом так. Огляд з питань ідентифікаційних карток, зроблений Privacy International, показав, що зловживання владою з боку поліції за допомогою карток мають місце практично в усіх країнах. У більшості таких випадків людей свавільно затримували, коли вони не могли пред'явити свою картку. Також засвідчені факти побиття неповнолітніх або представників меншин. Були навіть випадки масової дискримінації людей на підставі тієї інформації, що містилася на картках.

Хоча насправді на картках знаходяться не вразливі дані, які важко використати проти особи, картки часто стають засобом для дискримінаційних дій. Поліція, якій надано повноваження вимагати посвідчення особи, має право затримувати людей, які не мають картки, або які не можуть посвідчити свою особу. Навіть у такій розвиненій країні як Німеччина законом передбачено в таких ситуаціях право на затримання людей протягом 24 годин. Питання про те, хто саме підлягає такій перевірці, повністю віддано на розсуд поліції.

Ідентифікаційні картки часів війни застосовувалися у Сполученому Королівстві і пізніше. Вони знаходилися в загальному використанні до початку п'ятдесятих років. Поліція вимагала пред'явлення картки, поки в 1953 році Верховний Суд не визнав таку практику незаконною. Потім це призвело до скасування Закону про державну реєстрацію і всієї системи ідентифікаційних карток. Лорд Головний Суддя (Lord Chief Justice) зауважив:

«...хоча поліції можуть бути надані певні владні повноваження, це не означає, що вона може користуватися ними в усіх випадках... очевидно, що на сьогодні поліція, за існуючим порядком, вимагає пред'явлення державної реєстраційної ідентифікаційної картки, якщо вони зупинили водія в будь-якому місці з будь-якого приводу. Цей закон був ухвалений з метою дотримання безпеки, а не в тих цілях, за якими він зараз використовується..., в цій країні ми завжди пишалися добрими стосунками між поліцією та суспільством, а такі дії змушують роздратоване суспільство скоріше перешкоджати поліції, аніж сприяти їй».

10. Чи сприяють ідентифікаційні картки дискримінації?

Так. Успішне застосування ідентифікаційних карток як засобу боротьби із злочинністю або нелегальною імміграцією буде залежати від дискримінаційних перевірок, об'єктом яких стануть меншини.

Парадокс ідентифікаційної картки полягає в тому, що вона за визначенням сприяє дискримінації. Дискримінаційна практика – невід'ємна частина функціонування ідентифікаційної картки. Без такої дискримінації поліція була б змушена проводити випадкові перевірки, що в свою чергу було б політично неприйнятним.

Будь-яка дискримінація базується на одному з двох наступних принципів: ситуативний і секторальний. Ситуативна дискримінація застосо-

вується в незвичних ситуаціях, зокрема стосовно людей, які здійснюють нічні прогулянки, відвідують певні місця, які ведуть певний спосіб життя або дотримуються незвичної моди. Секторальна дискримінація вражає тих, хто має певні характерні ознаки: чорношкірі, молодь, британголові, мотоциклісти або бездомні. Ідентифікаційні картки, що містять інформацію релігійного або етнічного характеру, дозволяють ще на крок далі застосовувати дискримінаційний підхід.

Кілька розвинених країн за останній час були звинувачені в проведенні дискримінаційних дій з використанням ідентифікаційних карток. Уряд Японії нещодавно «потрапив під вогонь» Комітету ООН з прав людини за подібну практику. Комітет висловив занепокоєння тим, що в Японії був прийнятий законодавчий акт, яким на іноземців, що знаходяться на території держави, покладено обов'язок завжди мати при собі документи, що посвідчують особу. Комітет з 18-ти членів вивчав питання про дотримання прав людини в Японії відповідно до положень Міжнародного пакту про громадянські та політичні права 1966 року. Японія ратифікувала Пакт у 1979 році. У своєму висновку Комітет заявив, що Закон про реєстрацію іноземців є несумісним з положеннями Пакту.

Іронічний вигляд має те, що Парламенти кількох європейських країн, включаючи Францію й Голландію, ухвалили закони, що зобов'язують кожного ідентифікувати себе в багатьох ситуаціях, наприклад, на робочому місці, футбольному стадіоні, у громадському транспорті, у банку. Хоча формально картки називають добровільними, вони по суті є обов'язковим документом, який кожен громадянин Голландії завжди повинен мати при собі. Крім того, від іноземців можуть вимагати посвідчити свою особу в будь-який час за будь-яких обставин.

Французьку поліцію звинуватили в диспропорційному використанні ідентифікаційних карток проти чорношкірих і, особливо, алжирців. Звинувачення на адресу уряду Греції стосувалися застосування даних про релігійну приналежність, що містяться на державних картках, як засобу дискримінації стосовно людей, які не належать до грецької православної церкви.

11. Наскільки широко буде застосовуватися ідентифікаційна картка як внутрішній паспорт?

По суті ідентифікаційна картка є формою внутрішнього паспорта. Насправді сфера використання ідентифікаційних карток у всьому світі стає ширшою, ніж це передбачалося попередньо. Цей розвиток нових непередбачених заздалегідь цілей використання ідентифікаційних карток стає відомим як плаваюча функція.

Усі ідентифікаційні картки – як добровільні так і обов'язкові, – переросли у внутрішні паспорти різних видів. Без перебільшення можна сказати, що картка стає схожою на ікону. Їх застосування відбувається на підставі нерозумних норм або політики нехтування іншими засобами іде-

нтифікації, таким шляхом, що створює значні складності для тих, хто не має картки. **Картка стає важливішою, ніж особистість.**

Використання карток у більшості країн стало повсюдним. Усі державні соціальні виплати, стосунки з фінансовими закладами, працевлаштування або оренда житлових приміщень, оренда автомашин чи обладнання, отримання документів, здійснення всіх цих дій вимагає картки. Також вона застосовується в безлічі інших простих ситуацій, як вхід до офіційних установ (де охорона може забрати і залишити у себе картку).

Парадоксально, що багато хто протилежним чином тлумачить такий стан справ (картка допомагає людям у стосунках з владою, а не є дозволом для спілкування з владою). Кампанія з приводу Австралійської картки була викликана тим, що **картка ставала фактично дозволом на життя.**

Зрозуміло, що будь-яка офіційна ідентифікаційна система буде поступово включати в себе нові й нові функції. Не варто зважати на заяви про те, що офіційна картка є добровільною і що вона менш придатна виконувати функції внутрішнього паспорта, ніж обов'язкова картка. Насправді добровільні картки можуть мати недолік, який полягає в обмеженій законодавчій врегульованості.

Під час проведення кампанії проти Австралійської картки деякі радіостанції полюбляли повторювати цитату з одного параграфа проекту введення Австралійської картки: «Важливо зменшити будь-яку несприятливу реакцію суспільства на запровадження системи. Один із можливих варіантів полягає в тому, що на початку лише найменш вразливі дані будуть занесені до системи, з передбаченими можливостями введення додаткових даних пізніше, коли суспільство буде більше готовим до сприйняття цього».

Організатори кампанії наголошували на псевдодобровільній природі карток. Хоча технічно особа не була зобов'язана отримувати картку, було б надзвичайно складно жити в суспільстві без неї.

12. Що може статися у випадку втрати чи крадіжки ідентифікаційної картки?

Фактично в усіх країнах, де діють ідентифікаційні картки, повідомляється, що їх втрата або пошкодження створюють серйозні проблеми. Більше п'яти відсотків карток губляться, викрадаються або пошкоджуються щороку. В результаті можуть бути недоступними спеціальні соціальні виплати, а в більш широкому розумінні – неможливість ідентифікації особи.

Парадокс існує і при заміні карток. Заміна інтегрованих карток з високим ступенем захисту вимагає значного втручання органів влади. Видача документів має відбуватися офіційно і централізовано. Цей процес може забрати кілька тижнів. Хоча більш прості картки можуть бути замінені швидше, їх втрата складає загрозу через можливість підробки.

Люди, що втрачають гаманець з документами, швидко розуміють усі нещастя і неприємності, що можуть бути за цим. Одна втрачена ідентифікаційна картка може мати такий же вплив на життя людини.

13. Як впливають ідентифікаційні картки на приватність?

Кажучи стисло, вплив є дуже великим. Розміщення біографічних даних про людину в сотні не пов'язаних між собою базах даних – важлива умова, що є засобом захисту приватності. Збір і порівняння даних із цих окремих інформаційних центрів складає найбільшу загрозу для приватності. Будь-яка багатоцільова державна ідентифікаційна картка справляє такий ефект.

Деякі захисники приватності у Великобританії виступають проти ідентифікаційних карток, посилаючись при цьому на свідчення про різну загрозу їх використання в приватному секторі. Головним чином тут ідеться про передбачення, що в будь-який час один відсоток від числа персоналу захоче продати конфіденційну інформацію заради отримання прибутку. Щороку в багатьох країнах Європи до одного відсотка банківських працівників звільняють з роботи, часто через крадіжки.

Очевидність існування такої потенційної корупції є безперечною. Останні дослідження, проведені в Австралії, Канаді і Сполучених Штатах показують широкомасштабні зловживання у сфері комп'ютеризованих даних. Корупція серед користувачів інформацією в державних структурах та поза ними набуває ендемічного і епідемічного характеру в Новому Південному Уельсі. Практично всі приклади втручання у сферу приватності пов'язані з комп'ютерною обробкою і зберіганням даних.

Законодавство про захист даних взагалі не пристосовано до питань, пов'язаних з використанням ідентифікаційних карток. Насправді законодавство більшості країн сприяє застосуванню карток і водночас ніяк або дуже мало обмежує сферу їх використання чи накопичення інформації на картці або в пов'язаних з нею системах.

14. Чи існують країни, що відмовились від використання ідентифікаційних карток?

Так, кілька. Наприклад, запровадження Французької ідентифікаційної картки було зупинено на багато років через громадську та політичну опозицію. До кінця 70-х років від жителів Франції вимагали пред'явлення державних посвідчень особи. Вони були паперовими, і тому існував ризик їх підробки. В 1979 році Міністерство внутрішніх справ оголосило плани запровадження більш захищеної автоматизованої пластикової картки. Мета їх введення передбачала боротьбу з тероризмом та охорону правопорядку. Для забезпечення картками всього 50-ти мільйонного населення Франції необхідно було більше десяти років. Для їх виробництва було передбачено використання найновіших лазерних технологій.

Спочатку виник невеликий спротив цій пропозиції, але, подібно до прикладу Австралії (див. нижче), з появою нових подробиць проекту по-

літичний та громадський спротив зростав. Хоча ідентифікаційні номери не використовувалися (тільки номер картки), виникло занепокоєння з приводу можливого впливу, що справлятимуть картки. Французький заклад з нагляду за інформацією – CNIL – виступив проти автоматичного зчитування інформації з запропонованих карток, але тоді оптичний контроль за інформацією робив зайвою магнітну стрічку. Такі видання як Le Figaro висловлювали занепокоєння щодо можливості поєднання карток і пов'язаної з ними інформації з іншими поліцейськими та адміністративними системами.

Громадські дебати значно посилились у 1980 році, коли Союз Магістратів (Union of Magistrates) висловив стурбованість з приводу того, що картка потенційно обмежуватиме право на свободу пересування. У відповідь на ці та інші критичні зауваження CNIL було ухвалено рішення про те, що не можуть використовуватися особисті номери, проте кожна картка може мати такий номер. У випадку заміни картки новий номер стосувався б лише нового документа.

Долю ідентифікаційної картки змінили соціалісти, що отримали перемогу на виборах у 1981 році. У своїй виборчій програмі в питанні інформаційних технологій Франсуа Міттеран висловив думку, що створення машинозчитувальних ідентифікаційних карток є реальною загрозою для свободи людей. Його занепокоєння було підтримано Міністром юстиції Робером Бадінтером, який пояснив, що ідентифікаційні картки представляють реальну загрозу для особистих свобод і приватного життя громадян. Після цього новий Міністр внутрішніх справ оголосив, що ідентифікаційні картки не будуть вводитись у Франції. Проект потім знову було представлено наступним консервативним урядом.

У Сполучених Штатах основними аспектами у питанні ідентифікаційної картки стали недоторканність особи і державний суверенітет. Незважаючи на серйозне занепокоєння з приводу шахрайства, ухилення від сплати податків і незаконної імміграції, наступні адміністрації відмови-

лись від запропонованої ідентифікаційної картки. Розширення номера соціального забезпечення (SSN – Social Security Number) до рівня ідентифікаційної картки було відхилено Адміністрацією соціального забезпечення в 1971 році. В 1973 році Дорадчий комітет з питань автоматизованих систем персональних даних Секретаря з охорони здоров'я, освіти та соціального забезпечення дійшов висновку про небажаність державного ідентифікатора. В 1977 році Адміністрація Картера підтвердила, що номер соціального забезпечення не стане державним ідентифікатором, а в 1981 році Адміністрація Рейгана оголосила, що вона категорично проти створення ідентифікаційної картки. Під час обговорення реформ у галузі охорони здоров'я Адміністрація Клінтона постійно наголошувала, що вона проти державного ідентифікатора.

Але, незважаючи на суперечливі законодавчі норми, насправді номер соціального забезпечення продовжує виконувати роль державного ідентифікатора. За деякими розрахунками існує від 4 до 10 мільйонів фальшивих номерів, що викликає громадське занепокоєння, адже в такому разі номери соціального забезпечення фактично можуть сприяти зростанню нелегальної імміграції і шахрайства. Однак планів оновлення номерів поки що не існує.

Деякі федеральні агентства мають право використовувати номери соціального забезпечення. Серед них: Адміністрація соціального забезпечення (Social Security Administration), Комісія цивільних служб (Civil Service Commission), Служба внутрішніх прибутків (Internal Revenue Service), Департамент Оборони, Департамент Юстиції, Департамент Енергетики, Казначейство, Державний Департамент, Департамент Внутрішніх Справ, Департамент Праці, Департамент у справах ветеранів та всі федеральні служби, що використовують їх як ідентифікатори з метою зберігання даних. Державні установи також можуть використовувати номер для охорони здоров'я, а також з метою забезпечення матеріального добробуту та прибутків. Крім того треті сторони мають право звертатися за перевіркою номера соціального забезпечення для надання товарів та послуг.

Пропозиції Адміністрації Клінтона щодо реформ у сфері охорони здоров'я в США, розроблені за останні місяці, включають у себе плани покращання управління та обміну інформацією між страхівниками та постачальниками послуг. Передбачено також і введення державної картки, хоча федеральний уряд запевнив, що вона не буде за своєю природою мати загального застосування. Останні пропозиції у сфері працевлаштування також викликали протести через зростаючу стурбованість тим, що ці ініціативи можуть призвести до появи державної ідентифікаційної системи.

Найбільш успішну кампанію проти національної ідентифікаційної картки було проведено 10 років тому в Австралії. В 1986 році уряд Австралії представив законопроект, що передбачав введення державної ідентифікаційної картки під назвою «Австралійська картка». Головні завдан-

ня полягали в тому, щоб сформувати основу для управління основними державними службами, налагодити контакти між фінансовими інституціями та державними органами, а також виконання звичних завдань щодо ідентифікації, необхідних у комерційному секторі і в сфері соціального забезпечення.

Картка стала головною темою єдиної і найбільшої в новітній історії Австралії громадянської кампанії і, звичайно, найбільш значною кампанією такого роду у світі. Десятки тисяч людей вийшли на вулиці, у той час як серед урядовців погляди в цьому питанні розійшлися. Пропозиція викликала настільки ворожу реакцію, що в 1987 році було вирішено відмовитись від картки.

У 1991 році уряд Нової Зеландії розробив стратегію реформування системи охорони здоров'я та соціального забезпечення через розвиток програми збору даних і запровадження секторальної державної ідентифікаційної картки. Передбачалося, що картка стане засобом зв'язку між державними установами й допоможе контролювати всі фінансові операції і навіть географічне пересування. Цей план отримав назву «соціальний банк», а картка – «Ківі-картка».

Пропозиція введення державної картки викликала роздратування серед прихильників громадянських свобод і законодавчих реформ. Почасти через те, що таким чином може бути запроваджена частково платна система охорони здоров'я, частково через відсутність законодавчого захисту й частково тому, що можуть бути створені значні проблеми для певних меншин. У серпні 1991 року почалася кампанія проти цих планів, на чолі якої виступила Ауклендська Рада Громадянських Свобод. На відміну від учасників австралійської кампанії, що проходила на чотири роки раніше, активісти кампанії в Новій Зеландії мали прецедент, що допомагав розробити стратегію.

Хоч боротьба проти Ківі-картки не скрізь була настільки ефективною, як кампанія щодо Австралійської картки, як результат було досягнуто відмову від картки, натомість була запроваджена вузькоспеціалізована картка (двох видів), для отримання доступу до послуг у сфері охорони здоров'я.

24 серпня 1996 р.

Переклад з англійської Романа Романова та Олександра Парфенюка

ВВЕДЕННЯ ТА ВИКОРИСТАННЯ ОСОБИСТИХ ІДЕНТИФІКАЦІЙНИХ НОМЕРІВ: ПИТАННЯ ЗАХИСТУ ДАНИХ

Неофіційний переклад

Дослідження підготовлено Комітетом експертів Ради Європи з питань захисту даних у межах повноважень Європейського Комітету правового співробітництва.

Переклад зроблено Романом Романовим з брошури The introduction and use of personal identifcation numbers: the data protection issues. Strasbourg, Council of Europe, Publishing and Documentation Service, 1991, ISBN 92-871-1935-X

ПЕРЕДМОВА

Внесок Комітету експертів із питань захисту даних у створення та поширення міжнародної політики щодо захисту даних не обмежується тільки розробкою правових механізмів. Дійсно, відкриття до підписання 28 січня 1981 року першого міжнародного юридично зобов'язуючого документа з питань захисту даних – Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція про захист даних), і зараз вважається найбільшим досягненням Комітету. Але не менш важливими та успішними можна вважати намагання Комітету експертів запровадити загальні правила щодо окремих аспектів обробки даних. Шість рекомендацій, прийнятих Комітетом міністрів Ради Європи, що охоплюють різні сфери діяльності, пов'язаної з обробкою даних, засвідчують наполегливість, з якою Комітет експертів просуває саме секторальний підхід у питаннях захисту даних (Рекомендації № R(81)1, автоматизовані бази медичних даних; № R(83)10, наукові дослідження та статистика; № R(85)20, прямий маркетинг; № R(86)1, соціальна безпека, № R(87)15, поліція; № R(89)2, працевлаштування; № R(90)19, виплата заробітної плати та пов'язані з цим операції).

Та все ж робота Комітету експертів виходить за межі підготовки проектів правових актів. Він також проводить обговорення різних актуальних, іноді термінових, питань приватності. Це відбувається під час сесій, що проходять двічі на рік. Обмін інформацією з таких питань як СНІД, засоби інформації, генетика, роль саморегулювання в забезпеченні захисту даних і т. ін., допомагає відчути представникам усіх урядів держав-членів (заради повноти треба згадати також спостерігачів від інших міжнародних організацій, а також країн, що не є членами Ради Європи) проблеми, пов'язані з захистом даних, які стосуються вищезгаданих питань. Таким чином вони мають можливість обмінюватися досвідом та ви-

робляти пропозиції щодо розв'язання різних проблем, застосовуючи порівняння.

Іноді такі дискусії вказували на необхідність більш детального вивчення окремих питань. У такому разі може бути, наприклад, створено робочу групу для вивчення проблеми і подання інформації про можливі шляхи її розв'язання. Подібний підхід було застосовано щодо проблем захисту даних, що викликані використанням новітніх технологій. Перед тим, як викласти сухою юридичною мовою загрозу для захисту даних, що її утворюють новітні технології, Комітет експертів вирішив опублікувати висновки та дослідження своєї робочої групи (див. дослідження, що має назву «Новітні технології – виклик приватності?»)

Те ж саме стосується питань, що виникли у зв'язку із введенням і використанням особистих ідентифікаційних номерів та створених ними проблем для захисту даних. У ході обміну думками щодо особистих ідентифікаційних номерів Комітет експертів зауважив, що ця проблема не викликає байдужості. Представники держав-учасниць висловлювали різний рівень стурбованості стосовно планів їх введення та/або використання. Таке ж ставлення було відображено й у відповідях, що їх отримав Комітет на своє попереднє прохання, адресоване урядам держав-членів Ради Європи. Опитування ставило за мету отримати інформацію для з'ясування таких питань:

а) національне законодавство (якщо існує), яке регламентує введення та використання особистих ідентифікаційних номерів;

б) причини, що спонукали певні країни запровадити систему особистих ідентифікаційних номерів;

в) проблеми захисту даних, що виникли в різних країнах внаслідок введення та використання особистих ідентифікаційних номерів.

Комітет вважав, що обсяг та розмаїття інформації, отриманої в ході опитування, так само як і його власні попередні висновки стосовно делікатного питання особистих ідентифікаційних номерів, принаймні через стурбованість значної кількості країн, заслуговують подальшого дослідження. Тому Комітет створив невелику дослідницьку групу, до складу якої ввійшли експерти із Федеративної Республіки Німеччини, Нідерландів та Швеції, для більш глибокого вивчення всього спектра проблем, що можуть виникати у зв'язку із введенням та використанням особистих ідентифікаційних номерів, для політики захисту даних. Дослідницька група, що збиралася з 12 по 13 червня 1989 року, у стислі строки виконала доручення Комітету, підготувавши разом із секретаріатом доповідь з цього питання. Для її підготовки було використано, зокрема, інформацію, подану державами-учасницями, а також власний досвід членів групи.

Необхідно взяти до уваги, що групу було свідомо складено Комітетом експертів таким чином, щоб врахувати досвід трьох країн: Федеративної Республіки Німеччини, де особисті ідентифікаційні номери загального багатоцільового характеру було визнано анафемою для власної гід-

ності; Швеції, де особисті ідентифікаційні номери в такому вигляді були прийнятними протягом тривалого часу, але зараз відбуваються зміни в напрямку обмеження їх використання, а також Нідерландів, де особисті ідентифікаційні номери мали окремі вузькі сфери застосування, але згідно з новими законодавчими пропозиціями очікується подальше поширення їх використання. Цілком очевидно, що коло обговорюваних дослідницькою групою питань було зосереджено далеко поза правовими системами лише цих трьох країн. Так само висновки, викладені наприкінці цієї доповіді, розраховані для використання всіма урядами, розробниками політики в сфері захисту даних та правозастосовчими органами. Не пропонується жодних правових механізмів. Скоріше, є сподівання, що цим урядам та органам буде корисно вивчити ці питання, а також проллється світло на можливі шляхи розв'язання проблем, використовуючи можливість порівнювати та вивчати досвід. Комітет експертів із питань захисту даних вважає, що саме таким чином він може зробити значний внесок у обговорення проблем захисту даних у Європі.

ГЛАВА 1

Особисті ідентифікаційні номери: визначення, сфера їх можливого застосування; з чого вони можуть складатися; сучасні тенденції

Розробники цієї доповіді розуміли особисті ідентифікаційні номери як унікальний засіб ідентифікації індивідів в адміністративних реєстрах та базах даних. Це не означає, що особисті ідентифікаційні номери не мають застосування поза сферою діяльності державних органів. Особисті ідентифікаційні номери можуть бути засобом доступу до великого обсягу послуг у приватному секторі, наприклад, номер банківського рахунку, членський номер у клубі, номер читача в бібліотеці або контрольний номер, наданий особі для санкціонованого доступу до системи обробки даних приватного підприємства. У доповіді не приділено належної уваги окремим сферам використання номерів або питанням конкретної діяльності/випадків у приватному секторі. Скоріше, вона зосереджена на використанні особистих ідентифікаційних номерів державними установами в адміністративних цілях і в приватному секторі.

У деяких країнах особисті ідентифікаційні номери є універсальним багатоцільовим ідентифікатором. Це означає, що особисті ідентифікаційні номери можуть використовуватися як для адміністративних цілей, так і в інтересах приватного сектора. Один і той же номер може бути податковим кодом, номером соціального забезпечення, номером паспорта, номером посвідчення водія автотранспортного засобу і в той же самий час кодом доступу до товарів та послуг у приватному секторі. Такий особистий ідентифікаційний номер базується на принципі адміністративного поєднання. З іншого боку, особистий ідентифікаційний номер може мати обмежене використання. Він може застосовуватися лише для однієї адміні-

стративної мети: управління реєстром платників податків, визначення права на соціальну допомогу, встановлення особи власника паспорта або іншого посвідчення. В такому разі дані особи буде розміщено в різних ідентифікаційних засобах для різних адміністративних цілей. Використання особистих ідентифікаційних номерів у конкретних сферах адміністративного управління відображає принцип функціонального розподілу.

Нарешті, є приклади використання особистих ідентифікаційних номерів для ідентифікації особи в реєстрі населення або в реєстрі актів цивільного стану, але вони не застосовуються з іншою метою.

Розглянувши ситуацію в конкретних державах-членах Ради Європи, можна описати шляхи складання та застосування особистих ідентифікаційних номерів, а також сучасні тенденції щодо їх введення та використання.

Австрія

В Австрії не існує універсального ідентифікатора, незважаючи на те, що надходять такі пропозиції всередині країни. Є лише вузькоспеціалізовані особисті ідентифікаційні номери. Проте з 1988 року номер соціального страхування може також використовуватися для деяких фіскальних цілей.

Бельгія

З метою управління реєстром населення кожну особу в Бельгії, незалежно від того, чи то громадянин, чи іноземець, має бути ідентифіковано. Цей ідентифікаційний номер, що було запроваджено відповідно до Закону «Про національний реєстр», ухвалений у 1983 році, має тенденцію до переростання у прийнятний ідентифікатор для інших адміністративних потреб, а це у свою чергу веде до відмови від вузькоспеціалізованих ідентифікаційних номерів, наприклад, номер соціального забезпечення або фіскальний номер. Ця тенденція до універсалізації номера в реєстрі населення має місце, незважаючи на те, що закон 1983 року передбачає, що питання використання особистих ідентифікаційних номерів має бути визначено королівським указом після консультацій з дорадчим Комітетом захисту приватності. Ці передбачені в законі гарантії не обмежили використання особистих ідентифікаційних номерів їх початковими цілями та обумовленими користувачами.

Кіпр

Адміністративні органи використовують такі основні види особистих ідентифікаційних номерів:

а) номер соціального забезпечення;

б) номер ідентифікаційної картки;

с) номер посвідчення водія автотранспортного засобу.

Номер посвідчення особи також використовується для податкового контролю за доходами. Ідентифікатори також самостійно застосовуються в приватному секторі, головним чином банками для здійснення операцій з банківськими рахунками та кредитними картками.

Данія

Відповідно до закону, прийнятого в 1968 році, запроваджено десятизначні номері, набір чисел яких складається з дати народження, серійного номера та контрольного числа. Жителів Данії включено до центрального реєстру населення, і їх можна знайти в ньому за допомогою особистого ідентифікаційного номера. У реєстр занесено загальні персональні дані всіх жителів для використання відповідними адміністративними органами або приватними структурами за певних обставин. Застосування особистих ідентифікаційних номерів державними органами є достатньо широким. У приватному секторі існують значні обмеження, встановлені Законом «Про приватні реєстри». Він регламентує захист даних у приватному секторі.

Фінляндія

У Фінляндії особисті ідентифікаційні номери було запроваджено в шістдесятих роках. Планувалося їх використання в галузі соціального забезпечення. Ідентифікаційний номер складається із десяти цифр та риски. Перші шість чисел відображають дату народження особи, наступні три складають серійний номер для розрізнення тих осіб, що народилися в один день. Непарні серійні номери означають належність до чоловічої статі, парні – до жіночої. Останнє число є контрольним.

Встановлено певні норми, що регламентують використання та занесення ідентифікаційних номерів. Зокрема передбачено їх використання в реєстрі населення для реєстрації нерухомості, у посвідченнях водіїв автотранспортних засобів, а також у картотеках кредитних установ. Роботодавець також зобов'язаний повідомляти податкові органи про доходи своїх працівників і вказувати їхні ідентифікаційні номери.

Коли приймався Закон «Про бази персональних даних», відповідний парламентський комітет звернув увагу на поширення використання ідентифікаційних номерів, що, на його думку, створює загрозу для приватності. Для вироблення подальших дій спеціальною інституцією – Омбудсменом з захисту даних, було проведено дослідження різних форм використання ідентифікаційних номерів.

Закон «Про бази персональних даних» регламентує використання персональних даних, зокрема занесення, використання та передачу ідентифікаційних номерів. До баз персональних даних може бути занесено лише ті персональні дані, що необхідні для конкретних цілей. Тому потреба використання ідентифікаційного номера має вирішуватися в кожному конкретному випадку.

Франція

Кожному, хто народився у Франції, присвоюється тринадцятизначний номер, що відображає стать, рік та місяць його/її народження, місце народження (департамент, район) і номер у реєстрі народження. Ця система має назву Numero d'identification au reportoire. Номер присвоюється Національним інститутом економічної статистики та досліджень. Як у

державному, так і в приватному секторі, існує велика кількість інших вузькоспеціалізованих номерів (номер посвідчення особи, реєстраційний номер військовослужбовців, номер соціального забезпечення, номер банківського рахунку). Вже здійснено, як це буде показано в одному з наступних розділів, заходи для запобігання переростання Numero d'identification au reportoire в багатоцільовий номер. Але може бути дозволено його використання в інших сферах, наприклад, у системі соціального забезпечення. Державні установи прагнуть більш широкого використання замість Numero d'identification au reportoire, оскільки вважають систему вузькоспеціалізованих номерів надто затратною для створення та управління; наприклад, у такому разі потрібна розробка нового програмного забезпечення. Орган, що займається питаннями захисту даних – Національний комітетом з обробки даних і громадянських свобод (CNIL – Commission nationale de l'informatique et des libertes), навпаки, наполягає на використанні окремих ідентифікаторів для конкретно визначених цілей. Його заклики до Генерального директорату податкової служби щодо введення замість Numero d'identification au reportoire спеціального фіскального номера для контролю за податковими відрахуваннями, увінчались успіхом.

Німеччина[28]

Загалом не існує ніякого універсального номера. Те, яким чином відбувається ідентифікація особи як у державному, так і в приватному секторі, залежить від конкретних обставин. Спроби введення єдиного ідентифікатора зустріли спротив з боку Бундестагу (Bundestag) та Федерального Конституційного Суду.

Греція

Законом, ухваленим у 1986 році, було введено реєстраційний кодовий номер (ЕКАМ). Передбачено його використання в посвідченнях особи, свідоцтвах про народження, списках виборців та картках виборців, паспортах, картках соціального забезпечення, посвідченнях водіїв автотранспортних засобів, реєстрах платників податків, муніципальних реєстрах, реєстрах грецьких консульств. Номери не використовуються універсально в державному секторі, але реально існують у щоденних стосунках між державою та громадянином. Таким чином їх застосування є досить широким.

Насправді, норми закону про ЕКАМ ще не застосовувалися. Беручи до уваги реакцію засобів масової інформації, а також громадську думку, уряд створив робочу групу, якій доручено розробити поправки до закону.

Ісландія

Разом із введенням національного централізованого реєстру населення в 1953 році було запроваджено систему особистих ідентифікаційних номерів для полегшення управління реєстром в адміністративних та

[28] Цей звіт було підготовлено перед об'єднанням Німеччини у 1990 році. Хоча для зручності використовується назва «Німеччина», проте в доповіді немає даних про колишню Німецьку Демократичну Республіку.

статистичних цілях. На цей час особистий ідентифікаційний номер є десятизначним і складається із дати народження (день, місяць, рік, століття), контрольного шифру та двох чисел, довільно встановлених для людей, народжених в один день. Однак у 1987 році було прийнято рішення про ширше застосування цих десятизначних номерів у сфері державного управління загалом, щоб запобігти проблемам, пов'язаним з іменною ідентифікацією. Окрім їх застосування в державному секторі, особисті ідентифікаційні номери, що присвоюються кожному в Ісландії протягом першого року після народження, зараз також використовуються в банківській діяльності і заносяться до кожного фінансового документа, пов'язаного з конкретною особою.

Новий закон про захист даних набрав чинності 1 січня 1990 року. Відповідно до параграфа 4, розділу 1 нового закону, його норми застосовуються до даних, які містять інформацію про приватні стосунки особи, навіть якщо її не названо, але ідентифіковано за допомогою особистого ідентифікаційного номера. Відповідно до параграфа 1, розділу 6 закону, передача реєстрів, що містять персональні дані, заборонена. Але дозволено доповнювати реєстр даними щодо конкретного особистого ідентифікаційного номера, навіть якщо їх отримано з даних реєстру стосовно третіх осіб.

Ірландія

В Ірландії не існує універсального багатоцільового особистого ідентифікаційного номера. Однак є вузькоспеціалізовані особисті ідентифікаційні, наприклад, номер соціального забезпечення, який використовується з певною метою.

Немає єдиного принципу формування цих номерів. Особисті ідентифікатори все більш широко використовуються в приватному секторі, особливо у сфері фінансових послуг.

Необхідно зазначити, що має місце дуже обмежене публічне обговорення переваг та недоліків введення встановленого державою багатоцільового ідентифікатора. Якщо мають місце такі дискусії, здається вірогідним, що питання захисту даних, пов'язані з особистими ідентифікаційними номерами, будуть уважно вивчатися.

Люксембург

Прийнятий 30 березня 1979 року Закон «Про числову ідентифікацію фізичних та юридичних осіб» передбачає присвоєння ідентифікаційного номера кожній фізичній особі (також і юридичним на основі різних критеріїв), що проживає в Люксембурзі від народження або внаслідок імміграції, чи будь-якій іншій фізичній особі, зареєстрованій державним органом або закладом соціального забезпечення, що має правове зобов'язання отримати номер. Номер складається з одинадцяти чисел і містить у собі дані про дату народження, стать; числа, які розрізняють людей, народжених в один день, один місяць одного і того ж року, а також контрольне число. Використання номерів обмежується діяльністю установ державно-

го управління або закладів соціального забезпечення і стосується виключно їх безпосередніх відносин з власником номера. Велика Герцогська Постанова від 7 грудня 1979 року з пізніше внесеними змінами встановлює перелік документів та баз даних, до яких мають заноситися ідентифікаційні номери фізичних та юридичних осіб. Постанова містить у собі одну невдалу норму, яка дозволяє власникам реєстрів та баз даних, що використовують особисті ідентифікаційні номери, делегувати свої повноваження щодо їх використання іншим особам та органам. Як результат цього, наприклад, заклади соціального забезпечення просять медичних працівників вказувати ідентифікаційні номери своїх пацієнтів, а роботодавців – ідентифікаційні номери своїх працівників у всіх документах, що мають бути їм надані. Органи, що займаються захистом даних у Люксембурзі, стурбовані таким розвитком цього процесу, оскільки здається, що використання особистих ідентифікаційних номерів виходить за межі кола уповноважених користувачів, визначених Законом від 30 березня 1979 року «Про числову ідентифікацію фізичних та юридичних осіб».

Нідерланди

Загальний адміністративний номер існує в Нідерландах з 1968 року. Але поки що цей номер використовувався лише муніципалітетами для реєстрів населення. У 1985 році було запропоновано поступовий перехід та поетапне введення вузькоспеціалізованих особистих ідентифікаційних номерів у конкретних сферах громадського життя, де існує достатня законодавча база, здатна мінімізувати небажане втручання у приватне та сімейне життя. Так податкове законодавство тепер передбачає, що систематичне декларування доходів супроводжується податковим номером відповідних осіб. До 1989 року податковий код міг використовуватися лише для контролю за сплатою податків. З того часу його сфера використання значно розширилась до всієї сфери соціального забезпечення. Пропозиції щодо об'єднання загального адміністративного номера з соціальним фіскальним номером стали об'єктом критики. Опоненти цієї ідеї відстоювали необхідність правового захисту і зокрема потребу в законодавстві щодо захисту даних, оскільки особисті ідентифікаційні номери можуть бути використані на потребу всіх державних служб. Таким чином у Нідерландах зараз відбувається поетапне введення єдиного ідентифікатора для всього державного сектора, але при цьому забезпечується правовий захист. Використання загального номера в приватному секторі не дозволяється.

Норвегія

Кожному жителеві Норвегії присвоюється особистий ідентифікаційний номер на підставі норм Закону «Про реєстр населення».

Особистий ідентифікаційний номер складається з 11 знаків. Перші шість чисел містять у собі дату народження: два числа означають день, два числа – місяць і два інших числа – рік. Наступні три числа відрізняють осіб, народжених в один і той самий день. Парне дев'яте число означає жіночу стать і непарне – чоловічу. Останні два числа – контрольні.

Окрім їхнього використання в реєстрі населення, особисті ідентифікаційні номери застосовуються зараз у деяких інших сферах державного управління, що потребують ідентифікації громадян, наприклад, соціальне забезпечення та оподаткування.

Використання особистих ідентифікаційних номерів як засобу ідентифікації частково поширилося і на приватний сектор, зокрема на банківську діяльність, страхування.

Органи державної влади, виконуючи свої функції, потребують інформації стосовно певного ідентифікаційного номера, і, як правило, відповідно до закону та підзаконних актів мають право вимагати від громадян надання такої інформації. Законність вимог приватних компаній щодо надання такої інформації залежить від того, чи передбачено це угодою.

У відповідності до Закону «Про реєстр населення» контроль за створенням реєстрів, що містять персональні дані, та використанням особистих ідентифікаційних номерів у реєстрах, здійснює Інформаційний Інспекторат (Data Inspectorate). Норми діючого законодавства та підзаконних актів забороняють використання особистих ідентифікаційних номерів у багатьох видах реєстрів та баз даних. Використання особистих ідентифікаційних номерів в інших реєстрах здійснюється відповідно до норм законодавства, статутів або за дозволом Інформаційного Інспекторату. Що стосується надання такого дозволу, то Інформаційним Інспекторатом встановлено правила збору, зберігання та використання особистих ідентифікаційних номерів.

Португалія

Введення єдиних національних номерів суворо заборонено ст.35 Конституції, що прийнята в квітні 1977 року, з наступними поправками та доповненнями, внесеними в 1982 та 1989 роках. Закон, прийнятий у 1973 році, фактично передбачав присвоєння ідентифікаційних номерів усім фізичним та юридичним особам. Особисті ідентифікаційні номери мали заноситися до всіх офіційних документів та реєстрів з 1 січня 1975 року. Цей закон увійшов у протиріччя з Конституцію 1977 року. Таким чином у Португалії не існує єдиного ідентифікатора, проте є вузькоспеціалізовані номери: номер посвідчення особи, що складається без будь-якого спеціального принципу формування, номер у списку виборців, фіскальний номер (послідовне число, що не несе в собі певного змістовного значення), номер соціального забезпечення і т. ін. Звичайно ж, у Португалії, як і в інших країнах, існує велика кількість різних номерів у приватному секторі, що використовуються з різною метою.

Іспанія

Незважаючи на те, що спроби введення універсального ідентифікатора на зразок таких, що використовуються в Скандинавських країнах, відбувалися протягом усіх сімдесятих років, система особистих ідентифікаційних номерів Іспанії все ще прив'язана до номера документа, що посвідчує особу громадянина. Декретом №196/76 із змінами, внесеними

Декретом №1245/85, визначено номер посвідчення особи, який реально містить у собі інформацію про те, де було видано цей документ, а не дату та місце народження власника – як «загальний особистий ідентифікаційний номер». Він використовується у відносинах державних органів з фізичними особами, а також для регулювання стосунків між конкретними структурами приватного сектора (наприклад, банками) та окремими особами. Однак номери розширено за рахунок додатку контрольних чисел державними або приватними органами, що безпосередньо їх застосовують. У відповідності до норм закону 7/1985 особам, які не мають іспанського громадянства, надається разом із документом про місце проживання, дозволом на працю і т. ін., серійний номер, що має використовуватися у стосунках із державними органами. Також (з 1966 року) особам, які не є громадянами Іспанії, присвоюється спеціальний окремий номер соціального забезпечення. Він відображає місце реєстрації, серійний номер і одне або два контрольних числа.

У 1990 році було запроваджено новий фіскальний номер, що складається з номера посвідчення особи, до якого додано кілька контрольних чисел, які невідомі громадянинові. Номер присвоюється кожному з моменту народження.

Швеція

Ще в 1947 році з метою запровадження більш загального та зручного методу ідентифікації осіб, ніж через використання їх імен, був введений реєстраційний номер народження. Поступово він переріс у цивільний реєстраційний номер для широкого багатоцільового використання і мав замінити собою вузькоспеціалізовані номери. Зараз це десятизначний номер, що офіційно вважається особистим ідентифікаційним номером. Він містить у собі інформацію про місце народження особи (два числа означають рік, два – місяць і два – день). Реєстраційний номер народження складено таким чином, щоб можна було визначити стать особи, а також щоб уникнути складності з особами, народженими в один день. Число 9 у швецькому особистому ідентифікаційному номері означає, що особа була народжена за кордоном. Вона може мати як швецьке громадянство, так і бути іноземним громадянином. Число 9 також може означати, що особистий ідентифікаційний номер цієї особи було змінено. Наступного року використання цієї системи буде припинено. В майбутньому особистий ідентифікаційний номер буде побудовано таким чином, що відображатиме, – народжена особа за кордоном чи ні. Нарешті, є контрольне число. Особистий ідентифікаційний номер присвоюється кожній особі, що зареєстрована як швецький резидент.

Окрім застосування для цивільної реєстрації, вони широко використовуються різними державними службами (податки, охорона здоров'я та соціальні послуги, паспорт, митниця, вибори, кримінальне розслідування, судочинство, виконання судових рішень, права на керування автотранспортним засобом і т. ін.). Вони також широко використовуються приват-

ним сектором, де існують бази персональних даних з використанням особистих ідентифікаційних номерів працівників, учасників приватних компаній, орендодавців та орендарів, власників кредитних карток і т. ін.

Отже, особистий ідентифікаційний номер у Швеції – це універсальний, багатоцільовий ідентифікатор. Комісія з питань захисту даних та відкритості представила пропозиції щодо звуження використання особистих ідентифікаційних номерів. Наприклад, запропоновано внести доповнення до Закону «Про захист даних», щоб зменшити кількість випадків, коли відбувається занесення особистого ідентифікаційного номера. Управління Інформаційного Інспекторату може вважатися компетентним органом для здійснення нагляду за використанням особистих ідентифікаційних номерів власниками реєстрів та баз даних. З іншого боку, питання, пов'язані з використанням особистих ідентифікаційних номерів, можуть бути врегульовані окремим законом, яким би зокрема було передбачено неможливість використання особистих ідентифікаційних номерів у реєстрі для автоматичної обробки даних, якщо особа, чиї дані заносяться до реєстру, на це не погоджується або у випадку відсутності правових підстав для таких дій. Доповідь Комісії зараз розглядається урядом країни.

Швейцарія

Хоча в Швейцарії не існує єдиного номера загального використання, номер соціального забезпечення (AVS) все більше виконує цю роль. Насправді номер соціального забезпечення застосовується багатьма приватними та державними установами для управління фондом медичного страхування, у відділах кадрів, у реєстрі населення і т. ін. Він використовується навіть військовим керівництвом. Номер складено таким чином, що містить у собі закодовану інформацію про особу (ім'я, стать, громадянство Швейцарії) та контрольне число.

Після проведеного дослідження щодо нової системи ідентифікації людей було зроблено висновок про те, що використання номерів соціального забезпечення має більше переваг, а тому прийнятним визнано розширення сфери їхнього використання.

Туреччина

У свідоцтві про громадянство Туреччини вказується номер його власника поряд з іменем та прізвищем, іменами обох батьків, датою та місцем народження. Також ця інформація заноситься до реєстру актів цивільного стану. Але громадянський номер не є універсальним багатоцільовим ідентифікатором.

Сполучене Королівство

У межах органів державної влади існує велика кількість вузькоспеціалізованих особистих ідентифікаційних номерів, наприклад, національний номер служби охорони здоров'я, національний страховий номер, податковий номер, номер посвідчення водія автотранспортного засобу. Такі номери можуть бути складені на підставі імені, місця народження разом з іншими числами або мати форму простих послідовних серійних номерів.

Практика є різною в залежності від сфери використання. Не дивно, що кількість ідентифікаторів у приватному секторі є досить великою. Дискусії, що відбуваються зараз щодо введення посвідчення особи, так само як і нової форми місцевого оподаткування, порушили проблему єдиного ідентифікаційного номера та загрози, яку вони можуть становити для свобод взагалі.

ГЛАВА 2

Переваги введення особистих ідентифікаційних номерів та можливі загрози для прав людини

ПРИЧИНИ ВИКОРИСТАННЯ ТА ПЕРЕВАГИ

Із збільшенням кількості угод між державою та особою, що більш характерно для благополучних держав, стає все більш важливим винайти точні засоби ідентифікації користувачів соціальних послуг. Повоєнне зростання кількості населення спричинило збільшення числа управлінців, що в свою чергу збільшило адміністративний тягар (а тому виникла потреба в раціональних реєстрах населення). Держава як постачальник (соціальне забезпечення, гранти, освіта, охорона здоров'я і т. ін.) та контролер (поліція, в'язниці, податки, пересування людей, надання прав на керування засобами пересування, заняття підприємницькою діяльністю і т. ін.) швидко збільшує застосування адміністративних реєстрів, картотек, баз даних. У такому все більш складному стані відносин присвоєння єдиного ідентифікатора кожному громадянинові в межах юрисдикції конкретної держави значно спрощує контроль та здійснення державними органами регулюючих функцій. Але переваги з точки зору ефективності управління можуть бути досягнуті як шляхом введення багатоцільових особистих ідентифікаційних номерів, так і вузькоспеціалізованих. Хоча особисті ідентифікаційні номери передували появі автоматизованої обробки даних (наприклад, реєстри населення в багатьох країнах існували задовго до виникнення автоматизованої обробки даних), застосування технологій обробки даних державними органами зробило ще більш вигідним для владних структур використання особистих ідентифікаційних номерів.

У багатьох національних звітах, на основі яких було підготовлено це дослідження, ідентифікаційні номери розглядаються як вигідний та економний засіб підвищення ефективності управління. Наприклад, у законодавчому акті від 30 листопада 1979 року, яким було введено фіскальний номер платника податків у Португалії, було посилання на адміністративні переваги, викликані введенням особистого ідентифікаційного номера. Згідно з преамбулою, особистий ідентифікаційний номер може гарантувати точну та швидку ідентифікацію платника податків; слугувати підвищенню ефективності контролю за виконанням фінансових обов'язків; спростити стосунки між органами влади та платником податків. Комітет Ліндопа (The Lindop Committee), чиї висновки призвели до підготовки законопроекту про захист даних Парламентом Сполученого Королівства

(пізніше в 1984 році став законом «Про захист даних») також визнає цінність системи єдиних ідентифікаторів.

«Можна довести, що якби кожному мешканцеві було присвоєно єдиний загальний ідентифікатор, і якби його застосовували всі користувачі даних в усіх випадках, повні витрати користувачів могли б бути зменшені. Також можна довести, що громадянин також мав би перевагу від того, що не було б потреби записувати чи пам'ятати різні засоби ідентифікації для кожного роду його діяльності». (Глава 29, параграф 6, Звіт Комітету з питань захисту даних, 1978 рік).

Система особистих ідентифікаційних номерів забезпечує також точну ідентифікацію осіб та правильність персональної інформації, що заноситься до комп'ютерних систем. Тут є два питання. По-перше, особистий ідентифікаційний номер може розглядатися як шлях уникнення ускладнень, що мають місце, коли імена осіб збігаються. Було зауважено, принаймні у двох звітах (Франція та Люксембург), що імена та прізвища є абсолютно недостатніми для точної ідентифікації осіб, особливо у тих справах, коли ідентифікація має фінансові наслідки (право на різні види допомоги, контрольні списки ненадійних боржників і т. ін.) або соціальні наслідки (наприклад, поліцейське досьє). Багато людей у різних країнах мають однакове ім'я, частково за рахунок зменшення кількості імен, що знаходяться у використанні, частково тому, що в певний час конкретні імена стають модними, тощо.

По-друге, точність має й інший вимір. Особистий ідентифікаційний номер може забезпечити органи влади правдивою та надійною інформацією, що заноситься до адміністративного реєстру, картотеки чи бази даних. З такої позиції точність більше стосується контролю та перевірки інформації, що подається особою до органу влади з метою встановлення підстав для користування певними правами, перевагами та пільгами (соціальне забезпечення, гранти, компенсації і т. ін.), або з метою їх звільнення від певних стягнень чи інших покарань (податки, суспільні зобов'язання і т. ін.). Той факт, що інформацію про особу занесено до кількох баз даних для різних адміністративних цілей, дозволяє органам влади перевіряти точність наданої інформації, порівнюючи її з іншими базами даних. Універсальний ідентифікатор значно спрощує процес редагування та звірення інформації. І звичайно, автоматизована обробка даних ще більше покращує та спрощує цей процес. Так, наприклад, особа може звернутися до конкретного органу влади за грантом для отримання освіти. Вона повідомляє певну інформацію стосовно його фінансових можливостей для обгрунтування свого права на отримання такої допомоги. Обережний орган державного управління міг би, знаючи особистий ідентифікаційний номер, використовуючи засоби автоматизованої обробки даних у режимі реального часу, отримати доступ до бази даних, що містить інформацію про цю особу як платника податків, створеної податковими органами. Швидко може бути перевірено точність поданої заявником інформації стосов-

но його доходів, доступних грошових засобів. Перевірка точності поданої органам влади інформації, що є можливим завдяки використанню єдиного ідентифікатора для різних адміністративних цілей, також може бути засобом боротьби із шахрайством. Це також одна із причин існування єдиних ідентифікаторів.

Можливий ризик для окремих осіб

Привертає до себе увагу те, що в деяких країнах дискусії навколо проблем, пов'язаних із введенням чи використанням особистих ідентифікаційних номерів, спричинили обговорення питань захисту даних. У деяких країнах такі дебати закінчилися прийняттям законодавчих актів щодо захисту даних. Одним із таких прикладів є французький закон про захист даних, ухвалений 6 січня 1978 року, що став результатом дискусій навколо запропонованого в середині сімдесятих років проекту safari, який передбачав обмін інформацією між базами даних на основі ідентифікаційного номера (numero d'identification au reportoire). Німеччина також може розглядатися як ще одна країна, де загроза поєднання особистих ідентифікаційних номерів з автоматизованою обробкою даних спричинила підготовку законопроекту про захист даних (який у 1978 році набув чинності). Стаття 35 Конституції Португалії, ухваленої в 1989 році, також є цікавою в цьому сенсі, оскільки поєднує в собі заборону обміну інформацією між базами даних (стаття 35.3) із забороною присвоєння мешканцям єдиного ідентифікатора (стаття 35.5), і все це разом, за умов використання автоматизованої обробки даних, визнається таким, що суперечить правам громадянина.

Незалежно від того, чи виправдані вони, чи ні, але ці фактори викликають велику психологічну та емоційну стурбованість щодо введення та використання єдиних ідентифікаторів. Заслуговує на увагу рішення Конституційного Суду Німеччини про те, що введення універсальних особистих ідентифікаційних номерів може створити загрозу для людської гідності, відкриваючи шляхи для контролю за суспільством через зростаючі можливості обміну інформацією між базами даних та збором даних. Питання людської гідності також знаходить своє відображення в побоюванні того, що значення людей буде зведено до «номерів». Якщо продовжити цю думку, то держава не буде ставитися до людей як до таких, що заслуговують поваги. Таке поширене переконання викликано загрозою поступової появи держави на зразок тієї, що описана Оруеллом, побудованої на тотальному контролі, з широкими можливостями постійного стеження за членами суспільства.

Немає ніяких сумнівів, що принаймні універсальні ідентифікаційні номери становлять певну загрозу, доцільність їх введення та використання викликає певні сумніви. Наприклад, ухваленню Закону Австралії «Про приватність» передувала потужна кампанія проти нових можливостей стеження, у зв'язку із пропозицією введення так званої «австралійської картки», що передбачало присвоєння номера кожному власникові такої

картки. Проект було відхилено, а новим законом «Про приватність» було значно обмежено використання податкових номерів. У Канаді Уповноважені з питань приватності один за одним висловлювали стурбованість щодо все більшого поширення загального використання номерів соціального забезпечення. Наприклад, у своєму щорічному звіті за 1985-86 роки Уповноважений з питань приватності заявив, що «небажане поєднання інформації шляхом використання номера соціального забезпечення і надалі більш вірогідне, ніж за допомогою будь-яких інших часток персональної інформації». Уповноважений з питань приватності висловив занепокоєння у зв'язку з тим, що номер соціального страхування (SIN), введений у середині шістдесятих років, швидко вийшов за межі соціального страхування і став найбільш вживаним особистим ідентифікаційним номером у Канаді і зараз є ключовим елементом для створення адміністративних баз даних, що містять у собі персональну інформацію для різних цілей у сфері управління. Знову ж таки в Канаді звіт Постійної комісії з питань правосуддя та заступника міністра юстиції за 1987 рік («Огляд законодавства щодо доступу до інформації та приватності») містить суворі рекомендації щодо використання канадського номера соціального страхування. У звіті зауважено, що номер «настільки важливий, особливий, він наявно демонструє потребу у захисті даних, що очевидною стає необхідність певного контролю за його використанням». У своїй відповіді парламентському комітетові федеральний уряд зазначив, що буде діяти таким чином, щоб запобігти перетворенню SIN на універсальний ідентифікаційний номер. У червні 1988 року федеральний уряд обмежив застосування SIN. Будь-яке нове використання SIN структурами федерального уряду після цієї дати можливе лише з дозволу парламенту. У червні 1989 року федеральний уряд почав вимагати від федеральних органів виконавчої влади повідомляти осіб про мету використання їхнього номера соціального страхування (SIN) та про те, чи можуть вони втратити певні права, доходи, пільги або чи можуть на них бути накладені якісь покарання у випадку відмови від надання номера. Федеральний уряд працює також з органами влади на рівні провінцій для визначення того, чи можна обмежити використання SIN також у межах їхніх повноважень.

У Сполученому Королівстві продовжують виникати все нові пропозиції стосовно використання особистих ідентифікаційних номерів як у державному, так і в приватному секторі, наприклад, у зв'язку з новими місцевими податками, щодо виконання суспільних зобов'язань або застосування кредитними установами. Реєстратор захисту даних прокоментував ці та інші пропозиції і висловив побоювання з приводу неконтрольованого використання особистих ідентифікаційних номерів.

Таким чином, питання особистих ідентифікаційних номерів є знову актуальним. Закон «Про захист даних у Нідерландах», прийнятий у грудні 1988 року, виник на тлі дискусій про особисті ідентифікаційні номери. Уряд Швеції звернувся до Комісії з питань захисту даних та відкритості з

проханням вивчити загрозу для приватності, обумовлену використанням особистих ідентифікаційних номерів.

Не викликає сумнівів, що особисті ідентифікаційні номери разом з автоматизованою обробкою даних є засобом посилення органів влади. Як було зазначено вище, обмін інформацією між базами даних через використання єдиних ідентифікаторів дозволяє владним структурам збирати персональну інформацію, яку занесено до окремих баз даних. Накопичення інформації таким шляхом виключає суб'єкта цих даних з інформаційного кола. Більше немає потреби у спеціальних адміністративних органах для контактів з людьми, для отримання чи перевірки наданої інформації. Орган влади може проводити перевірку та здійснювати контроль, звернувшись до баз персональних даних інших адміністративних органів. Державний орган може також додавати певну інформацію до своєї бази даних, що отримана із баз даних інших владних структур, створених для різних адміністративних цілей. Єдиний багатоцільовий ідентифікатор для кожного жителя – небезпечна частина процесу адміністративного управління, що може призвести до неймовірного посилення органів влади.

Якщо використання єдиного ідентифікаційного номера не обмежується лише державним сектором, а він також застосовується в приватному секторі, небезпека непомірного зростання влади адміністративних органів стає ще більшою. Оцінка особистих ідентифікаційних номерів з точки зору «влади» зовсім не штучно порушує питання, пов'язане з індивідуальними свободами та контролем, оскільки номер завдає шкоди анонімності громадян, він може бути присвоєний особі на все життя, спрощуючи владним структурам визначення місця знаходження, шляхів пересування особи і т. ін., збір інформації з різних баз персональних даних без її відома, прийняття рішень стосовно цієї особи на підставі отриманої інформації. Усе це є можливим як на груповому, та і на індивідуальному рівнях.

Окрім вищенаведених, існують й інші загрози:

а) те, що особистий ідентифікаційний номер може містити в собі закодовану інформацію, яка відома лише тим посадовим особам, яким її надано, і може бути доступною лише при допомозі машинозчитувальних засобів;

б) те, що особистий ідентифікаційний номер може містити в собі вразливу інформацію, суто особисту за своєю природою (наприклад, деякі люди не захочуть мати такий номер, який показує, що вони розлучені, або що їм за 50, чи за 60, чи що-небудь інше);

в) деякі особисті ідентифікаційні номери можуть змінюватися. Набір їх символів може стати іншим через певні значущі події в житті власника. Наприклад, може змінитися стать власника. За таких обставин необхідно, щоб старий номер був знищений, або принаймні зберігався в таємниці;

г) існує небезпека того, що через особисті ідентифікаційні номери інформація із статистичних баз даних може пов'язуватися із конкретними особами, якщо статистичну інформацію створено на підставі номерів;

д) може чинитися певний тиск на власника особистого ідентифікаційного номера з метою надання номера посадовим особам, що забезпечують певні товари та послуги, навіть якщо це не було передбачено на той час, коли номер присвоювався. Наприклад, у Швеції було зауважено, що повідомлення особистого ідентифікаційного номера часто буває потрібним для отримання кредитів, певних послуг, членства в громадських об'єднаннях і т. ін. Якщо особа відмовлялася повідомляти свій ідентифікаційний номер, то вона мала бути готовою до того, що їй буде відмовлено.

є) із останнього факту можна зробити деякі більш загальні, проте значущі висновки про можливість (у кількох національних звітах це вже відображено як реальність) поступового виходу вузькоспеціалізованих особистих ідентифікаційних номерів за межі визначеної сфери застосування і, в найгіршому випадку, перехід до їх загального використання. Відсутність обмежень у часі, коли єдині чи вузькоспеціалізовані ідентифікатори мають використовуватися таким чином, як це було передбачено при їх запровадженні, або надто невизначені обмеження щодо їх обумовленого використання та органів, що можуть їх застосовувати, створюють таку ситуацію.

ГЛАВА 3

Аналіз правових засад введення та використання особистих ідентифікаційних номерів

МІЖНАРОДНІ МЕХАНІЗМИ ПРАВОВОГО ЗАХИСТУ

У міжнародно-правових документах немає ніяких згадок про особисті ідентифікаційні номери. Ні Європейська Конвенція про права людини, ні Конвенція про захист даних не звертаються до них. Незважаючи на це, обидві міжнародні угоди стосуються використання особистих ідентифікаційних номерів.

Наприклад, застосування особистих ідентифікаційних номерів державними органами певним чином і з певною метою може спричинити певні проблеми в контексті статті 8 Європейської Конвенції про права людини (право на недоторканність приватного та сімейного життя, житла й кореспонденції). Європейський Суд та Європейська Комісія з прав людини розглядають Конвенцію як діючий документ, що розвивається таким чином, аби вирішувати нові проблеми. Захист даних вважається обома органами як право, що підпадає під дію статті 8 Конвенції. Комісією розглянуто принаймні три справи, що стосувалися проблем використання особистих ідентифікаційних номерів державними органами:

Ліндквіст проти Швеції (№10879/84);

Лундвалл проти Швеції (№10473/83);

Козлер проти Швеції (№11762/85).

Незважаючи на те, що ці справи було відхилено Комісією як такі, що не порушують статтю 8, важливим є сам факт того, що за певних обста-

вин особисті ідентифікаційні номери можуть бути причиною порушення статті 8.

Що стосується Конвенції про захист даних, то не викликає сумнівів, що основні принципи, встановлені нею, діють як засоби контролю за можливим використанням особистих ідентифікаційних номерів. Такий підхід базується та тому, що особисті ідентифікаційні номери тісно пов'язані з обробкою персональних даних. Як уже було зазначено, вони забезпечують доступ до баз даних. Навіть звичайний незначний серійний номер може відкрити базу персональних даних з вразливою інформацією. Виходячи з цього, треба мати обережність, оскільки особисті ідентифікаційні номери задумано як:

- частки особистої інформації, що пов'язані з базами персональних даних;
- ключовий елемент всієї сфери обробки даних.

Застосовуючи положення Конвенції про захист даних до особистих ідентифікаційних номерів, можна дійти наступних висновків:

- особисті ідентифікаційні номери підпадають під визначення персональних даних, що міститься в статті 2 п. а Конвенції;
- користувачі інформацією мають довідуватися про особистий ідентифікаційний номер від самої особи чесним та законним шляхом у відповідності до вимог статті 5 п. а Конвенції. Це може означати наявність положень про те, що уповноважений орган має право звернутися до власника особистого ідентифікаційного номера з проханням про його надання. За відсутності подібних норм особа є вільною від відповідних зобов'язань і збір такої інформації можливий лише після того, як на те отримано її згоду;
- особисті ідентифікаційні номери не можуть бути використані іншим шляхом чи для інших цілей, ніж це було заздалегідь обумовлено (стаття 5 п. b). Наприклад, є сумніви, чи був б дотриманий цей принцип, якби вузькоспеціалізований особистий ідентифікаційний номер, використання якого було чітко визначено правовим актом, застосовувався для збору та поєднання інформації, або в цілому ряді інших випадків;
- особистий ідентифікаційний номер має бути складено таким чином, щоб він не містив у собі занадто багато інформації особистого характеру, це має відповідати цілям його використання (стаття 5 п.с);
- особисті ідентифікаційні номери мають бути точними і відображати всі зміни обставин, у яких опинився власник (стаття 5 п. d);
- особисті ідентифікаційні номери не повинні показувати категорії вразливої інформації, викладених у статті 6 Конвенції;
- особисті ідентифікаційні номери повинні зберігатися в таємниці, щоб уникнути несанкціонованого доступу чи передачі третій стороні (стаття 7 Конвенції);

- власникові особистого ідентифікаційного номера повинно бути забезпечено право доступу, виправлення та знищення даних, закодованих у числовому наборі ідентифікаційного номера, а також до бази персональних даних, що пов'язана з особистим ідентифікаційним номером (стаття 8 Конвенції).

Щоб завершити цей розділ стосовно міжнародних гарантій, треба звернутися до Принципу №5 Рекомендації №R(86)1 Комітету міністрів Ради Європи стосовно захисту персональних даних, що використовуються з метою соціального забезпечення. Розробники Рекомендації свідомо зробили попередження урядам щодо загрози, яка супроводжує введення або використання єдиного номера соціального забезпечення. Принцип №5 цієї Рекомендації передбачає, що введення та використання такого номера має супроводжуватися адекватними засобами захисту. При підготовці цих норм було визнано, що ідентифікатори викликають певну настороженість. У пояснювальному меморандумі до Рекомендації додатково звертається увага на те, що незважаючи на попередні задуми про використання номера в сфері соціального забезпечення, він швидко може перетворитися на універсальний номер. Розробники мали відчуття, що такі універсальні ідентифікатори не повинні вводитися утаємничено. Також цікаво зауважити, що розробники Рекомендації підштовхують уряди до запровадження правових гарантій захисту інформації, що несе в собі номери соціального забезпечення або подібні засоби ідентифікації. Наприклад, така інформація повинна бути зручною для читання і не надто пов'язаною із метою її використання.

Механізми правового захисту, встановлені національним законодавством

Те, що введення та використання особистих ідентифікаційних номерів пов'язано із питанням захисту даних підтверджується зокрема посиланням на них, що містяться в певних законах про захист даних, наприклад, у французькому та норвезькому законодавстві є спеціальні норми, що стосуються ідентифікаторів. Розділ 18 французького закону від 6 січня 1978 року фактично передбачає, що використання національного ідентифікаційного номера для обробки персональних даних може здійснюватися лише з дозволу Conseil d'Etat, за наявності відповідних висновків Національного комітету з обробки даних і громадянських свобод (CNIL). Починаючи з 1978 року, CNIL зробив лише близько п'ятнадцяти позитивних висновків стосовно використання номера. CNIL напрацював широке прецедентне право щодо інтерпретації розділу 18 закону і намагався, крім усього іншого, обмежити тлумачення слова «використання». Наприклад, CNIL дійшов висновку, що просте звернення до національного реєстру, навіть коли номер не встановлено (наприклад, звірення даних), підпадає під дію норм, викладених у розділі 18, а тому такі дії можливі лише з дозволу Conseil d'Etat. У Данії законодавством про захист даних, що регламентує використання приватних реєстрів, передбачено, що особисті ідентифікаційні номери можуть зберігатися приватними органами, якщо це

безпосередньо передбачено законом, або якщо сама особа дала свою згоду, і за умови, що така інформація необхідна для задоволення законних потреб.

Зв‘язок між питанням захисту даних та особистими ідентифікаційними номерами існує навіть за умов відсутності спеціальних посилань на те, що спеціальні органи повинні втручатися у справи, коли особисті ідентифікаційні номери спричинюють виникнення проблем, що стосуються захисту даних. Наприклад, у таких країнах як Австрія, Ісландія і Люксембург посадові особи, відповідальні за питання захисту даних, висловили свою готовність надати поліції можливості для використання особистих ідентифікаційних номерів. Відсутність у Швеції положень, що забороняють чи обмежують застосування особистих ідентифікаційних номерів, не створює перешкод для реалізації Управлінням Інформаційного Інспекторату своїх повноважень у випадку, якщо посадові особи проводять звірення інформації баз даних за допомогою особистих ідентифікаційних номерів. Закон Швеції «Про захист даних» передбачає, що для проведення таких дій необхідно попередньо отримати дозвіл Управління Інформаційного Інспекторату, який у свою чергу, відповідно до параграфа 1 розділу 6 закону «Про інформацію», має право обумовити порядок застосування особистих ідентифікаційних номерів при роботі з базами даних або може взагалі заборонити їх використання. Управлінням Інформаційного Інспекторату також вироблено загальні умови застосування особистих ідентифікаційних номерів у базах даних клієнтів. У відповідності до цих правил, коли певне об'єднання доходить висновку про необхідність реєстрації особистих ідентифікаційних номерів своїх членів, конкретна особа має бути готовою до того, що вона втратить своє членство у випадку відмови повідомляти свій номер. Але якщо вимога повідомити свій особистий ідентифікаційний номер визнається необгрунтованою, то Управління Інформаційного Інспекторату має право скасувати таку реєстрацію. Це питання також може бути направлено до Швецького Національного Управління з питань споживання (National Swedish Board for Consumer Policies). Як було вже зазначено стосовно Канади та Сполученого Королівства, уповноважені посадові особи з питань захисту даних мають намір провести політичні дискусії навколо проблеми введення та використання особистих ідентифікаційних номерів.

Навіть у тих країнах, де немає законодавства щодо захисту даних, також є можливим створення органу, наділеного повноваженнями здійснювати нагляд та розробляти загальні правила щодо використання особистих ідентифікаційних номерів. Наприклад, у Бельгії є дорадчий та консультативний комітет з питань втручання у приватне життя, який висловив готовність регулювати питання особистих ідентифікаційних номерів, хоча раніше вже згадувалося, що втручання цього органу не допомогло

запобігти виходу використання номерів за межі попередньо визначених цілей.

Окрім законодавства щодо захисту даних, нормативні акти, на підставі яких в суспільне життя запроваджуються особисті ідентифікаційні номери, можуть також містити в собі певні правові гарантії захисту стосовно їх використання, визначати повноваження осіб та органів щодо їх застосування. Прикладом є країни, що мають законодавство, яке регулює використання реєстрів населення (Данія, Норвегія, Нідерланди), або які ввели вузькоспеціалізовані особисті ідентифікаційні номери (Португалія, Швейцарія). В Іспанії Декретом №196/76 із доповненнями, внесеними Декретом №1245/1985, створено правову базу для регулювання питань, пов'язаних із національним посвідченням особи, що включає в себе особистий ідентифікаційний номер. Стаття 6 передбачає, що «приватне життя має поважатися» при використанні посвідчень державними органами, включаючи встановлення особи, що проводиться міністерством внутрішніх справ, яке відповідає за питання, що стосуються національного посвідчення особи.

ВИСНОВКИ

Висновки та пропозиції, що слід узяти до уваги розробникам політики стосовно захисту даних та відповідальним за захист даних у контексті використання особистих ідентифікаційних номерів.

Як показує проведений аналіз, введення та використання особистих ідентифікаційних номерів не є беззастережним питанням ні в країнах, що вже мають великий досвід їх застосування як універсальних багатоцільових ідентифікаторів чи вузькоспеціалізованих ідентифікаторів, ні в країнах, які відмовилися від введення універсальних ідентифікаційних номерів. Принаймні уважне порівняння ціни (з точки зору проблем захисту даних/приватності) та переваг (з точки зору підвищення ефективності управління й зменшення фінансових витрат за допомогою особистих ідентифікаційних номерів) є необхідною частиною обговорення кожної моделі.

Такий аналіз ціни/переваг міг би ґрунтуватися на таких факторах:

1) Там, де система ідентифікаційних номерів уже діє, слід запровадити обмеження на їх використання, щоб забезпечити необхідний баланс між приватністю та ефективністю адміністративного управління. Такі обмеження можуть бути у вигляді засобів правового контролю, що здійснюється шляхом втручання незалежних органів, таких як Уповноважені з захисту даних, або законодавчо обумовлених правил застосування особистих ідентифікаційних номерів державними органами. Законодавство щодо захисту даних може передбачати засоби контролю за використанням особистих ідентифікаційних номерів органами державної влади. Це один із можливих шляхів, який схвалено певними країнами. Однак відсу-

тність окремих положень щодо застосування особистих ідентифікаційних номерів органами влади у законодавстві про захист даних не виключає надання відповідних повноважень органам нагляду, що створені у відповідності до його норм. Це, зрештою, стосується випадків, коли особистий ідентифікаційний номер є ключовим елементом обробки даних. Збирання, зберігання та застосування персональних даних може здійснюватися на основі особистого ідентифікаційного номера. Обмін інформацією баз даних, як уже було показано, значно спрощується за допомогою особистого ідентифікаційного номера. На більш простому рівні особисті ідентифікаційні номери самі складають персональні дані. Одним словом, посадові особи та органи, що займаються питаннями захисту даних, можуть здійснювати функції нагляду та вирішувати питання щодо регулювання у використанні особистих ідентифікаційних номерів.

2) Там, де універсальні чи багатоцільові особисті ідентифікаційні номери вже існують або передбачається їх введення, необхідні правові механізми захисту. По-перше, вони мають бути законодавчо обумовленими. Їх використання слід чітко визначити в межах законодавства. Там, де немає правових підстав для вимог до особи повідомляти свій ідентифікаційний номер, їй має бути роз'яснено право безперешкодно відмовитися від надання такої інформації. Такий принцип міг би бути частиною законодавчої бази для введення та використання особистих ідентифікаційних номерів.

3) Необхідним є створення правової бази для введення та використання універсальних чи багатоцільових особистих ідентифікаційних номерів як гарантії того, що вузькоспеціалізовані особисті ідентифікаційні номери не будуть вживатися поза межами запланованого застосування, що може призвести до їх загального використання в усіх сферах без необхідного публічного обговорення та законодавчої бази, що має створити умови для введення універсальних ідентифікаторів. Маючи це на увазі, слід бути обережними, щоб гарантувати обмеження у застосуванні спеціалізованих особистих ідентифікаційних номерів виключно визначеною сферою. За відсутності відповідних правових норм, особа не повинна бути примушена повідомляти свій особистий ідентифікаційний номер, якщо його використання в цій сфері не передбачено. Знову ж таки, особі має бути забезпечено право безперешкодно відмовитися від повідомлення свого особистого ідентифікаційного номера. Фактично, слід визнавати незаконною будь-яку вимогу надати інформацію про особистий ідентифікаційний номер з боку приватного чи державного органу, якщо це безпосередньо не передбачено законом.

4) Звірення чи обмін інформацією між базами персональних даних з використанням особистих ідентифікаційних номерів заслуговує особливої уваги. Окремий контроль та засоби захисту слід встановити у використанні особистих ідентифікаційних номерів, щоб запобігти наданню дер-

жавним органам надмірних повноважень. Будь-які спроби пов'язати між собою бази даних різних структур державного апарату повинні відбуватися відкрито. Обставини, за яких можливий обмін інформацією між базами даних державних органів, мають бути заздалегідь відомими. Для таких дій повинні бути законні підстави, наприклад, згода органу, що займається питаннями захисту даних.

5) Оскільки особисті ідентифікаційні номери передбачені для ідентифікації осіб, то вони самі по собі є персональними даними. Тому вони повинні відповідати принципам якості даних. Цей фактор згадувався при розгляді повноважень посадових осіб та органів з питань захисту даних стосовно нагляду за використанням особистих ідентифікаційних номерів приватними та державними структурами. Проте здається, що їх введення та використання має забезпечувати права та засоби захисту суб'єкта даних, у відповідності до закону про захист даних. Можна запропонувати, щоб особи, наприклад, мали право змінити склад свого особистого ідентифікаційного номера, якщо він уже не відповідає реальному статусу власника номера. Наприклад, якщо особистий ідентифікаційний номер відображає громадянство чи сімейний стан його власника, то у випадку зміни громадянства, одруження або розлучення цій особі повинно бути гарантовано можливість змінити свій особистий ідентифікаційний номер. Такий номер не може бути складено таким чином, що дозволяє використання чи висвітлює вразливі дані. Особистий ідентифікаційний номер не повинен відображати національність, етнічну належність власника тощо. Більше того, необхідно спробувати складати особисті ідентифікаційні номери таким чином, щоб вони взагалі не містили в собі персональних даних. Наприклад, перевагу можна віддати використанню послідовних або «чистих» номерів. Але якщо все ж таки особистий ідентифікаційний номер містить у собі персональні дані, то необхідно не допустити неадекватного його використання.

6) Особистий ідентифікаційний номер має складатися таким чином, щоб це було зрозуміло його власникові. Він не повинен кодуватися так, щоб власник не міг зрозуміти зміст чисел або літер, які складають номер.

7) Особа має бути проінструктована про те, як користуватися та зберігати у безпеці особистий ідентифікаційний номер, аби уникнути його небажаного застосування третіми особами.

Подаючи ці пропозиції, розробники обмежилися лише розглядом різних типів особистих ідентифікаційних номерів. Проте вони свідомі того, що інші види ідентифікаторів (ім'я, адреса тощо) можуть дозволяти посадовим особам державних органів проводити звірення різних баз персональних даних. Здається, такий спосіб зв'язку між базами даних спричинює ті ж самі проблеми стосовно індивідуальних прав та свобод. Згідно із ви-

щенаведеними принципами щодо гарантій правового захисту та відкритості у випадку обміну інформацією між базами даних, а також із принципами функціонального розподілу, бажаним є використання ідентифікаторів, в основі яких не лежить особистий ідентифікаційний номер.

Розробникам також відомі нові засоби ідентифікації осіб. Наприклад, отримання відбитків пальців із застосуванням генетики, засоби голосової ідентифікації тощо. Розробники дійшли висновку, що стосовно цих нових видів ідентифікаторів їх введення та використання має відбуватися особливо обережно. Зокрема, попередньо варто проводити громадське обговорення, щоб знайти баланс між очікуваними перевагам від їх застосування та приватністю.

В. ПРОТИ ФРАНЦІЇ

У своїй практиці Європейському Суду з прав людини доводилося неодноразово розглядати справи, коли предметом розгляду ставали питання, що пов'язані з ідентифікацією особи. В ряді справ на перший план виходили зокрема новітні технології, їхнє використання у сфері державного управління. Системи ідентифікації осіб, що використовуються державами Європи, можути створювати серйозні перешкоди для громадян вільно чинити своєю долею без втручання у їхнє приватне та сімейне життя. Саме тому створення нових систем ідентифікації та реєстрації осіб має знаходитися під контролем суспільства. Важливо розуміти, що занадто великі повноваження в цій дуже специфічній сфері, передані державним органам, можуть бути використані проти інтересів як окремих людей так і суспільства загалом. Чи не було у Вас такого відчуття, зокрема при спілкуванні з працівниками паспортної служби при оформленні так званої «прописки»? В певних ситуаціях та за певних обставин формальний запис, зроблений в реєстрах, документах, занесеної до бази даних тощо може створити в майбутньому безліч проблем для конкретної людини. Чи мають зберігатися документи, що засвідчують певну ідентифікацію особи, якщо в подальшому її було змінено? Що саме вони мають відображати: реальний стан чи історичний факт? Чи вільна людина чинити своєю долею в питанні зміни своєї ідентичності? В чому полягають функції держави у сфері реєстрації та ідентифікації і де їхня межа? Що саме мають враховувати державні органи при запровадженні нових ідентифікаційних систем для дотримання права людини на приватність? Відповіді на такі питання не є очевидними. Наочною ілюстрацією цьому може бути справа **В. проти Франції**, рішення у якій було прийнято Європейським Судом з прав людини 25 березня 1992 року.

Заявниця пані В. народилася у 1935 році в Алжирі і мала громадянство Франції. Від народження вона була записана в реєстрі актів цивільного стану як особа чоловічої статі під іменем Норбер-Антуан. Проте з дуже раннього віку вона поводилась як особа жіночої статі, четверо її братів і сестер вважали її дівчиною. Як було повідомлено, їй було важко пристосуватися до цілком сегрегаційного ставлення під час навчання у школі.

Вона як чоловік пройшла військову службу в Алжирі, і її поведінка в цей період була помітно гомосексуальною. В 1963 році вона виїхала з Алжиру, оселилася в Парижі і знайшла роботу в кабаре.

У 1967 році вона пройшла курс лікування у зв'язку із приступами нервової депресії. Її лікар помітив гіпотрофію чоловічих статевих органів

і призначив терапію жіночими гормонами, результатом якої став швидкий розвиток молочних залоз і зміна зовнішнього вигляду на жіночий. З того часу заявниця почала носити жіночий одяг. У 1972 році вона пройшла хірургічну операцію в Марокко, яка полягала у видаленні зовнішніх статевих органів і утворенні вагінальної порожнини.

На цей час пані В. живе з чоловіком, якого зустріла незадовго до операції і якому вона одразу ж повідомила про своє становище. Вона більше не працює на сцені і, як заявила сама, не може знайти роботу з причин ворожого ставлення до себе.

Позовна заява пані В. про зміну запису щодо її статі в реєстрі актів цивільного стану з чоловічої на жіночу під іменем Ліна-Антуанетта, щоб мати можливість взяти шлюб, була відхилена Трибуналом великої інстанції Лібурга. Апеляційний суд Бордо, а згодом і Касаційний суд, відхилили її скаргу. Останній постановив, що нижчі суди виправдано відмовляли у наданні засобів судового захисту у подібних випадках, коли докази не підтверджують, що зміна статі, про яку заявлено, є «результатом факторів, що існували до операції, і викликана потребами лікування», а навпаки, – особа просто бажала провести таку зміну.

Проведення гормонального лікування чи хірургічної операції з метою надання транссексуалам зовнішніх ознак статі, до визнання якої за собою вони прагнуть, не вимагає ніяких юридичних формальностей або дозволу.

Події, що відбуваються в житті окремих осіб і впливають на їх цивільний стан, є підставою для внесення у свідоцтво про народження примітки або запису: визнання незаконнонародженої дитини, усиновлення, шлюб, розлучення, смерть тощо.

Повна копія свідоцтва про народження може видаватися лише самим особам, їх родичам по прямій висхідній і нисхідній лінії, чоловікові, дружині або законному опікунові. Проте виписку може отримати будь-яка особа. Для певних формальних цілей державні установи мають право отримувати свідоцтво про цивільний стан, у якому не вказується стать. З метою виправлення помилок та заповнення прогалин було прийнято законодавче положення про те, що «за наявності законного інтересу», будь-яка особа може звернутися з проханням, щоб у її свідоцтві про народження були змінені імена. В противному випадку особа має використовувати імена, вказані у свідоцтві.

Згідно з рішенням Касаційного суду, що було прийнято після розгляду заяви про зміну запису про цивільний стан у свідоцтві про народження, не повинні враховуватися статеві зміни, що виникли після гормонального лікування й хірургічної операції, на проведення яких зацікавлена особа добровільно погодилася, але суди можуть брати до уваги недобровільно набуті морфологічні зміни після лікування, проведеного у концентраційних таборах під час Другої світової війни.

При розгляді однієї справи суд мав прийняти рішення про становище транссексуала, який перебував у шлюбі і був батьком дитини. Хоча Апеляційний суд Німа визнав, що генетично ця особа все ще залишалася чоловіком, 2 липня 1984 року цей суд видав наказ про виправлення запису в його свідоцтві про народження і про зміну імен. За касаційною скаргою прокуратури Касаційний суд скасував це рішення на тій підставі, що встановлені ним факти не підтвердили наявність зміни статі, викликаної фактором, незалежним від волі зацікавленої особи. Зазначалося, що: «транссексуалізм, навіть якщо він підтверджений медично, не може вважатися справжньою зміною статі, оскільки транссексуал, хоча і втратив певні характеристики своєї початкової статі, проте не набув ознак протилежної статі…»

Згідно з загальним правилом, стать не вказується в адміністративних документах, що видаються фізичним особам, таких як звичайні державні посвідчення особи, стандартні паспорти, посвідчення водія, картки виборця, посвідчення про громадянство тощо. Однак у нових машинозчитуваних ідентифікаційних картках визначається стать, щоб машина змогла ідентифікувати особу і врахувати існування неоднозначних імен. Це також стосується паспортів Європейського Співтовариства, які поступово замінюють національні паспорти.

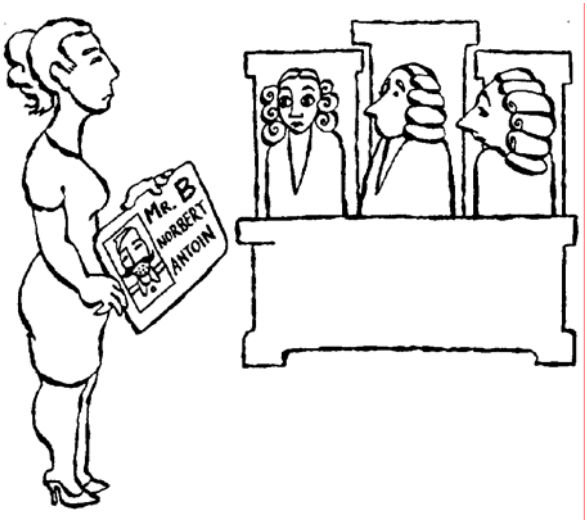
Національний інститут статистики й економічних досліджень INSEE надає кожній людині номер. Перша цифра номера означає стать (1 – чоловіча, 2 – жіноча). Номер заноситься до національного ідентифікаційного реєстру фізичних осіб; органи соціального забезпечення використовують його разом із додатковими цифрами для кожної застрахованої особи. Дозвіл на використання цих номерів дає Державна рада своїм декретом, який видається після консультацій з Національним комітетом з обробки даних і громадянських свобод (CNIL). Реєстр не може використовуватися для стеження за людьми.

У своєму висновку, зробленому в червні 1981 року CNIL дав загальне визначення принципів, що він мав намір їх дотримуватися, здійснюючи нагляд за користуванням реєстром і занесеними до нього реєстраційними номерами. **Було рекомендовано не використовувати номери або припинити їх використання у багатьох випадках, які, окрім іншого, стосуються сфери оподаткування і державної освіти.** Проте було схвалено їх використання для перевірки особи людей у зв'язку з комп'ютеризацією досьє злочинців і центральної бази даних про чеки Банку Франції. Декретом від 11 квітня 1985 року установам соціального забезпечення було також дозволено користуватися реєстраційним номером. CNIL також дозволив використовувати номер для обміну інформацією з органами соціального забезпечення при розробці правил оплати праці.

Не існує жодних законодавчих положень, якими було б передбачено обов'язкове використання банківськими та поштовими установами на чеках звернення «мадам», «мадемуазель» чи «месьє», але на практиці їх пе-

реважно вказують. Однак кожен може звернутися з вимогою, щоб використовували лише його прізвище та ім'я.

Заявниця стверджувала: через те, що французькі власті не дали дозволу виправити запис про її стать у реєстрі актів цивільного стану й офіційних документах, що посвідчують особу, вони примусили її відкрити інформацію суто особистого характеру третім особам; вона також стверджувала, що зіткнулася зі значними труднощами у своєму професійному житті.



Судом були взяті до уваги дві попередні справи: **«Ріс проти Сполученого Королівства»** і **«Коссі проти Сполученого Королівства»**, у яких було відхилено вимоги транссексуалів про виправлення запису про цивільний стан, зважаючи на неоднаковий підхід до вирішення цього питання у договірних державах.

У своєму рішенні у справі **Коссі** Суд зазначив, що з часу ухвалення рішення у справі **Ріса**, як йому було повідомлено, «суттєвого наукового прогресу не відбулося»; «зокрема, хірургічна операція зі зміни статі й далі не приводить до набуття всіх біологічних характеристик протилежної статі».

За словами заявниці, наука, очевидно, внесла два нових елементи до дискусії про невідповідність між зовнішнім виглядом (змінена соматична стать і сформовані гонади) і реальністю (незмінна стать за хромосомним набором, але протилежна стать з психосоціальної точки зору) в питанні про стать транссексуалів. По-перше, хромосомний критерій не безпомилковий (випадки існування осіб з тестикулами в черевній порожнині, так звана тестикулярна фемінізація, або з XY хромосомним набором, незважаючи на жіночу зовнішність); по-друге, сучасні дослідження пока-

зують, що введення деяких речовин на певному етапі вагітності або протягом перших кількох днів життя зумовлюють транссексуальну поведінку і що транссексуалізм може стати результатом хромосомної аномалії. Тому цьому явищу можна дати й фізичне, а не тільки психологічне пояснення, і це означатиме, що не існує підстав для того, щоб відмовлятися враховувати його з юридичної точки зору.

Суд зауважив, що залишається деяка непевність у питанні про справжню природу транссексуалізму і що законність хірургічного втручання в таких випадках інколи залишається під питанням. Крім того, внаслідок цього виникають надзвичайно складні юридичні ситуації: анатомічні, біологічні, психологічні й моральні проблеми у зв'язку з транссексуалізмом і визначенням цього поняття; надання згоди та інші вимоги, які повинні бути задоволені перед проведенням будь-якої операції; умови, за яких можна давати дозвіл на зміну статевої належності (обгрунтованість, наукові припущення та юридичні наслідки проведення хірургічної операції, спроможність жити з новою статевою належністю); міжнародні аспекти (місце проведення операції); ретроспективні чи інші юридичні наслідки зміни статі (виправлення документів про цивільний стан); можливість обрати інше ім'я; конфіденційність документів і даних, де згадується зміна статі; наслідки сімейного характеру (право на вступ у шлюб, доля існуючого шлюбу, встановлення батьківства) тощо. Між державами – членами Ради Європи ще не існує достатньо широкої згоди щодо цих різних моментів, щоб переконати Суд дійти висновків, протилежних тим, які зроблені в рішеннях у справах **Ріса** і **Коссі**.

Заявниця стверджувала, що долю транссексуалів у Франції можна вважати набагато тяжчою, ніж в Англії, з огляду на ряд моментів, і Комісія погодилася з цією думкою. Однак, на думку уряду, стосовно Франції Суд не може відступати від вирішення проблеми, застосованого в рішеннях у справах **Ріса** і **Коссі**. Безсумнівно, у повсякденному житті заявниця могла стикатися з низкою складних ситуацій, але вони не були настільки вагомими, щоб порушувати статтю 8. Французька влада ніколи не відмовляла транссексуалам у праві жити так, як вони бажають. Свідченням цього є історія самої заявниці, оскільки пані В. з успіхом видавала себе за жінку, незважаючи на те, що була чоловіком за цивільним станом. Крім того, транссексуал, який не хоче, щоб треті сторони знали його біологічну стать, перебуває у стані, подібному до стану особи, яка хоче приховати іншу інформацію особистого характеру (вік, прибуток, адресу тощо).

Насамперед Суд дійшов висновку, що між Францією й Англією існують помітні відмінності у праві й практиці стосовно цивільного стану, зміни імен, користування документами, що посвідчують особу тощо. Нижче ним буде досліджено можливі наслідки цих відмінностей для даного випадку з точки зору Конвенції.

Щодо англійської системи реєстрації актів цивільного стану, то Суд встановив, що мета ведення реєстрів полягає не у визначенні існуючої

належності особи, а у фіксуванні історичного факту, і їх публічний характер перетворив би захист приватного життя на ілюзію, якщо можна було б надалі вносити до них виправлення або доповнення такого роду. У Франції справа має інший вигляд. Заплановано, що свідоцтва про народження повинні оновлюватися протягом життя відповідної особи, тому у судовому рішенні цілком можливо давати розпорядження про зміну запису щодо початкової статі. Більш того, єдиними особами, які мають прямий доступ до них, є державні посадові особи й особи, які отримали дозвіл від прокурора Республіки; їх публічний характер забезпечується видачею повних копій або виписок. Тому Франція може задовольнити вимогу заявниці без внесення змін до законодавства. Для цього достатньо змінити прецедентне право Касаційного суду...

Суд зазначив, що оскільки судове рішення ухвалено, ніщо не може стати на заваді внесенню до свідоцтва про народження пані В. у тій чи іншій формі запису, метою якого, точно кажучи, є не виправлення фактичної початкової помилки, а оновлення документа так, щоб він відповідав нинішньому стану заявниці. В результаті операції пані В. безповоротно втратила зовнішні ознаки своєї початкової статі. Суд вважає, що за даних обставин яскраво виражена рішучість заявниці є фактором, достатньо суттєвим для того, щоб врахувати його поряд з іншими факторами у зв'язку зі статтею 8.

Заявниця підкреслила, що законом забороняється будь-якому громадянинові мати прізвище або ім'я, відмінні від тих, що записані у його свідоцтві про народження. Тому з точки зору закону її ім'я – Норбер – вказувалося в усіх документах, що посвідчують особу (ідентифікаційна картка, паспорт, виборча картка тощо), чекових книжках і офіційних повідомленнях (телефонні рахунки, податкові повідомлення тощо). На відміну від цього, у Сполученому Королівстві можливість змінити своє ім'я не залежала б лише від її бажання; стаття 57 Цивільного кодексу ставить у залежність цю можливість від судового дозволу і доведенню «законного інтересу», яким може бути обгрунтовано внесення змін.

З іншого боку, уряд стверджував, що з даного питання існує багате прецедентне право, яке може бути використане і яке було підтримане органами прокуратури. Згідно з ним необхідно просто обрати «нейтральне» ім'я, таке як Клод, Домінік або Каміль. Однак заявниця звернулася з проханням взяти собі ім'я, що дається тільки жінкам. Багато людей часто користуються неофіційно взятим іменем (prenom d'usage), що відрізняється від того, яке записане у їх свідоцтві про народження. Однак уряд визнає, що така практика не має юридичної сили.

Судові рішення, представлені Судові урядом, справді показують, що невизнання зміни статі не обов'язково стоїть на заваді отримання тією чи іншою особою нового імені, яке б краще відповідало її фізичному зовнішньому вигляду. Однак прецедентне право у цій частині ще не було усталеним тоді, коли суди Лібурна і Бордо ухвалили свої рішення. Спра-

вді, воно, здається, не є усталеним і нині, оскільки Касаційний суд, очевидно, так і не підтвердив його. Більше того, ті двері, які воно відчиняє, є занадто вузькими, оскільки обрати можна лише кілька нейтральних імен.

Підсумовуючи, Суд вважає, що відмова надати заявниці дозвіл змінити ім'я, за яким вона звернулася, також є вагомим фактором з точки зору статті 8.

Заявниця наголосила, що стать вказується у все більшій кількості офіційних документів: випсках зі свідоцтв про народження, комп'ютеризованих ідентифікаційних картках, паспортах Європейського Співтовариства тощо. Як наслідок, транссексуали не можуть перетинати кордони, проходити перевірку особи або займатися багатьма повсякденними справами, де необхідно підтверджувати свою особу, без того, щоб не розкривати невідповідність між своєю юридично зареєстрованою статтю та статтю, що відповідає їх зовнішньому вигляду.

За словами заявниці, стать також вказується на всіх документах, де використовується ідентифікаційний номер, наданий INSEE кожній людині. Цей номер використовується в системі ділових відносин між установами соціального забезпечення, роботодавцями й страховими установами; тому він вказується в облікових відомостях про зроблені внески і квитанціях. Як наслідок, транссексуал не має змоги приховати своє становище від потенційного роботодавця й його адміністративного персоналу; те саме стосується багатьох випадків, що трапляються у повсякденному житті, коли необхідно підтвердити доходи і їх розмір (оренда, відкриття рахунку в банку, звернення за наданням кредиту тощо). Це призводить до труднощів на шляху до соціальної і професійної інтеграції транссексуалів. Як стверджується, пані В. сама стала жертвою цього. Наданий INSEE номер також використовується Банком Франції для ведення обліку вкрадених і незабезпечених чеків.

І, нарешті, заявниця стикається з економічними проблемами у повсякденному житті, оскільки в рахунках і чеках вказується її початкова стать, а також прізвище та ім'я. Європейська Комісія з прав людини по суті погодилася з твердженнями заявниці. На її думку, внаслідок частої необхідності розкривати інформацію про своє приватне життя третім сторонам, заявниця зазнавала надто серйозних страждань, які не можна виправдати на підставі поваги до прав інших людей.

У відповідь уряд заявив, що у свідоцтвах про цивільний стан і французьке громадянство, посвідченнях водія, виборчих картках і національних ідентифікаційних картках традиційного зразка стать не вказується. Що ж стосується паспорта Європейського Співтовариства, то його визначають норми, вироблені в Брюсселі, тому не може бути предметом вимог до Франції. Номер INSEE було введено після Другої світової війни для демографічної статистики, і він використовується надалі для визначення осіб, які мають отримувати соціальну допомогу від Франції. Він не вказується на ідентифікаційних картках, паспортах або інших адміністративних документах. У будь-

якому разі, державні органи, яким він повідомляється, зобов'язані тримати його в таємниці. Щодо роботодавців, то їм необхідно його знати, щоб виплачувати певний відсоток від прибутків своїх працівників до фонду соціального забезпечення. Також, на думку уряду, не існує причин, які не давали б можливості звернутися до банків з проханням видруковувати на чеках прізвище й імена особи, яка виписує чек, без скороченого звернення «M», «Mme» або «Mlle», Банки не проводять перевірку того, чи вказані імена збігаються з іменами, занесеними до реєстру актів цивільного стану. Так само в рахунках-фактурах, як правило, не вказується стать чи ім'я клієнта, а лише прізвище. Тому у розпорядженні транссексуалів є засоби, що дають можливість зберігати недоторканність свого приватного життя.

Суд визнав наведені урядом аргументи непереконливими і він визначив, як і Комісія, незручності, на які скаржилась заявниця, достатньо серйозними, щоб їх врахувати для цілей статті 8.

Суд дійшов висновку, що заявниця щоденно знаходилася в ситуації, що в цілому не відповідає належній повазі до її приватного життя. Як наслідок, навіть враховуючи межі свободи розсуду, відведені для держави, не було встановлено справедливого балансу між загальними інтересами та інтересами особи. Тому Суд постановив 15 голосами проти 6, що мало місце порушення статті 8.

За матеріалами рішення Європейського Суду з прав людини підготував Роман Романов

Також були використані видання:

Гілль Дютерт і Якоб ван дер Вельде, Ключові витяги з вибраних рішень Європейського Суду з прав людини і ухвал та звітів Європейської Комісії з прав людини, Директорат прав людини, Рада Європи, 1998

Марк Дженіс, Річард Кей, Ентоні Бредлі, Європейське право у галузі прав людини: джерела і практика застосування, Інститут Конституційної і Законодавчої політики (COLPI), Будапешт, 1997

Роман Романов,Севастопольська правозахиснга група

ГРОМАДЯНИН І ДЕРЖАВА: СУЧАСНІ ПРОБЛЕМИ ІДЕНТИФІКАЦІЇ ОСОБИ В УКРАЇНІ

Що таке ідентифікаційний номер, знає вже, напевне, кожен в Україні. Відомо, що без нього вам на виплатять зарплату, пенсію, відмовлять у прийомі на роботу, не нададуть соціальні субсидії, не візьмуть речі на реалізацію в комісійному магазині… Набір цифр у певній послідовності, що визначається уповноваженим на те органом державної влади, став необхідною умовою для доступу громадян України до широкої сфери соціальних послуг, а фактично – для фізичного існування.

Йдеться про запровадження нової для нас системи персональної ідентифікації, що побудована не на імені та прізвищі, як це було донедавна, а на числовому коді. Але що ж таке насправді особистий ідентифікаційний номер? Чому його введено і які недоліки та переваги від нього слід очікувати нам, громадянам України?

Номер побудовано не як випадковий набір цифр. Знаючи порядок його формування, деяку інформацію про особу, якій він належить, можна довідатись лише поглянувши на нього. Так, перші п’ять цифр означають дату народження людини. Відлік ведеться починаючи від 1 січня 1900 року. Таким чином число 00001 означає, що людина народилась 1 січня 1900 року. Наступні чотири цифри – порядковий номер людини серед тих, хто народився в один день. Дев’ятий знак означає статеву приналежність. Парне число – чоловічу, непарне – жіночу. Як тут не зауважити, що певні проблеми будуть відчувати, наприклад, особи, що змінили свою стать (див. наведену вище справу **В. проти Франції**). Нарешті остання цифра ідентифікаційного номера – контрольне число. Порядок його призначення визначається податковою адміністрацією. З метою захисту від підробок принцип присвоєння цього числа не розголошується.

У тому варіанті, що зараз запроваджується в Україні, сам номер є лише видимою частиною єдиної державної ідентифікаційної системи і ключовим елементом доступу до великого обсягу інформації персонального характеру. Запровадження такої системи є в інтересах держави. Перш за все, значно збільшуються можливості контрольних механізмів державних органів. Спочатку особистий ідентифікаційний номер запроваджено у сфері оподаткування. Сам процес присвоєння громадянам іде-

нтифікаційних номерів покладено на податкові адміністрації. Безперечно, що ефективна робота фіскальних органів держави відповідає інтересам суспільства, адже за рахунок зібраних податків відбувається процес регулювання суспільних відносин з боку держави. Це дає змогу виконувати витратну частину державного бюджету, тобто забезпечувати виплату зарплат працівникам бюджетної сфери, пенсій пенсіонерам та інвалідам, субсидій малозабезпеченим, утримувати державний апарат тощо.

Проте дуже важливо дотримуватися певного балансу в цих відносинах, щоб виконання своїх функцій державними органами не ставало причиною порушень прав та інтересів громадян. Тому наданню органам держаної влади нових контрольних механізмів має передувати широка дискусія – громадське обговорення, а в разі ухвалення остаточного рішення про їхнє запровадження – мають бути передбачені можливості для належного захисту прав усіх суб'єктів цих правовідносин, у першу чергу, особистих прав громадян. На жаль, нічого подібного в Україні не відбулося. Всі рішення були ініційовані державою і одразу ж отримали своє втілення у вигляді нормативно-правових актів.

На сьогоднішній день їх уже ухвалено чимало. Але деякі з них дійсно заслуговують, на мій погляд, не лише згадування, але й певного аналізу.

Базовим документом можна вважати Закон України «Про Державний реєстр фізичних осіб- платників податків та інших обов'язкових платежів» від 22 грудня 1994 року. Проте потім, після масових протестів значної частини населення України, 16 липня 1999 року було ухвалено Закон України «Про внесення змін до Закону України «Про державний реєстр фізичних осіб- платників податків та інших обов'язкових платежів» (текст Закону наведений нижче). Зроблено виняток для віруючих, що за своїми релігійними переконаннями відмовляються отримувати ідентифікаційний код. Від моменту набрання чинності цього нормативного акту ідентифікаційний код фактично із примусового стає добровільним. Але ця надзвичайно важлива подія пройшла майже непомітно. Якщо про запровадження ідентифікаційних кодів написано досить багато статей у відкритій пресі, то зміна статусу номерів отримала мінімальне висвітлення. Більшість населення України не отримала інформації про це і, як на мене, це зроблено свідомо.

Лишається малозрозумілим, яким чином ідентифікаційна і паспортна системи діятимуть за вибірковим принципом. Хто визначатиме наявність релігійних поглядів і які довідки треба буде приносити? Скільки разів на день молитися? Чи буде достатньо написати заяву про відмову отримання коду? Як бути із присвоєнням номерів з моменту народження дитини і чи матимуть право батьки відмовитися від надання дитині номера? На ці питання відповіді у Законі немає.

Постанова Кабінету Міністрів України «Питання паспортизації громадян» від 28 вересня 1996 року №1182 визначає: «вважати за доцільне поєднати виготовлення картки фізичної особи-платника податків та інших обов'язкових платежів – з виготовленням паспорта громадянина України у вигляді паспортної картки і встановити назву цього документа – паспорт-картка».

«Установити, що до паспорта-картки вноситься така інформація: прізвище, ім'я, по батькові, дата і місце народження, ідентифікаційний номер, дата видачі і код органу, що її видав, ідентифікатор особи, дані біометричної ідентифікації та машинозчитувальна інформація, а також особистий підпис власника».

Постановою Кабінету Міністрів України від 2 серпня 1996 року №898 «Про створення Єдиної державної автоматизованої паспортної системи» зокрема передбачено: «започаткувати роботи, пов'язані із створенням Єдиної державної автоматизованої паспортної системи (далі – Система), яка забезпечуватиме видачу громадянам паспортів, що оформлюватимуться за єдиною технологією, та облік громадян за місцем проживання із застосуванням комп'ютерної мережі на єдиних принципах їх ідентифікації (із використанням особистих (ідентифікаційних) номерів громадян, відцифрованого образу осіб і біометричної ідентифікації) і взаємодії з базами даних інших інформаційних систем (як вітчизняних, так і іноземних)» і далі: «…Система входитиме складовою частиною до Державного реєстру населення». Замовником створення Системи визначено Міністерство внутрішніх справ.

Постанова Кабінету Міністрів України від 31 травня 1995 року № 382 «Про затвердження плану заходів щодо впровадження з 1 січня

1996 року Державного реєстру фізичних осіб – платників податків та інших обов'язкових платежів» також визначає, що ідентифікаційна система буде інтегрована з паспортною системою, що значно збільшує її інформаційні потужності, коло користувачів тощо: «Установити, що ідентифікаційні номери Державного реєстру фізичних осіб – платників податків та інших обов'язкових платежів є єдиними з особистими номерами громадян, що використовуватимуться в Єдиній державній автоматизованій паспортній системі та інших інформаційних системах, які за чинним законодавством використовують інформацію про фізичну особу».

Постановою визначено перелік державних установ, що беруть участь у розробці концепції введення ідентифікаційних номерів, отже, відповідно, будуть користувачами створених за їх допомогою баз даних. Такими є Міністерство внутрішніх справ, Служба безпеки України, Міністерство фінансів, Головна державна податкова інспекція, Міністерство статистики, Міністерство оборони, Міністерство юстиції, Міністерство праці, Пенсійний фонд. Також у п.4 Постанови серед інших державних органів згадується і Адміністрація Президента України. Проте в чому саме полягає її роль та якими є повноваження, залишається лише здогадуватися, адже формулювання «для вирішення питань оперативного управління» може включати в себе будь-який зміст. Взагалі, серед нормативних актів, відповідно до яких прийнято Кабінетом Міністрів цю Постанову, названо також Указ Президента України від 30 листопада 1994 року №709/94 «Про інформаційно-аналітичне забезпечення Президента України». Отже, Адміністрація Президента також буде мати доступ до інформаційних ресурсів Системи. Знати про це напевне ми не можемо, тому що вищезгаданий Указ Президента має позначку «не для друку», так само як і пункти 71-77 Указу Президента від 27 січня 1999 року №70/99, де йдеться про внесення змін до Указу №709/94.

З цього можна зробити невтішний висновок про те, що громадянин України навіть не може довідатися про те, хто і яким чином буде використовувати його персональні дані. Такі дії Президента вочевидь є порушенням Конституції України, зокрема ст.57 передбачає, що «закони та інші нормативні акти, що визначають права та обов'язки громадян, мають бути доведені до відома населення у порядку, встановленому законом. Закони та інші нормативні акти, що визначають права та обов'язки громадян, не доведені до відома населення у порядку, встановленому законом, є нечинними.»

Постановою Кабінету Міністрів України від 20 січня 1997 року №40 затверджено Концепцію створення Єдиної державної автоматизованої паспортної системи. Концепція визначає, що Єдина державна автоматизована паспортна система є найважливішою складовою частиною Державного реєстру населення і буде використовуватися для «формування загальної системи обліку громадян… а також організації різноманітної аналітично-довідкової роботи».

Передбачається створення Державного реєстру населення України. Від самого народження дитини заноситимуть до свідоцтва про народження її ідентифікаційний код. Той же самий набір чисел міститиметься в паспорті, що буде отримано після досягнення 16 років. Реєстрація посвідчень про освіту, дипломів та атестатів також відбуватиметься на підставі ідентифікаційного номера. Передбачається використання ідентифікаційного коду в цілому ряді облікових систем. Їх повний перелік навряд чи хтось може навести. Зокрема сьогодні йдеться про систему пенсійного забезпечення. Так звана персоніфікація пенсійних відрахувань провадитиметься на підставі особистого коду. Надання різного роду субсидій також планується проводити на підставі тієї інформації, доступ до якої забезпечує наявність ідентифікаційного коду. Отже, цілком очевидно, що ідентифікаційний код стає ключовим елементом доступу до соціальних послуг. Але, крім можливостей для державного контролю, ця система має бути побудована таким чином, щоб забезпечити невтручання у приватне та сімейне життя особи.

Слід зауважити, що сьогодні важко визначити повне коло користувачів Системи (зокрема неопубліковані Укази Президента в явному вигляді цьому перешкоджають). Так само важко впевнено сказати у яких саме сферах застосовуватиметься інформація Системи. Безперечно, можна говорити про спрощення та полегшення державного управління, проте, скажімо, в разі підробки ідентифікаційного коду шкода може бути заподіяна набагато більша, ніж у разі таких самих дій, якщо йдеться про один лише документ, а не про інтегровану інформаційну систему (більш детально про це див. матеріал, підготовлений Privacy International «Ідентифікаційні картки. Питання, що виникають найчастіше»). Нарешті, які гарантії має особа, що інформацію, зібрану про неї в Системі, не буде використано всупереч її інтересам? Особливо, зважаючи на рівень корупції в державі.

Анахронізмом видається також існування паспортної системи в структурі Міністерства внутрішніх справ України. Це створює можливості для безперешкодного доступу співробітників МВС до персональних даних громадян України, а отже, обумовлює вірогідність широкого спектру зловживань.

Не зрозуміло також процедуру внесення змін до тих даних, що занесені до Системи. Чи може сама особа наполягати і домогтися таких змін та виправлень? Для цього, принаймні, їй треба отримати повний доступ до інформації, що про неї зібрана. Чи буде таке право гарантоване?

Дуже показовим з точки зору врівноваження інтересів держави і суспільства є відсутність до цього часу нормативного акту, який би гарантував дотримання індивідуальних прав громадян, адже в основі нової системи обліку та ідентифікації є обробка інформації особистого характеру. Слід зазначити, що на рівні проекту вже підготовлено Закон України «Про захист персональних даних», проте для мене є очевидним, що його

ухвалення мало би передувати вищенаведеним нормативним актам, що регулюють питання запровадження індивідуальних кодів. Однак насправді органи державної влади України чинять всілякі перешкоди для його прийняття, щоб закон «Про захист персональних даних» набрав чинності лише після завершення робіт щодо створення Державного реєстру населення і Єдиної державної автоматизованої паспортної системи.

Отож, виникає багато запитань, на які бажано було б отримати зрозумілі відповіді до того, як Система стане реальністю. Механізми захисту персональних даних, що є сьогодні, не можуть відповідати вимогам сьогодення. Небезпека створення потужних інтегрованих ідентифікаційних систем в Україні за умов відсутності ефективних та зрозумілих засобів захисту персональних даних, невизначеності повної сфери їх застосування, є надто великою, щоб можна було не помічати потуг держаних органів у запровадженні нових ідентифікаційних та контрольних механізмів.

ДОДАТОК

ЗАКОН УКРАЇНИ

«Про внесення змін до Закону України «Про Державний реєстр фізичних осіб – платників податків та інших обов'язкових платежів»[29]

З метою запровадження альтернативної форми обліку громадян України – платників податків та інших обов'язкових платежів, які через свої релігійні або інші переконання відмовляються від прийняття ідентифікаційного номера фізичної особи – платника податків та інших обов'язкових платежів та офіційно повідомили про це відповідні державні органи, Верховна Рада України **постановляє:**

Внести до Закону України «Про Державний реєстр фізичних осіб – платників податків та інших обов'язкових платежів» (Відомості Верховної Ради України, 1995 р., № 2, ст. 10) такі зміни:

1. Статтю 1 доповнити частиною другою такого змісту:

«Для осіб, які через свої релігійні або інші переконання відмовляються від прийняття ідентифікаційного номера та офіційно повідомляють про це відповідні державні органи, зберігаються раніше встановлені форми обліку платників податків та інших обов'язкових платежів. У паспортах зазначених осіб робиться відмітка про наявність у них права здійснювати будь-які платежі без ідентифікаційного номера».

2.У статті 5:

1) доповнити статтю після частини першої новою частиною такого змісту:

---

[29] Відомості Верховної Ради України, № 41, 1999.

«До Державного реєстру не вноситься інформація про осіб, які через свої релігійні або інші переконання відмовляються від прийняття ідентифікаційного номера та офіційно повідомляють про це відповідні державні органи».

У зв'язку з цим частини другу – сьому вважати відповідно частинами третьою – восьмою;

2) частину п'яту доповнити словами «за винятком осіб, які через свої релігійні або інші переконання відмовилися від прийняття ідентифікаційного номера та офіційно повідомили про це відповідні державні органи».

3. Частину другу статті 7 доповнити словами «за винятком звітних та облікових документів, у яких відсутні ідентифікаційні номери осіб, які через свої релігійні або інші переконання відмовилися від прийняття ідентифікаційного номера та офіційно повідомили про це відповідні державні органи».

4. Абзац перший частини третьої статті 9 після слів «обов'язкових платежів» доповнити словами «крім осіб, які через свої релігійні або інші переконання відмовилися від прийняття ідентифікаційного номера та офіційно повідомили про це відповідні державні органи».

5. Частину другу статті 11 доповнити реченням такого змісту: «Ця норма не застосовується до осіб, які через свої релігійні або інші переконання відмовилися від прийняття ідентифікаційного номера та офіційно повідомили про це відповідні державні органи».

Президент України
Л. КУЧМА

м. Київ, 16 липня 1999 року
№ 1003-XIV

ІДЕНТИФІКАЦІЙНИЙ НОМЕР – КОЖНОМУ?
(ЛИСТ, КОМЕНТАР, ВИСНОВОК)

ДЕРЖАВНА ПОДАТКОВА АДМІНІСТРАЦІЯ УКРАЇНИ

Л И С Т

№ 4376/6/19-0116 від 11.07.2002

О.Радченку
м. Приморськ
Запорізької обл.

Згідно зі статтею 67 Конституції України (254к/96-вр) «кожен зобов'язаний сплачувати податки і збори в порядку і розмірах, встановлених законом».

Усі громадяни щорічно подають до податкових інспекцій за місцем проживання декларації про свій майновий стан та доходи за минулий рік у порядку, встановленому законом.

Функції по контролю за дотриманням податкового законодавства, правильністю обчислення, повнотою і своєчасністю сплати до бюджетів, державних цільових фондів податків та інших обов'язкових платежів покладено на державні податкові органи, а за рахунок податків держава виплачує мільйонам громадян пенсії, житлові субсидії, фінансує заклади охорони здоров'я та освіти, утримує армію, міліцію тощо.

Прийняття змін до Закону України «Про державний реєстр фізичних осіб – платників податків та інших обов'язкових платежів» (320/94-вр) (далі – Закон), згідно з якими для осіб, які через свої релігійні або інші переконання відмовляються від присвоєння ідентифікаційних номерів, вносяться спеціальні відмітки про наявність у них права здійснювати будь-які платежі без ідентифікаційного номера.

На даний час конкретний механізм реалізації ст. 1 Закону України «Про державний реєстр фізичних осіб – платників податків та інших обов'язкових платежів» (320/94-вр) з урахуванням внесених змін ще не визначений на законодавчому рівні.

Аналіз конституційних норм показує, що існування розподілу на тих, хто виконує Закон (320/94-вр) і реєструється в Державному реєстрі і тих, хто відмовляється від цього, означає надання певних привілеїв окремим категоріям громадян в залежності від їх ставлення до релігії, а це суперечить ст. 24 та 35 Конституції України (254к/96-вр), де зазначено, що громадяни не можуть мати жодних привілеїв за ознакою релігійних пере-

конань та ніхто не може бути увільнений від своїх обов'язків перед державою або відмовитися від виконання законів за мотивами релігійних переконань.

Внесення відміток в паспорти фактично суперечить статті 4 Закону України «Про свободу совісті і релігійні організації» (987-12), де сказано, що в офіційних документах ставлення громадянина до релігії не вказується.

Всі записи, які вносяться в паспорт громадянина України, регламентуються положенням «Про паспорт громадянина України», затвердженим постановою Верховної Ради України від 26 червня 1992 року № 2503-XXII (2503-12) (в редакції постанови Верховної Ради України від 2 вересня 1993 року № 3423-XII (3423-12) (далі – Положення), на основі якого Міністерство внутрішніх справ України розробило інструкцію щодо правил та порядку оформлення і видачі паспорта громадянина України, затверджену наказом Міністерства внутрішніх справ України від 17 серпня 1994 року № 316 (z0211-94) та зареєстровану в Міністерстві юстиції України 5 вересня 1994 року за № 211/421 (далі – Інструкція).

Оскільки відмітка про наявність у громадянина, який через свої релігійні або інші переконання відмовляється від прийняття ідентифікаційного номера, права здійснювати будь-які платежі без ідентифікаційного номера, не передбачена цим положенням (3423-12) та інструкцією (z0211-96), потребується внесення змін в ці документи.

Враховуючи таку суперечність, Державна податкова адміністрація України на виконання доручення Кабінету Міністрів України розробила, узгодила з міністерствами і відомствами та подала на розгляд до Верховної Ради України альтернативний чинному закону проект Закону України «Про внесення змін та доповнень до Закону України «Про Державний реєстр фізичних осіб – платників податків та інших обов'язкових платежів» (320/94-вр) (реєстр № 4306 від 19.01.2000), стосовно якого до цього часу не було прийнято ніякого рішення.

Також Державна податкова адміністрація України порушила питання щодо внесення змін до положення та розробки порядку внесення відміток у паспорти фізичних осіб, зауважуючи при цьому, що глава Української православної церкви Московського патріархату блаженнійший Володимир заперечував у 1999 році проти внесення відміток в паспорти віруючих громадян.

Державна податкова адміністрація України наполегливо проводить політику щодо обов'язкового виконання чинного законодавства, особливо у частині використання ідентифікаційних номерів.

Заступник голови ДПА України О.Шитря

«Урядовий кур'єр», № 142, 6 серпня 2002 року

КОМЕНТАР

Лист, підписаний заступником голови Державної податкової адміністрації України паном Шитрею дуже яскраво ілюструє намагання посадових осіб ДПА відмовитися від виконання вимог чинного законодавства.

Законом України «Про внесення змін до Закону України «Про Державний реєстр фізичних осіб – платників податків та інших обов'язкових платежів» від 16 липня 1999 року передбачено, що фізична особа має право на відмову від присвоєння ідентифікаційного номера. Так, Ст.1 Закону України «Про Державний реєстр фізичних осіб – платників податків та інших обов'язкових платежів» доповнено ч.2 такого змісту: «Для осіб, які **через свої релігійні або інші переконання** відмовляються від прийняття ідентифікаційного номера та офіційно повідомляють про це відповідні державні органи, зберігаються раніше встановлені форми обліку платників податків та інших обов'язкових платежів. У паспортах зазначених осіб робиться відмітка про наявність у них права здійснювати будь-які платежі без ідентифікаційного номера».

Можна погодитись з тим, що внесення відміток до паспортів громадян «про наявність права здійснювати будь-які платежі без ідентифікаційного номера» не можна вважати найкращим механізмом реалізації встановленого законом права. Взагалі, зміст першого речення ч.2 Ст.1 Закону дещо суперечить другому. Якщо в першому передбачається, що відмова від отримання ідентифікаційного номера здійснюється шляхом офіційного повідомлення (тобто не встановлюється дозвільний порядок такої відмови), то внесення спеціальних відміток в паспорт громадянина передбачає, що певна службова особа ДПА має повноваження вносити такі відмітки. Не зовсім зрозуміло, в який момент виникає у фізичної особи право на здійснення платежів без присвоєння ідентифікаційного номеру – чи то після офіційного повідомлення ДПА, чи то після внесення відповідної відмітки до паспорту громадянина.

Як випливає із змісту листа заступника голови ДПА, посадові особи податкової адміністрації вважають, що право виникає лише після внесення відмітки. Проте, Закон не встановлює повноважень службових осіб ДПА відмовляти громадянам у випадку офіційного повідомлення про відмову від прийняття ідентифікаційного номеру через свої релігійні або інші переконання. В разі, якби ДПА мала такі повноваження, це би означало право цієї установи на контроль за переконаннями людей, що, здається, божевільною ідеєю. Переконання людей не можна контролювати і не можна перевіряти.

Лист взагалі виходить з презумпції недовіри до громадян, з того, що намагання уникнути отримання номеру є намаганням уникнути оподаткування власних прибутків. Так само, як військові комісаріати вважають, що альтернативна невійськова служба є намаганням ухилитися від призову на військову службу.

Контроль за сплатою податків не є тим же самим, що сплата податків. Сплата податків є конституційним обов'язком кожного, контроль за дотриманням законодавства щодо сплати податків є завданням державних органів. Він має бути побудований таким чином, аби не порушувати права людини. Саме в цьому є ключ до розуміння проблеми.

Органи державної влади України за рахунок податків, що сплачуються громадянами України, мають створити таку систему контролю, в тому числі за сплатою податків, яка з одного боку буде ефективною, з іншого, буде достатньо гнучкою, аби не порушувати права людини. Запровадження в Україні ідентифікаційного номеру з надзвичайно широкою сферою застосування, за умов відсутності адекватних механізмів захисту персональних даних створює реальну загрозу тотального контролю над громадянами з боку держави.

При цьому органи державної влади України відмовляються робити виключення по відношенню до тих людей, що вважають таку систему контролю занадто сильним втручанням в їхнє приватне життя, розцінюють її як загрозу своїй свободі, в тому числі свободі релігійних переконань. Отож, нездатність побудувати ефективну систему контролю, що не порушувала б права та інтереси значної частини суспільства, органи державної влади намагаються обґрунтувати за допомогою вельми сумнівних з правової точки зору аргументів. До того ж, свої сумніви щодо можливого порушення Конституції України ДПА могла розвіяти, звернувшись до Конституційного суду України, однак, про такі дії заступник голови ДПА в своєму листі не повідомляє. Замість цього ДПА розробила власний проект Закону, чекає на його ухвалення Верховною Радою України, а до того часу фактично відмовляється виконувати норми чинного законодавства. Очевидним є намагання ДПА звузити коло осіб, що можуть скористатися своїм правом на відмову від отримання ідентифікаційного номеру лише до віруючих. Проте, Закон передбачає, що таким правом може скористатися особа, незалежно від того, якого характеру переконання заважають особі отримати ідентифікаційний номер (релігійні та інші). Вичерпного переліку таких переконань не встановлено. Отож, посилання заступника голови ДПА на положення Ст.24 та 35 Конституції України щодо надання привілеїв в залежності від ставлення до релігії викликає подив. Так само, як твердження про те, що внесення відмітки в паспорт суперечить Ст.4 Закону України «Про свободу совісті і релігійні організації», адже Закон України «Про внесення змін до Закону України «Про Державний реєстр фізичних осіб – платників податків та інших обов'язкових платежів» не передбачає, що ДПА має вносити в паспорти відмітки про ставлення громадян до релігії.

Тим часом, виникають все нові сфери застосування ідентифікаційних номерів. Так, в деяких готелях Києва (зокрема, готель «Козацький») в нових бланках реєстраційних форм з'явилася графа – ідентифікаційний номер. Поки що при поселенні заповнення цієї графи не вимагається. Мі-

ністерство внутрішніх справ України завершує роботи з запровадження Єдиної державної автоматизованої паспортної системи України (ЄДАПСУ), в основі якої все той же ідентифікаційний номер. Пропозиції Міністерства юстиції щодо заміни позаконституційної системи прописки реєстрацією за місцем проживання також включають в себе збільшення кількості інформації, що фізичні особи надають органам, які здійснюють реєстрацію, включаючи ідентифікаційний код. Таким чином, ідентифікаційний код платника податків стає ключовим елементом державного контролю над громадянами в Україні, далеко виходячи за межі декларованої мети – контролю за сплатою податків.

Роман Романов, Севастопольська правозахисна група

ВИСНОВОК

щодо листа Державної податкової адміністрації України
№ 4376/6/19-0116 від 11.07.2002 року

Згідно з частиною 2 статті 147 та пунктом 2 статті 150 Конституції України тільки Конституційний Суд України вирішує питання про **відповідність законів** та інших правових актів Конституції України **і дає офіційне тлумачення Конституції та законів України.**

Як вбачається з вищезгаданого листа, у даному випадку податкова адміністрація в особі заступника голови ДПА України вдалася до питань тлумачення терміна «привілеї» («пільги») у співвідношенні з терміном «право» та терміном «обов'язки», посилаючись на статті 24, 35 Конституції України і на Закон України «Про внесення змін до Закону України «Про державний реєстр фізичних осіб – платників податків та інших обов'язкових платежів», тобто, фактично вона привласнила собі повноваження Конституційного Суду України.

Згідно зі статтею 19 частиною 2 Конституції Україні органи державної влади та місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України.

При прийнятті нових законів або внесенні змін до чинних законів не допускається звуження змісту та обсягу існуючих прав і свобод (стаття 22, частина 2 Конституції України).

Невиконання службовими особами вимог Закону України «Про внесення змін до Закону України «Про Державний реєстр фізичних осіб – платників податків та інших обов'язкових платежів» може тягнути юридичну відповідальність згідно з чинним законодавством України.

Іван Ткач, адвокат

Руслан Тополевський

ОКРЕМІ АСПЕКТИ ПРАВОТВОРЧОСТІ У СФЕРІ РЕЄСТРАЦІЇ ОСОБИ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Про зміни, які відбулися в свідомості наших громадян протягом останнього десятиріччя, свідчить поява законопроектів, які тією чи іншою мірою стосуються ідентифікації та реєстрації особи. Безумовно, не може не радувати той факт, що законодавці вже дозріли до необхідності врегулювати ці питання на рівні закону. Разом з тим слід також відзначити наявність певних негативних тенденцій, які виявляються в процесі правотворчості в цій сфері. Саме на це вказує відхилення Верховною Радою низки законопроектів щодо реєстрації фізичних осіб.

Загалом нормативне врегулювання цієї проблеми повинне носити системний характер і вирішувати низку взаємопов'язаних питань: ведення реєстрів, ідентифікація особи, реєстрація особи за місцем проживання, захист персональних даних особи тощо. Загалом видається доцільним створити єдиний закон.

Питання ідентифікації особи та захисту персональних даних є ключовим для побудови правової держави та розвитку громадянського суспільства. Порушення балансу між правом особи на захист приватності (і, зокрема, конфіденційності персональних даних) і бажанням держави знати все про всіх (як нас переконують, з благими намірами) може призвести в найгіршому випадку до побудови поліційної недемократичної держави, а в найкращому – до визнання Конституційним Судом України певних статтей цих законів неконституційними або до програшу в Європейському суді з прав людини справ щодо порушення статті 8 Європейської конвенції про захист прав людини та основних свобод.

Як свідчить історія, суттєве обмеження свободи громадян має своїм наслідком зниження динаміки суспільного розвитку, тоді як неналежне регулювання цієї сфери надасть можливість на законних підставах втручатися в таку вразливу сферу буття людини як приватне життя.

Розробка законопроектів, які в той чи інший спосіб мали врегулювати проблему реєстрації постійного місця проживання, внаслідок відміни системи прописки, не обмежилися лише цим. Фактично неодноразово було зроблено спроби, які мали на меті впровадження універсального ідентифікаційного коду, який би застосовувався в усіх документах, що посвідчують особу.

Слід зазначити, що застосування єдиного багатоцільового ідентифікаційного коду створює загрозу конфіденційності інформації про особу

(персональних даних). Це пов'язане перш за все з тим, що розміщення універсального ідентифікаційного коду на всіх документах особи призведе до можливості об'єднувати між собою різні реєстри (бази даних, в яких міститься та чи інша персональна інформація) тоді як з ч.2 ст. 32 Конституції України випливає неприйнятність збирання, зберігання, використання та поширення інформації про особу без її згоди.

Хоча ці технічні переваги підвищують ефективність систем обробки інформації та прийняття управлінських рішень, однак ціна за це – загроза приватності особи – надто висока. Загроза з боку впровадження універсального багатоцільового ідентифікаційного коду полягає перш за все в можливості його використання як інструмента поєднання всіх інших баз даних, в яких міститься інформація про особу.

Окремі законопроекти в цій сфері намагалися подолати цю суперечність, пропонуючи багаторівневі реєстри, розбиваючи їх на низку підсистем, однак все ж найкращим захистом персональних даних було б розділення певних видів персональних даних в різних реєстрах, у відповідності до конкретної мети збирання інформації.

Розробка цих законопроектів потребувала врахування низки факторів:

- законопроект мав передбачати особливості обробки персональних даних, зокрема, забезпечувати конфіденційність персональних даних.
- законопроект мав враховувати міжнародно-правові документи, присвячені обробці персональних даних і роботі з реєстрами
- законопроект не повинен був суперечити Конституції України і враховувати приписи міжнародних договорів, ратифікованих Верховною Радою України та, наскільки це можливо, приписи інших законів.
- законопроект не повинен був порушувати права людини, зокрема, право особи на захист персональних даних.

Разом з тим ці законопроекти мали низку спільних недоліків:

- не передбачена заборона на об'єднання баз персональних даних, що обробляються з різними цілями, без відома особи.
- Низка законопроектів передбачала впровадження єдиного універсального ідентифікаційного коду, який мав полегшити діяльність державних органів за рахунок звуження «зон свободи» особи, за рахунок збору і обробки персональних даних без участі власника персональних даних
- як правило, не розділялися загальні і вразливі персональні дані, які потребують додаткового рівня захисту.
- як правило, не передбачається доступ особи до всього маршруту обробки персональних даних, тоді як це правило повинне мати юридичне закріплення. Винятки з цього положення можливі лише для цілей, передбачених в ст. 32 Конституції України.

- як правило, не передбачається повідомлення особи про мету обробки персональної інформації, що в свою чергу може впливати на реалізацію прав і свобод особою.
- реєстри персональних даних нерідко передбачаються як такі, що містять інформацію про особу не лише для конкретної мети, але й на всяк випадок, що, безумовно, у випадку зі збиранням і обробкою персональних даних неприпустимо.

Особливу увагу привертає процедура захисту персональних даних. Безперечно, організаційно-технічні заходи відіграють важливу роль для забезпечення конфіденційності і таємності персональних даних. Зрозуміло, однак, що вагому увагу слід звернути на людський фактор, як можливу загрозу конфіденційності персональних даних. Оскільки обробкою персональних даних будуть займатися державні органи, слід передбачити можливість порушення конфіденційності персональних даних, інших порушень режиму роботи з персональними даними. Для покращення захисту персональних даних, на нашу думку, слід запровадити таку інституцію як Уповноважений (Омбудсман) з питань захисту персональних даних. В перспективі саме на цю інституцію покладатиметься обов'язок контролю за правомірним веденням інших реєстрів, які стосуються персональних даних. Окремі законопроекти передбачають таку інституцію, другі – покладають цей обов'язок на спеціальний державний орган, треті взагалі вважають, що для захисту прав особи достатньо наявності судів загальної юрисдикції.

Покажемо вади та переваги законопроектів у сфері захисту персональних даних на конкретних прикладах:

Проект Закону України №1089 від 23.05.2002 р. «Про свободу пересування та вільний вибір місця проживання в Україні»

Перш за все зауважимо, що для повноцінного функціонування цей закон потребує також прийняття щонайменше Закону «Про єдиний реєстр фізичних осіб за місцем проживання», Закону «Про захист персональних даних» та Закону «Про реєстрацію осіб», які б врегульовували окремі аспекти, неврегульовані законопроектом №1089.

Визначення в ст. 2 законопроекту місця перебування і місця проживання розходиться з поняттям «місця проживання», яке визначене Цивільним кодексом (2003 р.). В законопроекті також не передбачено особливості реєстрації неповнолітніх осіб, недієздатних та новонароджених. Викликає здивування спроба реєстрації місця перебування особи, що, в свою чергу, фактично створює передумови для контролю за пересуванням особи, що неприйнятно в демократичному суспільстві.

Стаття 6 законопроекту передбачає досить простий спосіб реєстрації особи, передбачаючи в загальному вигляді підставою реєстрації лише заяву

громадянина. Разом з тим, з тексту незрозуміло чи потрібно подавати цю заяву особисто, чи розробники законопроекту передбачали можливість подання такої заяви поштою.

Законопроект передбачає реєстрацію постійного місця проживання органами РАГСу, а тимчасового – органами внутрішніх справ, а також передачу останньої інформації органам РАГСу. Здатність органів РАГСу на сучасному етапі забезпечити конфіденційність персональних даних викликає певне занепокоєння. Зрозуміле бажання авторів законопроекту забезпечити конфіденційність інформації, однак виникає питання, чи приведуть такі дії до досягнення цього результату.

З тексту законопроекту не зовсім зрозуміло, що мається на увазі під зонами обмеженого доступу де обмежується право на свободу пересування (ст.11). Крім того, законопроект не передбачає обмеження права на свободу пересування військовослужбовців строкової служби.

Проект Закону України № 2618 від 10 січня 2003 р. «Про захист персональних даних»

В основі цього законопроекту лежить концепція права власності особи на персональні дані. Навряд чи можна охопити відносини щодо персональних даних лише правом власності. Право на персональні дані слід віднести до немайнових, так само як і інші, передбачені в Книзі другій Цивільного кодексу (від 16 січня 2003 р.). Це витікає, зокрема, з права на особисте життя (приватність), проголошеного статтею 32 Конституції України і статтею 301 нового ЦК України. Конвенція Ради Європи про захист особи в зв'язку з автоматичною обробкою персональних даних (1981) стосується перш за все захисту права на недоторканність особистої сфери. Персональні дані не є майном, законна передача персональних даних у користування, як правило, не передбачає плати за них. Не належить право на персональні дані і до права на інтелектуальну власність. Більше того, виникнення права на персональні дані не відповідає жодній з підстав виникнення права власності на інформацію ч.3 ст. 38 Закону про інформацію. Разом з тим персональні дані як інформація безумовно підпадають під дію закону «Про захист інформації в автоматизованих системах». В свою чергу, створення бази персональних даних призводить до виникнення права інтелектуальної власності на неї (п.3 ч.1 ст.433 ЦК України). Таким чином, цей законопроект повинен відобразити особливий характер права на персональні дані.

Однак, як видається, прийняття законопроекту з трактуванням права на персональні дані як права на власність персональних даних створить колізію між Законом «Про захист персональних даних» і Конституцією України, Цивільним кодексом, іншим законодавством у визначенні статусу персональних даних.

При визначенні кола осіб слід чітко визначити на кого поширюється дія цього закону, не припускаючи невизначеного кола осіб за допомогою слова тощо (ст.1)

Слід позитивно відзначити положення ст.4 законопроекту, яка передбачає, що персональні дані фізичної особи, яка претендує чи займає вибірну посаду (в представницьких органах) або посаду державного службовця першої категорії не відносяться до інформації з обмеженим доступом. Однак, на нашу думку, навряд чи доцільно обмежувати коло таких осіб лише вибірними посадами або державними службовцями першої категоріх. Як свідчить практика Європейського суду з прав людини, обмеження конфіденційності персональних даних особи можливе в тому разі, коли її діяльність набуває публічного характеру, коли вона стає публічною особою. Саме це підкреслює ч.9 ст.30 Закону України «Про інформацію», яка дозволяє поширювати суспільно значиму інформацію без згоди її власника.

Слід зазначити розбіжність між тестом законопроекту (ст. 5), який передбачає можливість обробки даних про фізичну особу без її згоди, крім випадків, визначених цим Законом, і лише в інтересах національної, економічної і громадської безпеки чи з метою захисту прав людини, тоді як ч.2 ст.32 Конституці України забороняє збирання, зберігання, використання і поширення інформації про особисте життя фізичної особи без її згоди крім випадків, визначених законом і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Стаття 23 законопроекту передбачає, що про зміну, доповнення, знищення персональних даних або обмеження до них доступу володільці персональних даних повідомляють органи державної влади та органи місцевого самоврядування, організації, установи і підприємства усіх форми власності, яким ці дані передаються, якщо це необхідно для захисту інтересів власника персональних даних, тоді як суб'єкт (власник) персональних даних про зміну, доповнення і знищення персональних даних не повідомляється, що, безумовно, обмежує його право на захист персональних даних.

Законопроект передбачає впровадження інституції Уповноваженого з питань захисту персональних даних, а також Спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних. Однак видається зайвим існування як інституції Уповноваженого з питань захисту персональних даних (стаття 25), так і Спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних (стаття 26), з повноваженнями, які частково співпадають.

Видається за доцільне створення саме інституту Уповноваженого з питань захисту персональних даних та інформації, який би опікувався не лише захистом персональних даних, а й права на інформацію. На нашу

думку, цей Уповноважений мав би призначатися Верховною Радою. Цей інститут можно також створити як окремий підрозділ апарату Уповноваженного ВРУ з прав людини. Необхідно передбачити вимоги, що пред'являються до осіб, які претендують на цю посаду: освіта, відсутність судимості, практика тривалої професійної діяльності чи значні наукові досягнення, громадське визнання, тощо. Також слід передбачити можливість Уповноваженого з питань персональних даних і інформації призначати представників в регіонах і умови функціонування бюро уповноваженого.

Хоча законопроект передбачає можливість забезпечення статистичними, соціологічними і науково-дослідними відомостями органів державної влади, з урахуванням права власності на персональні дані та за умови їх знеособлення (ст. 29), однак не передбачена можливість надання знеособленої персональної інформації науково-дослідним установам.

Слід також передбачити можливість передання персональних даних у архівні установи за умов забезпечення останніми належного рівня захисту персональних даних.

Складається враження, що законопроект створювався спершу для захисту автоматизованої обробки персональних даних. Спроба регулювання картотек в цьому законопроекті не носить системного характеру. Так, ст.12 «Накопичення персональних даних» не передбачає накопичення даних в картотеках, тощо. На нашу думку, на першому етапі доцільно впроваджувати захист персональних даних лише стосовно персональних даних, які зазнають автоматизованої обробки (тобто зі сфери дії закону слід виключити ручні картотеки). На цьому етапі також не варто поширювати його діяльність на окремих фізичних осіб, що займаються приватною практикою. З часом дію цього закону можна буде поширити і на картотеки, і таких осіб.

Стосовно таких категорій персональних даних, які стосуються медичної інформації про особу або тих, які зберігаються в архівах, і тих, які стосуються захисту персональних даних в сфері телекомунікацій, необхідно буде прийняти окремі закони.

Зауважимо, що цей законопроект залишив поза розглядом такі важливі проблеми як:

– заборону на об'єднання баз персональних даних, що обробляються з різними цілями;

– заборону на введення універсального особистого багатоцільового ідентифікаційного коду;

– не врегульовано процедуру знищення персональних даних;

– не передбачається розділення персональних даних на

1) загальні персональні дані: ім'я, прізвище по-батькові, дата і місце народження, адреса:

2) спеціальні (вразливі) персональні дані: етнічне (расове) походження, політичні погляди чи партійна приналежність, релігійні або інші переко-

нання, стан здоров'я, статеве життя, наявність судимості за кримінальні злочини. Подібне розмежування дасть можливість створити різні режими користування і поширення персональних даних – більш відкритий для першої групи і більш закритий для другої.

Слід зауважити, що прийняття цього закону повинно потягти за собою зміни ч.2 статті 23 Закону «Про інформацію» з метою узгодження двох законів. Ця стаття проголошує: «Основними даними про особу (персональними даними) є: національність, освіта, сімейний стан, релігійність, стан здоров'я, а також адреса, дата і місце народження» . Очевидно, що з основних даних слід виключити ті, які є вразливими: релігійність, стан здоров'я.

Проект Закону України №4002 від 17.07.2003 р. «Про Єдиний реєстр персональних даних»

Питання реєстрації особи можна розглядати в різних аспектах. Так, можна дивитися на неї з точки зору зручності і спрощення роботи державних органів влади. А можна з точки зору захисту прав і свобод людини. В цьому випадку, з урахуванням нашої історії слід дуже обережно підходити до впровадження універсального реєстраційного коду, який би мав розміщатися на всіх документах особи (як це передбачено в статтях 3 і 27 законопроекту), точніше, слід вважати такий реєстраційний код неприйнятним. Необхідність застосування єдиного ідентифікаційного номеру у всіх документах, що належать особі, тягне за собою порушення права особи на конфіденційність персональних даних, внаслідок, в цьому випадку, можливості у держави відслідкувати всі дії і пересування конкретної особи. На нашу думку, в законі повинні бути чітко визначені цілі збору інформації про особу: наприклад, ідентифікація особи або реєстрація постійного місця проживання.

На жаль, цей законопроект, хоча й намагався уникнути недоліків своїх попередників, так і не зміг цілком позбутися спокуси принести право особи на конфіденційність інформації про неї (ч.2 ст. 32 Конституції України) в жертву зручності діяльності державних органів. Показовим в цьому відношенні є той факт, що слова «персональні дані» зустрічаються в тексті законопроекту лише два рази, причому обидва рази в назві реєстру. Далі реєстр починає називатися Єдиний реєстр фізичних осіб (ст.1).

Стаття 14 законопроекту передбачає визначення Адміністратора Єдиного реєстру на конкурсних засадах: юридична особа, з урахуванням встановленим Мін'юстом кваліфікаційних вимог та з укладанням договору з Мінюстом на виконання цих функцій. Це положення викликає низку запитань, зокрема, чи не загрожуватиме запрошення сторонньої юридичної особи для виконання функцій конфіденційності персональних даних?

На нашу думку, персональна інформація, збір якої передбачений ст.24 законопроекту, є надлишковою для виконання передбачених функцій. Так, наприклад виникає питання в потрібності внесення ідентифікаційного номера дітей, батьків, подружжя.

Ми вважаємо, що окремо повинен виділятися реєстр з інформацією щодо військового обов'язку, про розшук, про обмеження дієздатності тощо.

Даний законопроект, на жаль, як і низка попередніх не вільний від певних недоліків. Так, бажання авторів зробити більш ефективною обробку персональних даних тим самим створює загрозу для порушення конфіденційності персональних даних. Автори законопроекту, навіть не вважають за потрібне інформувати особу про те, що її персональними даними хтось користується і взаємозв'язки між Єдиним реєстром і громадянином будують за принципом «громадянин зобов'язаний», забуваючи, що громадянин перш за все має право. В законопроекті, на жаль, не згадується інституція Уповноваженого з персональних даних. Загалом складається враження, що збір персональних даних в Єдиний реєстр за цим законопроектом дасть можливість вдатися до глобального контролю за діяльністю особи, наприклад, завдяки пов'язанню ідентифікаційного коду з оподаткуванням.

Необхідно зауважити, що законопроект не передбачає можливості особи відмовитися від надання ідентифікаційного коду з релігійних переконань, що, як свідчила процедура надання податкового ідентифікаційного номеру є необхідним. Більше того, законопроект скасовує усі існуючі заперечення щодо такої відмови, що викличе загострення конфліктів у цій сфері.

Таким чином, мусимо констатувати, що, на превеликий жаль, всі існуючі законопроекти у сфері реєстрації особи та захисту персональних даних далекі від досконалості.


A
B
C

ПРАВО НА ПРИВАТНІСТЬ ТА ДОСТУП ДО АРХІВІВ

Замість передмови

Увазі читачів пропонуються переклади декількох матеріалів літньої школи Центрально-Європейського університету 2000 року по доступу до інформації і доступу до архівів, підготовлені Харківською правозахисною групою, у яких викладені сучасні підходи до законодавчого регулювання і практики доступу до архівної інформації, зокрема архівних джерел, пов'язаних з політичними репресіями за часів тоталітарних режимів. Розглядається майже весь спектр проблем – методи та загальні принципи регулювання, балансування дотримання права на приватність та реалізації права знати зміст відомостей, що зберігаються, доцільність зберігання в архівах персональних даних, реалізація доступу до них, процедурні гарантії доступу до архівних даних, особливості законодавства та практики доступу до архівів служб безпеки колишніх тоталітарних режимів. Обговорюється роль архівів для реалізації колективних і індивідуальних прав, необхідність зберігання архівів репресивних режимів, розголошення інформації про них і створення відповідної законодавчої бази, Етичний Кодекс архівного працівника і багато інших важливих питань. На мою думку, вони вкрай актуальні для сьогодення і майбутнього нашої країни, вивчення її новітньої історії.

Як казав Володимир Буковський, комунізм у СРСР не був переможений, він зруйнувався від власної ваги. Тому в Україні не було процесу декомунізації на зразок польського, чеського чи угорського. Серед вищих посадових осіб держави чимало людей, причетних до переслідувань правозахисників за тоталітарного режиму. Це обумовило досить таки утруднений доступ до архівних джерел, що стосуються політичних репресій. Наприклад, доступ до архівно-слідчих справ реабілітованих можливий тільки для самих реабілітованих або їх нащадків, або дослідників за згодою реабілітованого чи його родини. Архівно-слідчі справи тих, хто не реабілітований, охороняються як відомості, віднесені до державної таємниці. Але, як стверджують дослідники, навіть маючи дозвіл на вивчення архівно-слідчої справи чи відповідну форму допуску до відомостей, що складають державну таємницю, все одно дістатися до архівних матеріалів важко. Що ж стосується справ оперативного обліку, то, як відомо, ще в 1989 році було прийняте рішення про їхнє знищення. Хтось

скаже: кому потрібні сьогодні оперативні розробки дисидентів, докладні секретних агентів КДБ, дані зовнішнього стеження, записи телефонних розмов тощо? Проте, достатньо навести тільки один приклад, щоби стало ясно, чого нас лишили: остання книга поезій і перекладів Василя Стуса «Птах душі», написана під час перебування в спецполітзоні в Кучино в останні роки життя, мабуть, знищена разом з його справою оперативного обліку. На нашу думку, необхідно ретельно облікувати архівні джерела, пов'язані з політичними репресіями, розробити нормативні акти щодо зберігання і доступу до цих даних, забезпечуючи баланс можливості доступу дослідників і захист приватності жертв політичних репресій.

Щоправда, архіви СБУ копіюють деякі документи для публікацій, друкується фаховий журнал «З архівів ВЧК-ГПУ-НКВД-КГБ», ведуться певні наукові дослідження по історії політичних репресій. Але стан з доступом до архівних даних про репресії і загалом доступом до архівів, як на мене, не можна визнати задовільним. Певною мірою це пов'язане з прогалинами в законодавстві, зокрема відсутністю закону про захист персональних даних. Сподіваємося, що висвітлення досвіду більш успішних країн приверне увагу громадськості до цієї проблеми й стимулюватиме зміни в законодавстві і практиці України.

Євген Захаров

Ганс Пітер Буль

ДОСТУП ДО ІНФОРМАЦІЇ: ЮРИДИЧНІ АСПЕКТИ

Нове законодавство щодо архівів як продукт сучасної юридичної думки: баланс свободи інформації і захисту даних

Свобода інформації і доступу до архівів не є традиційним предметом законодавства. Про неї не згадується ні в Десяти заповідях, ні в національних конституціях. Насправді, до останніх років були лише закони, які стосувалися створення чи організації архівів. Доступ до архівів регулювався лише внутрішніми нормами; загалом архіви могли самостійно визначати зв'язки з користувачами.

Однак вимога відкритості й, у широкому значенні, свободи інформації, яка виразно постала за останні десятиліття, спричинила прийняття нового законодавства в багатьох країнах. Уряди змушені були відповісти людям, які хотіли знати, що відбувається за лаштунками. Не лише архіви були примушені відкрити свої досьє, але також діючі державні органи влади були змушені відкинути традицію офіційної таємності. Таким чином, доступ до інформації і через це – доступ до архівів стали питанням громадського інтересу і, в результаті цього, предметом законодавства. Декілька країн ввели детальні закони про свободу інформації. Інші – мають лише проекти нормативних актів про відкритість і право особи бути інформованою щодо спеціальних категорій даних. Таке законодавство розглядається як індикатор ступеня політичної свободи і демократії, впровадженої в країні; чим менше обмежень накладено на вільний доступ до архівів, тим більше можливі політичні дискусії і тим більший рівень участі в них.

Потрібно нагадати другу причину створення і, до певної міри, модифікації нового законодавства щодо доступу до інформації і архівів: динаміка приватності і захисту даних. З моменту розуміння того, що збір і обробка даних за допомогою комп'ютерів може нести ризик правам та інтересам особи, законодавці в усьому світі прийняли закони про захист даних і створили відповідні органи влади спеціально для того, щоб перевіряти і наглядати за інституціями, які обробляють дані. Для архівів це може призвести до проблем з агенціями й іншими органами влади, які збиралися передати свої досьє і записи до архівів, і з особами, згадуваними в збірках інформації. Захист даних, здається, має за мету захист таємниць, які закони про свободу інформації покликані знищити, але обидві позиції може бути, до певної міри, гармонізовано, і вони *повинні* бути зроблені сумісними. Проблема полягає у збалансуванні інтересів тих, хто вимагає інформацію, і тих, хто покладається на конфіденційність. Цей баланс мо-

жна досягти у щоденній адміністративній практиці, але він також вимагає законодавчих рішень. Уряди в цілому і архіви зокрема потребують моральної довіри від широкої публіки як основи їхньої діяльності, і її може бути збільшено засобами належного застосування справедливих норм.

У цій роботі розглядаються засади і принципи, сформульовані в міжнародному праві та елементи їх реалізації в національному законодавстві різних країн.

МІЖНАРОДНІ ЮРИДИЧНІ РАМКИ

Загальна декларація прав людини, прийнята 10 грудня 1948 року Генеральною Асамблеєю ООН, надає кожному право шукати, отримувати і розповсюджувати інформацію та ідеї будь-якими засобами і незалежно від кордонів (стаття 19). На додаток до цього, кожний має право вільно брати участь у культурному житті суспільства, насолоджуватися мистецтвом, брати участь у науковому прогресі і користуватися його благами (п.1 статті 27). Архіви є важливим засобом інформації і їхнє використання складає частину культурного життя кожної спільноти.

Міжнародний пакт про громадянські і політичні права 1966 року повторив статтю 19 Загальної декларації прав людини приблизно тими ж словами (п.2 ст.19), але припустив, що здійснення цього права може підлягати певним обмеженням, якщо вони передбачені законом і є необхідними для поваги прав чи репутації інших, чи для захисту національної безпеки, громадського порядку, суспільного здоров'я або моралі. Це ж право гарантується Європейською Конвенцією прав людини 1950 року (п.1 стаття 10). У відповідності до п.2 здійснення цих свобод може підлягати формальностям, умовам, обмеженням або санкціям, що встановлені законом в інтересах національної безпеки, територіальної цілісності або громадської безпеки для охорони порядку або запобігання злочинам, для охорони здоров'я або моралі, для захисту репутації або прав інших осіб, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету і безсторонності суду, і є необхідними в демократичному суспільстві. З іншого боку, Європейська конвенція також підтверджує право особи на приватність (стаття 8) з майже таким же положенням про вилучення, як і в статті 10. Ці статті описують конфлікт інтересів і позицій, який потрібно враховувати у процесі створення законів про архіви.

Американська Конвенція з прав людини (результат Конференції, що проходила у Сан-Хосе, Коста-Ріка, у 1969 році) підтверджує свободу шукати, отримувати і передавати інформацію та ідеї всіх видів, незалежно від кордонів... (ст.13). Цікаво, що ця конвенція також встановлює право на відповідь: будь-хто, кому було завдано шкоди неточними чи образливими твердженнями чи ідеями, поширеними серед громадськості, через юридично регламентовані засоби комунікації мають право відповісти чи внести виправлення, використовуючи той самий засіб комунікації, в від-

повідності до тих умов, які закон може встановити. Хоча архіви не є засобами комунікації у строгому значенні, ідея, яка призвела до цієї статті, може бути передана до них: не виправлення, а відповідь чи доповнення до вмісту архівів могло б бути більш адекватним рішенням для обох сторін, тобто і для архівів, і для осіб, яких це стосується.

На завершення, держави-учасниці Організації Африканської Єдності уклали Африканську Хартію з прав людини і народів у 1981 році. Тут також закріплюються право отримувати інформацію (ст.9), як і право брати участь у культурному житті суспільства (п.2 ст.17).

Європейський парламент і Рада Європейської Спільноти встановили зобов'язання для країн-учасниць щодо обробки персональних даних у Директиві 95/46/ЕС (від 24 жовтня 1995 року). Країни повинні гарантувати, що ці дані збираються з точно визначеними, явними і законними цілями і що надалі обробки даних способом, несумісним з цими цілями, не буде. Крім того, обробка даних з історичною, статистичною чи науковою метою не визнається несумісною передбачаючи, що країни-учасниці забезпечать відповідну охорону для такої обробки (п.1b ст.6) чи для довготривалого зберігання з метою історичного, статистичного чи наукового використання (п.1e ст.6). Ці захисні заходи повинні, зокрема, виключити використання даних для мети підтримки заходів чи рішень стосовно будь-яких особливих персон (виклад фактів №29).

НАЦІОНАЛЬНЕ ЗАКОНОДАВСТВО: МЕТОДИ І ПРИНЦИПИ

Методи регулювання

Існують різні традиції законодавства і нормотворчості. У країнах загального права суди відіграють найбільш важливу роль у створенні права; в інших юридичних культурах на більшість юридичних питань дає відповідь законодавство, яке можна охарактеризувати як більш абстрактне у порівнянні з прецедентним правом. У сфері права про дані та інформацію обидві моделі сходяться; ми часто знаходимо комбінації системних законодавчих конструкцій і додаткового прецедентного права. Часто спеціальні аспекти виражені точно і конкретно, але загальні і більш абстрактні норми змішуються з тими, що необхідні для використання правниками їхнього професійного досвіду з тим, щоб знайти прийнятні рішення щодо обговорюваних справ. Крім того, адміністративні керівні вказівки пишуться для допомоги правникам-практикам, щоб вони могли діяти згідно з чинними нормами права.

Разом з тим існує ще альтернативний шлях досягнення балансу між таємністю і відкритістю: саморегуляція тими, хто зберігає і використовує дані та їхніми професійними асоціаціями (напр. Етичні кодекси).

У відповідності до європейської юридичної традиції, адміністративні керівні роз'яснення і саморегуляція є недостатніми для визначення й обмеження індивідуальних прав людини стосовно офіційних органів, на кшта-

лт державних чи муніципальних архівів. Фактично, тільки несуттєві питання (напр. плата і витрати на використання архівних документів) можуть бути врегульовані цим способом. Але, звичайно, повинні поважатися юридичні традиції кожної країни.

ЗАГАЛЬНІ ПРИНЦИПИ

Відкритість проти таємності. Ні повна відкритість, ні цілковита таємність не були б розумними, і жодна країна у світі не зайняла одну з цих крайніх позицій. Може бути поставлене лише питання про те, якої відкритості і якої таємності ми потребуємо. Це означає: які типи даних повинні зберігатися в таємниці, згідно з якими обставинами і на який період, з яких причин і в інтересах якої особи чи інституцій. Законодавство про доступ до архівів зустрілося з викликом, кинутим йому фундаментальним *правом особи знати*, і це приводить нас до питання: наскільки відкритість можлива, і наскільки таємність необхідна. Ось чому державна традиція таємності поступово відходить у минуле; *arcana imperii*[30] більше не сприймається як нормальний феномен у демократичному суспільстві.

Ми припускаємо, що це відбувається не скрізь. Але політичні революції, що змінили юридичні структури багатьох країн протягом останніх кількох років, також вплинули на місце архівів у цих країнах і на доступ до них. Наприклад, Албанія внесла зміни до законодавства про архіви у 1993 році: до цього часу воно було надзвичайно заполітизоване і антинаукове і дотримувалося принципу таємності без обмеження у часі. Тепер воно визнає документи у звичайній справі вільними для доступу через 25 років після їхнього створення.

УМОВИ ОПРИЛЮДНЕННЯ

- *Період закритості*

Законодавство про архіви в усьому світі містить різні періоди закритості, під час яких документи можуть бути відкритими у відповідності до спеціальних обмежувальних умов (наприклад, для використання органами, що їх створили). Ці періоди можуть коливатися від 25 до 50 років після року, в якому ці документи були створені; видається, що стандарт становить 30 років. Файли і документи, які стосуються приватних осіб, звичайно, зберігаються у таємниці протягом 30 років після смерті особи, якої це стосується, але в декількох країнах, за певних обставин, зберігаються і до 150 років після смерті особи.

- *Законні інтереси*

У деяких країнах потенційні користувачі повинні довести свій законний інтерес щодо згаданих документів, а найбільш ліберальні законодавці надали доступ кожному тільки на основі заяви, без будь-якої пере-

[30] *Таємниця імперії(лат.)*

вірки. Інший спосіб врегулювати доступ – визначити певні цілі, для яких документи можуть бути відкриті (напр. наукова, технологічна, культурна чи економічна діяльність – як це зробила Польща, декілька земель Німеччини та інші).

- *Винятки*

Навіть у цьому випадку потрібно розглянути винятки. Типовими і найбільш часто згадуваними причинами зберігання файлів і документів у таємниці є наступні: (а) національна безпека, оборона й іноземна політика; і (б) приватність, торгові інтереси та інші законні інтереси третіх осіб.

Крім того, мета запобігання – зберегти архівні документи фізично і знизити адміністративні зусилля щодо нагляду за документами. Виразити словами це можна по-різному, але переважно майже всі існуючі закони про доступ до архівів зосереджуються на двох вищезгаданих сферах, у тому числі – положення про повний захист інтересів особи (що стосується, наприклад, комерційної та фінансової інформації, кримінальних справ і медичних карток) та публічних інтересів (наприклад, правоохоронна діяльність і розвідка). Статті загального характеру іноді використовують для охоплення як приватних, так і публічних інтересів тоді, коли таємність необхідна через спеціальну природу справи (Данія).

Обмеження в інтересах захисту авторських прав, права на використання та інших приватних прав, що стосуються даних, взагалі рідко або, наскільки нам відомо, ніколи не забезпечується конкретними статтями законодавства про архіви. Ці інтереси гарантувались на більш ранній стадії процесу, яка настає тоді, коли дані передаються до архіву. Тоді можуть бути укладені приватні договори для захисту цих прав (напр., шляхом продовження терміну закритості, обмеження права архівів приймати рішення і впровадження положень, що обмежують доступ до файлів для певних категорій громадськості). Наприклад, у відповідності до закону Франції «Адміністрації, які на це вповноважені, зобов'язані дотримуватись умов збереження та оприлюднення, які можуть бути надані власником (ст. 10)».

Ми повинні розрізняти закони, які точно передбачають винятки, і ті, які уповноважують самих міністрів чи архіви розглядати спеціальні справи щодо розкриття чи нерозкриття (напр., Данія, Росія і Польща). Звичайно, суперечка між заявниками і архівами може постати навіть тоді, коли сам закон визначає умови та обмеження відкритості; у цьому випадку наступним питанням є те, чи заявники можуть звертатися до суду і чи має він владу зобов'язати архіви.

Дуже часто ми знаходимо комбінацію статей про винятки і періоди закритості, результатом яких є певні категорії даних, особливо щодо вразливої персональної інформації, які підлягають обмеженням на *довший період*, ніж звичайні дані (наприклад, у Данії, Франції, Португалії і Росії). Так, Данія дозволяє архівам встановлювати період закритості довший ніж

30 років, коли вони вважають, що це необхідно для захисту «основних інтересів, на кшталт національної безпеки чи оборони держави, захисту звинувачених осіб, свідків чи будь-яких інших осіб, втягнутих у кримінальні справи чи дисциплінарні провадження.» На противагу цьому Чеська Республіка зайняла протилежну позицію, заборонивши архівним працівникам *скорочувати* період закритості, коли національна безпека чи інтереси особи можуть бути піддані небезпеці.

СПЕЦІАЛЬНІ КАТЕГОРІЇ ДАНИХ

Ми вже згадували, що спеціальні категорії персональних даних трактуються по-різному. Європейський Союз наказав своїм країнам-учасницям заборонити обробку персональних даних, що розкривають расове чи етнічне походження, політичні погляди, релігійні чи філософські переконання і членство в профспілці та обробку даних стосовно здоров'я чи статевого життя.

Повинні передбачатися особливі заходи охорони для обробки даних, пов'язаних з правопорушеннями, кримінальними вироками чи заходами безпеки (Європейська Директива Захисту Даних п.п.1 і 5 ст.8). Національні закони про захист даних, загалом, гарантують сильніший захист для цих видів інформації, ніж для інших. Але цей принцип не спрацьовує щодо архівів. Вони повинні бути зацікавленими у збереженні такої інформації для майбутньої наукової, журналістської чи особистої оцінки, таким чином, щоб конфліктуючі інтереси були гармонізовані. Цього можна досягти суворим дотриманням періоду закритості – можливе його продовження – та додатковими застереженнями, і, перш за все, обережною перевіркою і збалансуванням інтересів. Європейська Директива дозволяє винятки із заборони (п.1 ст.8) з причини суттєвого публічного інтересу (п.4 ст.8), але не згадує архіви в цьому контексті.

Федеральна Республіка Німеччини повинна подолати особливу проблему, підняту її об'єднанням з Німецькою Демократичною Республікою (НДР) – а саме делікатний спадок від колишнього Міністерства Державної Безпеки (Штазі): сотні тисяч досьє, що містять приватну, часто невизначену, інформацію про осіб, вироблену в процесі масового нагляду цією величезною організацією внутрішньої розвідки, яка була інструментом придушення. Ці документи отримали за законом спеціальний юридичний статус, і вони управляються агенцією, очолюваною незалежним уповноваженим, який був видатним дисидентом у НДР. Доступ до цих документів надається для історичних досліджень і людям, яких переслідували при комуністичному режимі, для щоб переглянути їхню персональну інформацію. Крім того Федеральним архівом було засновано фонд управління комуністичними архівами та архівами інших масових організацій у НДР. Тридцятилітній період закритості не застосовується щодо того, що зберігається у цьому фонді.

ПРАВО НА ДОСТУП ДО ПРИВАТНИХ АРХІВІВ

У Нарисі Стандартів Європейської Політики про доступ до архівів, що був підготовлений Міжнародною радою архівів, справедливо стверджується, що у правовій системі, яка гарантує приватну власність, роль держави стосовно захисту приватних архівів (напр. ділових, родинних архівів чи архівів об'єднань громадян або релігійних груп) є необхідно обмеженою у підтримці і сприянні, і що закон може ясно зв'язати виплату публічних субсидій власникам приватних архівів з їхньою згодою на норми доступу, співставні з тими, які застосовуються у публічних архівах (p.5 no.7). Звичайно, публічні архіви повинні намагатися (і повинні бути в змозі), набути приватні збірки, які представляють загальний інтерес, для того, щоб відкрити ці документи громадськості (порівняйте ICA Principles for Archives and Current Records Legislation, Ottawa 1996, p.3 no.5).

КОНФЛІКТ МІЖ ВИЛУЧЕННЯМ І ЗБЕРЕЖЕННЯМ ПЕРСОНАЛЬНИХ ДАНИХ

Закони про захист даних звичайно вимагають, щоб персональні дані, які зберігаються публічними органами влади чи приватними компаніями, але більше не потрібні для первинної адміністративної чи приватної мети, того, хто їх створив, були знищені чи, принаймні, заблоковані. Але вони не повинні призначатися для наголошення на знищенні всієї персональної інформації такого роду, замість передачі їх до архівів. Таке законодавство про захист даних призвело до проблеми: як здійснити обов'язок знищити інформацію, яка не є необхідною (і полегшити зберігання даних діючих організацій), і у той же час набути відповідного матеріалу для архіву. Архіви як пам'ять націй і суспільств не може обмежити себе неперсональними даними. Вони потребують більше ніж специфічного вилучення персональних даних, тому що сучасні соціальні дослідження та, імовірно, майбутні соціальні дослідження вимагають значних обсягів даних для того, щоб зуміти використати статистичний та інші подібні методи. У відповідності до федерального права Німеччини, норми права, що встановлюють обов'язок знищити документи, вважаються не чинними (у зв'язку з наявністю обов'язку передати документи до Федерального архіву), але право земель дещо відмінне.

Ми повинні трактувати цей пункт навіть більш загально і відзначити зв'язок між колом документів, які повинні бути передані до архівів, і ступенем відкритості, наданої архівами громадськості. Ті, хто відповідальний за документи, будуть неохоче передавати їх до архівів, якщо архіви юридично зобов'язані відкрити свої двері першому-ліпшому. Приватні особи, а також державні органи влади, які стурбовані, що таємні файли можуть стати публічними, дуже рано намагатимуться уникнути поширення такого матеріалу. Знищення документів – згідно з положеннями про захист даних чи без такого юридичного підґрунтя – може бути вчинене для того, щоб захистити приватність осіб, завдаючи шкоди архівам.

Щоб запобігти цьому, закон Німеччини «Про архіви» говорить, що з моменту, коли документи передано до Федерального архіву, архів повинен поважати законні інтереси осіб, яких вони стосуються, такою ж мірою як і агенцій, які їх передали. Зокрема, архів повинен дотримуватися положень про обробку і забезпечення безпеки персональних даних, які застосовуються до агенцій, що їх передають (п.4 ст.2). Очевидно, що конфлікт між знищенням і збереженням персональних даних залишається головною проблемою і дуже важко знайти задовільні правила для збалансування залучених у справу інтересів.

ПРИВІЛЕЇ ПУБЛІЧНИХ ПОСАДОВЦІВ

Як підтвердив Нарис, публічні посадовці не можуть запобігати доступу до публічних документів, вироблених у процесі виконання їхніх адміністративних обов'язків, на основі вимоги поважати їхню власну приватність (p.4 no.2 iv; дивися також Principles p.2, no.3). У цьому контексті цікаво відзначити, що, згідно з правом Німеччини, період закритості може бути скорочено, якщо особи, що представляють публічний інтерес або публічні посадовці виконують свій обов'язок (п.5, ст.5, 4-те речення).

ІНДИВІДУАЛЬНІ ПРАВА ЗАЦІКАВЛЕНИХ ОСІБ (ІНФОРМАЦІЯ, ДОСТУП ДО ВЛАСНИХ ДАНИХ, ВИПРАВЛЕННЯ)

Багато законів про захист даних визначають право зацікавлених осіб (суб'єктів даних) бути інформованими щодо збирання і зберігання їхніх персональних даних. Європейська директива з захисту даних конкретизує, які види інформації країни-учасниці Європейського Союзу повинні забезпечити суб'єктам даних: інформацію, коли дані збираються у суб'єкта даних (ст.10); і інформацію, коли дані не збиралися від суб'єкту даних (ст.11). Архівів стосується п.2 ст.11. Він містить виключення з цього зобов'язання, коли (особливо із статистичною метою, чи з метою історичних або наукових досліджень) забезпечення такої інформації підтверджує неможливість чи, ймовірно, втягнення непропорційних зусиль, чи якщо запис або розголошення чітко передбачено законом. У цих випадках країни-учасниці повинні забезпечити відповідні заходи безпеки.

Більше того, суб'єкти даних загалом мають право доступу до їхніх власних персональних даних. Це право складає основний елемент законодавства захисту даних в усьому світі і може бути використане у підготовці до можливого внесення змін і знищення даних. Ст.12 Європейської директиви встановила серед інших індивідуальне право суб'єктів даних отримувати від контролерів даних:

– оброблену інформацію про себе та її джерела; і

– в залежності від обстановки право на виправлення, знищення чи блокування даних, що обробляються, які не відповідають статтям Директиви, особливо через неповноту чи неточну природу даних.

Використання цих прав – особливо права на виправлення – може призвести до конфлікту з філософією, згідно з якою архіви повинні зберігати інформацію, навіть якщо інформація, що міститься в них, є неправильною чи недостовірною. Але, наскільки ми бачимо, законодавство про захист даних і архіви стосовно цього все ще потребує гармонізації. Європейська Директива дозволяє країнам-учасницям ЄС обмежити сферу цих зобов'язань і прав, щоб гарантувати деякі цілі (напр., національну безпеку), але історичні дослідження, – що відрізняються від наукових досліджень – не згадуються у цьому списку (ст.13). Так що обговорення повинно бути продовжене. На наш погляд, було б можливим знайти альтернативні рішення (напр., право додати пояснення до документа, яке б зберігалося разом з ним) (Gegendarstellung, порів. Закон Баварії про архіви п.3 ст.11).

ПРОЦЕДУРНІ ГАРАНТІЇ ДОСТУПУ ДО АРХІВІВ

Принципи, що супроводжують Нарис Стандартів Європейської Політики про доступ до архівів справедливо вказують, що особи, які вимагають доступу до архівів, повинні мати можливість подавати апеляцію на негативні рішення (p.6 no.14). У цьому ж розумінні Нарис вимагає, щоб особи мали право апелювати до вищої адміністрації тієї служби, яка заборонила доступ, і до суду у випадку відмови вищою адміністрацією (p.8, no.13). Питання, чи такі права надаються відповідним національним законодавством, залежить від того, як загалом відправляється правосуддя, і до якої міри поважаються права людини в країні. Багато країн встановили чітку систему судового нагляду.

ВИСНОВКИ

Цей огляд показав, що законом може бути врегульовано і фактично врегульовано багато аспектів архівної роботи, але багато інших відкрито для подальшого обговорення і внесення у законодавство. Ми поділяємо думку Міжнародної ради архівів, що повинно бути сформульовано таку сукупність принципів, які б підтверджували демократичні ідеали, були сумісними із стандартами моралі всіх країн, та, імовірно, надихали політику країн-учасниць стосовно доступу до архівів. Ми сподіваємося, що наші примітки зроблять внесок у ці зусилля.

А.П. ван Вліст

ПРАВО ЗНАТИ, ПРАВО ЗАБУТИ?

ПЕРСОНАЛЬНА ІНФОРМАЦІЯ В ПУБЛІЧНИХ АРХІВАХ[31]

Це починається з народженням: готуючи посвідчення про народження, держава починає записувати інформацію про свого нового громадянина. Але досьє не порожні: ще до народження держава сама займається реєстрацією і збором архівів, наприклад, коли районний суддя повинен призначити опікуна ненародженій дитині вдови після смерті чоловіка. І так продовжується протягом усього життя особи. У різноманітних формах держава збирає і оформлює навіть багатогранну персональну інформацію. Тільки подумайте самі – ваші водійські права, паспорт, бібліотечна перепустка, документи, які стосуються вашого дому, ваше призначення на державну службу, перегляд права на пенсію, призначення вашого номера соціального забезпечення, податкова декларація. І це відбувається з усією персональною інформацією, яку ви знаєте і яку ви переважно самі надаєте в офіційних формах, анкетах чи деклараціях. Але чи знаєте ви, що саме у ваших файлах зберігає податкове відомство: ваші податкові декларації, звіти про фінансові розслідування, дані про ваші позики, записи компаній страхування життя, банків та інших інституцій, дані з відділу податкових розслідувань й інших підрозділів податкової служби, вирізки з щоденних видань і тижневиків (наприклад, які стосуються оренди кімнат чи другої квартири), подальші шматочки інформації, які мають постійне значення і стосуються питань на кшталт розподілу майна, угоди про щорічні виплати, надання субсидії для чийогось житла, купівля і продаж нерухомості тощо, тощо, тощо.

Ці файли складають лише одну серію урядових документів. Але існують тисячі інших. *Персональний інформаційний індекс* Канади підсумовує більше ніж 4000 серій персональних файлів: сільськогосподарські субсидії, досьє колишніх військовослужбовців, субсидію на квартиру, дозвіл на проживання і багато інших.[32] Усі ці серії містять персональну інформацію і складають велику і реальну частину державних записів. Час-

---

[31] Дещо скорочений варіант оригіналу, надрукованого в Archives and manuscripts//The Journal of the Australian Society of Archivists 23 (1995) p. 8-17. Пізніше також надруковано з деякими змінами і доповненнями як Bescerming van de privacy// Nederlands Archievenblad 99 (1995) p. 102-108.

[32] Terry Cook, *The archival appraisal of records containing personal information: a RAMP study with guidelines* (UNESCO; Paris, 1991)

тина з них через деякий час передається до публічних сховищ, де вони можуть використовуватися громадянами, які шукають справедливості чи доказів чогось, державними органами влади чи дослідниками історії.

Але чи повинно це завжди бути саме так? Ні, не повинно, тому що персональна інформація є за своєю природою інформацією про персональну сферу. Витік чи оприлюднення такої інформації є порушенням приватності. Однак приватність захищається, і цей захист складається з певних шарів.[33]

Перший шар – це законодавство. Наша Конституція [Нідерландів] передбачає законодавство для захисту персональної сфери з огляду на убезпечення й отримання персональних даних. Цей закон відомий як «*Wet Persoonsregistraties»* (WPR) – Закон «Про персональні дані». «WPR» не застосовується до персональних архівів у архівних сховищах згідно з термінологією Закону «Про архіви» від 1962 року. Саме тому захист приватності повинен гарантуватися режимом законодавства про архіви.

Це законодавство про архіви визначає, що обмеження на доступ до архівних матеріалів у публічному сховищі – національному, обласному чи місцевому – може встановлюватися тільки за згодою власника архіву і тільки з огляду на «повагу приватності особи» чи для «запобігання непропорційній вигоді або шкоді, завданій фізичним і юридичним особам, залучених до цього, чи третім особам». У випадку обмеженого доступу, керівництво архівів може, після відповідної консультації з агенцією, яка створила ці документи, надати дозвіл на доступ, тобто зняти обмеження на прохання заявника, якщо більш пізній інтерес в ознайомленні з записами чи їх використанні переважує інтереси, яким слугують ці обмеження.

Обмеження на доступ мають визначатися часом, коли записи передані у сховище. Саме тому умови передачі складають другий шар первинного захисту через регулювання доступу і порядку розкриття персональної інформації.

Умови передачі персональної інформації часто включають у себе правило, яке обумовлює, щоб архіви з вразливою інформацією були доступні лише дослідникам, які підписали певне зобов'язання.[34] Це зобов'язання визначає третій шар регулювання доступу до персональної інформації та її опублікування.

Четвертий шар захисту приватності сформовано фізичними і практичними правилами, згідно з якими архіви на місцях повинні запобігати ознайомленню з персональною інформацією осіб, які не мають на це дозволу: зберігання в безпечних сховищах (інколи, додатково, в теках, що замикаються), обережність у процедурах поводження зі справами і їх-

[33] Ми запозичили цей образ шарів захисту з H.Raaska, «Personal privacy and the archivist» (неопубліковані матеріали NARA Professional Career Training Program; 1989)

[34] Дивись моє ессе «Archives of the people, by the people, for the people» з тому 1 лекційного курсу Доступ до інформації, доступ до архівів, CEU Summer University 2000

ньому наданні, контрольна система архівів (на кшталт «Архейону», який використовується в усіх державних архівах Нідерландів), який повідомляє про небезпеку, в тому випадку, коли частина з групи записів не може видаватися дослідникові, тощо .

Ці чотири форми захисту – законодавство, умови передачі, зобов'язання дослідників і фізичні умови видаються цілком достатніми. Але не повністю.

По-перше, має бути зібраний досвід із застосування цих правил, головним чином той, що стосується використання персональної інформації з довоєнного часу. Віднедавна ми маємо справу із зберіганням урядових документів, щодо яких примусова передача даних архівам з п'ятдесяти років знижена тепер до двадцяти років. Сховища, набагато більше ніж раніше, містять персональну інформацію. І можливість того, що дані стосуються живих осіб, підвищується через те, що передача матеріалів в архів є більш недавньою. Ми розуміємо це тепер після підготовки для передачі архівів Кабінету Королеви, Глави Кабінету Міністрів та інших урядових органів.

По-друге, перші три захисні шари складають частково еластичні, гнучкі положення. Наприклад, як у випадку першого і другого шарів, підтвердити «повагу приватності особи», як збалансувати потребу обмежити розкриття персональної інформації з інтересами дослідників, які просять зробити виняток, як провести перевірку на третьому шарі, про те «[чи] інтересам живих осіб може бути несправедливо завдано шкоди?»

У цьому місці ми досягли п'ятого шару, сферу ні формально, ні юридично не визначену: сферу, в якій тільки професійна етика може забезпечувати керівництво[35]. Сферу, де кордони все ж буде визначено, але вони можуть бути змінені в залежності від суспільства – врешті, через суди і тією мірою, якою це дозволить законодавець. Архівні працівники і дослідники повинні домовитися про свою власну поведінку на цій арені. Багато що залишається незрозумілим, ось чому ми попросимо вас допомогти нам знайти правильний шлях.

Перед тим, як персональну інформацію, що призначена для постійного зберігання, буде передано до публічного сховища, має бути визначено, чи ця інформація має таку природу, що її розкриття і опублікування могло б створити неприйнятне порушення приватності. Не вся персональна інформація є вразливою. Консультуючись з агенціями, що створюють документи, архівні працівники повинні оцінити

---

[35] Anne Cooke «A code of ethics for archivists: some points for discussion»// Archives and Manuscripts, 15. No.2 (1987), p.85, цитуючи Е.В.Рассела (1978): щодо професійної етики «будучи занадто особливою для того, щоб контролюватися законом, підзаконними актами чи іншими положеннями, але занадто загальна для того, щоб розглядатися виключно як питання для індивідуальних судових рішень стосовно архівних працівників». Дивися G.V.Peterson, T.Huskamp Peterson «Archives & Manuscripts: Law» (Chicago, 1985), для розуміння різниці між етичною і формально-юридичною відповідальністю.

інформацію особисто. Саме тоді може бути визначено, чи вони насправді мають справу з вразливим матеріалом і чи, як наслідок, ці матеріали можуть бути доступними для ознайомлення, чи ні, і якщо можуть, то за яких умов. Саме тому потрібен подвійний тест: оцінка значення персональної інформації і визначення ризиків.

Спершу розглянемо останній пункт. Приватність є основним правом. Європейська конвенція прав людини дозволяє втручання в приватність тільки тоді, якщо в демократичному суспільстві це необхідно «в інтересах національної і громадської безпеки або економічного добробуту країни, з метою запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або з метою захисту прав і свобод інших осіб».

Історичне дослідження не охоплюється цією конвенцією. У випадку наукових медичних досліджень, якщо їх доведено до кінця, з огляду на покращання рівня лікування, значення дослідження може переважити будь-яке порушення індивідуальної приватності. Це відіграє певну роль у випадку епідеміологічних досліджень, а також у наданні медичних порад стосовно генетики і в дослідженні членів сім'ї, які можуть нести підвищений ризик народження дитини з ризиком генетичного захворювання чи інфекції. Ці ситуації порушують питання етики: коли люди можуть зустрічатися з реальністю чи можливістю, що така подія станеться? У французькому розслідуванні справи про особу з маніакально-депресивним психозом, яка страждала від особливої форми глаукоми і проживала у Норд-Па-де-Кале, було встановлено за допомогою комп'ютера, що всі особи отримали це у спадок від певної пари, яка жила 500 років тому. Чи повинні були і чи могли слідчі повідомити всіх живих нащадків, близько 30000 французів, про ризик сліпоти, яка з урахуванням спадковості визначається на досить ранній стадії і може бути попереджена? Ні, – відповіла комісія з приватності, *Commission Nationale d'Informatiques et des Libertes*.[36]

У колах наукової і медичної спільнот існує побоювання, що вимога індивідуальної згоди громадян може призвести до зменшення обґрунтованості і об'єктивності результатів наукових досліджень. Дослідження, які базуються на інформації про випадки смерті від раку в районах, залежать «від милості» – за виразом заступника Комісара з приватності – тобто індивідуальної згоди пацієнтів, яка може поставити під питання репрезентативність чинного обстеження. Такі випадки охоплюються Wet Geneeskundige Behadelingsovereenkomst (WGBO) – Закон «Про згоду на лікування». WGBO дозволяє винятки з правила щодо індивідуальної згоди для користі статистичного чи наукового дослідження у сфері національного здоров'я, маючи на увазі дослідження, яке б служило загальній потребі і не могло проводитися без відповідних даних[37], таке собі прак-

[36] Spuren im Stambuch// Der Spiegel, No. 80, (1991).

[37] Дослідження можливе тільки в тому випадку, коли відповідний пацієнт спеціально не стверджував, що він/вона заперечує проти використання даних.

тичне наближення, яке означає, що ризики особи повинні бути менш серйозними, ніж користь досліджень.[38]

Історичне дослідження, однак, не надається саме до такого аналізу ризиків і користі. Альтернативний варіант запропоновано американцем Гербертом Кельманом.[39] У цьому запропонованому варіанті не зачіпаються ризики, дотичні до наслідків дослідження, а радше ризики самого дослідження. У відповідності до пропозиції Кельмана має бути визначено, чи розслідування, що використовує персональну інформацію, може бути примирене з людською гідністю. В цій праці людська гідність розуміється у кантіанському значенні: особа не повинна використовуватися іншими особами як засіб для якоїсь мети, але повинна використовуватися лише як мета. Дій, каже Кант, таким чином, щоб принцип твоїх дій міг використовуватися як загальний принцип. Або, більш буденною мовою: роби іншим тільки те, що бажав би собі.

Цей етичний тест містить два питання:

- Який ризик виникає для людської гідності через розголошення конфіденційно переданих даних?
- Чи є цей ризик прийнятним з огляду на переваги для особи або для суспільства, які можна визначити?

Цей «тест Кельмана» повинен застосовуватися перед тим, як персональну інформацію буде передано на постійне зберігання в архів. Якщо відповіді на цей тест негативні – випадок, який буває рідко – досьє повинні бути знищені. Навіть ізолювання їх на певний період невиправдане через можливість оприлюднення, і саме тому переважання інтересів, яким служить обмеження доступу, завжди залишається для даних, які не проходять тест Кельмана. Частіше, однак, результатом тесту буде більш збалансований висновок: що використання персональних даних повинно узгоджуватися з повагою людської гідності, передбачаючи обмеження доступу. Тоді ми переходимо до другого тесту, оцінюючи персональну інформацію і обставини, за яких вона може використовуватися.

На нашу думку, в майбутньому використання персональної інформації повинно б відбуватися за допомогою моделі оцінки персональної інформації, яку було розроблено канадцем Террі Куком – одним з десяти найвідоміших архівних науковців у світі. Його модель, призначена для відбору персональної інформації, може також відіграти певну роль у *використанні* персональної інформації, окрім тесту Кельмана, на який ми

[38] H.MacNeil, Defining the limits of freedom of inquiry: the ethics of disclosing personal information held in government archives// Archivaria 32 (1991) p. 139; H.MacNeil, Without consent; the ethics of disclosing personal information in public archives (Metuchen; N.J., 1992) p. 160-161.

[39] H.MacNeil, Defining the limits p. 140; H.MacNeil, Without consent, p. 164-166

вже посилалися[40]. Кук зосереджується на взаємодії між державою і громадянином, поза яким бурхливо формується персональна інформація. Оціночна модель відштовхується від трьох взаємопов'язаних факторів: програма, агенція і громадянин.

Програма – це мета, ідея, навіть ідеологія спеціального урядового завдання, частково фіксована, але часто відмінна від наміру і дійсності. Згадайте вашу власну податкову декларацію. Чим більше розрив між нормою і практикою, тим більш важливою є персональна інформація, зібрана за рішенням уряду. Природа державних програм, державних процедур впливає на природу персональної інформації. Чи питання формалізовано, створивши процедури з незначною можливістю для держави чи особи змінити інформацію або взагалі з відсутністю такої, чи можливістю навіть утримувати інформацію? Чи була ця інформація надана особисто, чи була зібрана агенцією – відкрито або без відома суб'єкта? На нашу думку, цінність джерела інформації для дослідника історії і доступ до джерела детерміновані як обсягом свободи індивіда надати інформації про нього чи про неї, так і ступенем, до якого суб'єкт має можливість контролювати і виправляти зафіксовані дані та їхнє використання. В ситуації, коли дані збиралися про індивіда не тому, що він чи вона поступали на державну службу, а тому, що уряд визнав цю інформацію необхідною, як на мене, свобода доступу до цієї інформації для історичного дослідження повинна бути обмеженою.

Кук відзначив, що чим більше простору надає урядова програма для персональних думок і варіантів, тим більший існує шанс того, що повернута, зібрана і оброблена персональна інформація буде мати значною мірою форму незалежної «картини» намірів взаємодії між державою і громадянином. Ця картина, не кажучи вже про завдання, яке держава мала на увазі, буде також визначатися урядовою агенцією, яка виконує це завдання. На агенцію, у свою чергу, впливають її службовці, культура й ідеологія як в самій агенції, так і за її межами. Розвідувальна служба відрізняється від центру зайнятості, а центр зайнятості, у свою чергу, відрізняється від податкової інспекції. Ця відмінність впливає на характер збору, обробки і використання персональної інформації. І використовується також істориками, які можуть тільки оцінити її чи його джерела в історичному й організаційному контексті, в якому цю інформацію було створено.

Третім фактором у взаємодії між державою і громадянином є сам громадянин або громадянка. Як багато ідей, емоцій і думок особи знаходиться у файлах? Як багато з того, що робить його чи її особою, можна побачити? Наскільки достовірною є інформація, отримана від суб'єкта у

[40] Cook, The archival appraisal; E. Ketelaar, Archives of the people, by the people, for the people// South African Archives Journal 34 (1992) p. 5-16

співставленні з інформацією отриманою через третіх осіб? Професійний дослідник враховує ці фактори.

Держава, агенція, громадянин – ці три змінні визначають оцінювання персональної інформації: чи правдиве представлення взаємодії між громадянином і державою, чи створено нехарактерне, побічне або нечесне враження.[41] Правдиве чи неправдиве – з усіма градаціями між ними. Ця оцінка персональної інформації, я вважаю, повинна сформувати основу для визначення, за якими умовами може бути дозволено доступ до персональної інформації – те, що я раніше називав другим шаром захисту приватності шляхом врегулювання забезпечення і розкриття персональної інформації.

Саме тому я вважаю, що, наприклад, персональна інформація, яка вільно надається агенції, що діє як «ліцензійна фабрика», ним чи нею, за встановленою процедурою, вимагає менш строгого захисту, ніж вразливі дані, які було зібрано через загрозу і використовуються розвідувальною агенцією без надання суб'єктові будь-якої можливості звертатися до прослуховування чи оприлюднення з обох боків. Для першої категорії захист шляхом вищезгаданої підписки дослідників є достатнім – можливо навіть без застереження, що будь-яка спроба опублікування має бути подана на розгляд архівним працівникам. Саме тому це значить, що відповідальність за законність використання персональної інформації покладається на дослідника, який повинен дати підписку про неопублікування будь-яких матеріалів, що могли б несправедливо зашкодити інтересам живих осіб.

Однак для такої категорії персональної інформації, як у другому випадку, класична підписка дослідника є, як ми гадаємо, недостатньою. Не так через те, що персональна інформація може бути вразливою, як через те, що в другому випадку цілісність тристороннього зв'язку: держава – державна агенція – громадянин буде значно послаблена. Послаблення цілісності вимагає від цієї трійці посилення захисту щодо персональної інформації. Захист цілісності зв'язку між громадянином і державою витікає з обов'язку архівних працівників гарантувати цілісність архіву, вважає Гізер МакНейл, інший канадський колега, який присвятив своє дисертаційне дослідження етиці оприлюднення персональної інформації з публічних архівів[42].

Цілісність, об'єктивність і неупередженість – ось ключові слова в *Міжнародному етичному кодексі* Міжнародної ради архівів. Історики також мають кодекс, наприклад, *Стандарти професійної поведінки* Амери-

[41] Cook, The archival appraisal, p. 44

[42] H.MacNeil, Without consent, p. 174

канської історичної асоціації[43]. Цілісність є також одним із пунктів у їхньому кодексі поведінки.

Цілісність, моральна чистота дослідження мають формувати основу для строгого захисту персональної інформації, для якої звичайної підписки дослідників про нерозголошення недостатньо. Це не та справа з приводу якої дослідник може самостійно прийняти рішення. Це питання об'єкта і методу дослідження. Так само як у кримінальному судочинстві результат не виправдовує будь-які засоби, історичне дослідження також має свої обмеження[44]. Вони повинні бути визначені шляхом міжпредметного тестування у процедурі етичного розгляду, як це звичайно робиться в медичних дослідженнях і як це було описано МакНейлом про архівні дослідження на основі американської і канадської практики[45].

На противагу МакНейлу, однак, я не вважаю, що тестування історичного дослідження через призму кодексу поведінки для дослідників – первинне завдання архівних працівників. Роль архівних працівників, на мою думку, обмежується оцінкою персональної інформації у відповідності до моделі Кука. Оцінювання архівів є спеціальністю архівного працівника. Але оцінка досліджень це не його/її завдання: це належить до професійної сфери істориків за допомогою етологів і правників. Це не те саме, що сказати, що архівні працівники не повинні займатися перевіркою дослідження оскільки його/її досвід корисний для зрівноваження приватності і оприлюднення, права забути і права знати.

Їхній професійний кодекс вимагає від архівних працівників поважати приватність, особливо осіб, які нічого не кажуть про використання чи місце призначення архівних матеріалів. Цього можна лише досягти у відносинах довіри з дослідниками, для яких існують публічні архіви, підтримуються і робляться доступними для використання. Від обох груп – архівних працівників і дослідників – очікується, що вони знатимуть, як чинити з дилемами, які самі представляють, на кшталт колізії цінностей індивідуальної автономії і свободи досліджень.

---

[43] Надруковано в Perspectives, September 1987, p. 4-6

[44] H.MacNeil, Defining thelimits p.143-144

[45] H.MacNeil, Without consent, p.201

Антоніо Ґонзалес Куінтана

АРХІВИ СЛУЖБ БЕЗПЕКИ КОЛИШНІХ РЕПРЕСИВНИХ РЕЖИМІВ

Звіт підготовлено для ЮНЕСКО від імені Міжнародної Ради Архівів

ВСТУП

Цілі

У 1993 році під час круглого столу конференції, що проходила у Мехіко, Міжнародна Рада Архівів вирішила створити групу експертів для обговорення проблем, пов'язаних з архівами колишніх репресивних режимів і скласти серію рекомендацій щодо того як обійтися з такими архівами.

Метою було досягнення практичних результатів. Неможливо надати набір правил, прийнятних у всіх випадках, тому що кожний процес політичних змін відрізняється, але через відкриту дискусію в цій групі було б можливе забезпечення архівних працівників країн, що переживають процес демократизації, інформацією щодо рівня проблем, з якими вони повинні будуть зустрітися. В той же час було б надано список методів, розвинутих в різних країнах, які були залучені до подібного процесу.

Експерти також поставили за мету виявити положення, щодо яких існує згода, і які б містилися в рекомендаціях робочої групи, від чисто архівних до суто політичних, які архівні працівники повинні активно підтримувати, незважаючи на те, що вони не належать до сфери їхньої компетенції.

Експерти також враховували той факт, що архівні працівники, які мають справу з документами, працюють з дуже вразливим матеріалом. Саме тому видається важливим запропонувати етичний кодекс для роботи з такою документацією. Цей кодекс включено до цього звіту.

Робоча група розпочала роботу зі збору інформації про архіви репресивних інституцій для того, щоб скласти список цих інституцій. Без сумніву, первинною вимогою збереження цих документальних свідчень є збільшення обсягу знань про їхнє існування. Група розпочала з інформації, наданої її членами, щодо їхніх власних країн, до якої було додано інформацію від колег з обмеженої кількості інших країн (Зімбабве, Латвія, Литва, Парагвай, Польща і Португалія).

У перший список, який робоча група створила спочатку, було вирішено, в принципі, включити лише репресивні інституції, які зникли між 1974 і 1994 роками у таких країнах: Бразилія, Зімбабве, Іспанія, Латвія, Литва, Німеччина, Парагвай, Південно-Африканська Республіка, Польща,

Португалія, Росія, Угорщина і Чилі. Хоча інформація, отримана від цих країн, була неоднаковою за обсягом, вона все ж включала назви основних джерел, граничні дати документів, що зберігаються, стан їхнього зберігання, приблизний обсяг, а там, де це можливо, ще й зв'язок між основними документарними серіями, що містяться в архівах. Група також відчувала, що певний інтерес могло б представляти додавання практичної інформації, на кшталт використання цих документів за нового політичного режиму і умови такого використання. Це дозволило провести попередню статистичну оцінку, яку група вважає цінною.

Не вся зібрана інформація може включатися у дане дослідження через брак місця. Однак короткий виклад інформації дано в розділі 5, названому «Путівник по джерелах репресій: огляд архівів колишніх репресивних інституцій у нових демократичних державах (1974 – 1994)». Група сподівається, що цей короткий звіт підніме обізнаність у країнах, що знаходяться у процесі переходу до демократії, щодо важливості предмета і ролі архівних працівників.

Нарешті, усвідомлюючи величезне завдання, що стоїть перед професіоналами, що керують такими архівами, група включила до своїх висновків список пропозицій для міжнародної спільноти. Вони послужать зростанню обізнаності на міжнародному рівні у потребі управління документальним спадком. Саме це дослідження є елементом такого знання. Це дослідження також включає коротку бібліографію та перелік відповідного законодавства.

РОБОЧИЙ ПЛАН І МЕТОДОЛОГІЯ

Група, яка фінансувалася ЮНЕСКО, була створена в лютому 1994 року і включала архівних працівників, досвідчених у роботі з цим типом архівів чи архівної етики, разом з експертами у сфері прав людини. Члени групи були обрані з тим, щоб гарантувати рівне представництво країн Центральної і Східної Європи, Латинської Америки, Африки і Західної Європи, залучених до політичних змін. Загальну відповідальність за проект ніс Антоніо Ґонзалес Куінтана, який був Директором секції Громадянської війни Національного Історичного Архіву Саламанки (Іспанія) з 1986 по 1994 роки. Інші члени: доктор Даґмар Унвергау, директор Архіву Штазі у Берліні (Німеччина), Лазло Варґа, директор Муніципального архіву Будапешта (Угорщина), Володимир Козлов з Державного архіву Російської федерації у Москві (Росія), Алеандро Ґонзалес Поблєт, президент Національної комісії з відшкодування і примирення з Сант-Яго (Чилі), Нарісса Рамдані, директор Архіву Африканського національного конгресу у Йоганнесбурзі (Південно-Африканська Республіка) і Мері Ронан з Національного архіву Сполучених Штатів Америки.

Група провела свою першу зустріч у штаб-квартирі ЮНЕСКО в Парижі у 1994 року. На першій зустрічі було прийнято попередню заяву про наміри й першу заяву про цілі та робочий план. Група знову зустрілася в

лютому 1995 року у Коблензі (Німеччина), щоб зібрати разом результати роботи, виконаної її членами, і особливо постаратися обговорити проблему оцінки документів. Останню зустріч було проведено у Саламанці (Іспанія) у грудні 1995 року для того, щоб схвалити кінцевий текст звіту після двох років роботи. Для того щоб збирати інформацію, члени групи склали коротку історію більшості недавно діючих репресивних інституцій у їхніх країнах, і як опис того, як вони [країни] вчинили з архівами цих інституцій. Дані, зібрані таким чином, були дуже корисні для редагування остаточного звіту, але група також поширила єдиний запитальник для того, щоб зібрати інформацію в синтетичній формі, придатній для використання архівними працівниками в інших країнах. Запитальники було складено для того, щоб зібрати інформацію, яка б склала частину «Путівник по архівах репресій».

Архіви репресій: соціальна проблема, яка перевищує компетенцію адміністрації архівів

1980-і мали вигляд неперебірного процесу демонтажу репресивних політичних режимів у всьому світі.

Серед країн Центральної і Східної Європи, які були в орбіті Радянського Союзу з часу Другої світової війни, у світі, розділеному Холодною війною, процес розпочався стартом з Польщі, досягнувши кульмінації у 1990-их тотальним колапсом існуючих політичних структур. Найбільш символічним елементом цього процесу було падіння Берлінської стіни і возз'єднання Німеччини.

Паралельно з цими подіями в Європі, в Латинській Америці розпочалися інші безупинні процеси знищення репресивних політичних режимів. Це були консервативні військові диктатури, які панували практично на всьому континенті, в деяких випадках більше ніж п'ять десятиріч, хоча у певних країнах вони перемежовувалися з більш чи менш стабільними демократичним інтервалами.

У той же час в іншому місці Африканський континент побачив, після періоду тривалої боротьби, кінець режиму, що базувався на репресіях політичної влади щодо певних рас чи етнічних груп. Він видозмінювався від демократизації у Зімбабве до поворотного пункту повалення режиму апартеїду в Південній Африці.

Нарешті, 1970-і роки побачили зникнення консервативних диктатур Західної Європи: Португалія, Греція і Іспанія. Відбувшись на ранній стадії загального процесу, описаного вище, демократичні зміни в цих трьох країнах призвели до трьох дуже різних варіантів досвіду, але кожний має значну цінність для згадуваних цілей.

Дане дослідження охоплює період трохи більше ніж двадцять років між «Революцією гвоздик» у Португалії в квітні 1974 року до кінця режиму апартеїду. Це не тому, що не представляє інтересу розгляд подій, що сталися раніше, до середини 20-го століття, кінець італійського фаши-

зму чи падіння німецького нацизму, і про ці обидва періоди ми будемо згадувати далі в тексті. А тому, що тільки використання найбільш недавнього досвіду може встановити точку відліку, чинну у світовому політичному контексті на початку 21-го століття.

Якби ми пішли б навіть далі, до початків сучасних держав, ми могли б побачити перші приклади влади, яка спеціалізувалась на репресіях, з яких найвідомішим була іспанська інквізиція. Цілком імовірно, що архіви цієї організації були предтечею сучасних архівів репресій. Важко переоцінити величезне значення, яке має належне збереження цього архіву для істориків сучасних держав. Фактично Національний Історичний Архів у Мадриді (Іспанія) зберігає записи Верховного Конгресу Інквізиції, так само як і більшість записів Окружних Трибуналів, створивши незрівнянне джерело для вивчення не тільки владних зв'язків монархів Іспанії, але також менталітету і культури Відродження в усій Європі.

Очевидно, що репресивні режими поширювались від початків сучасної держави. В архівах у всьому світі існують документи, які це доводять. Предмет цього дослідження – архіви і недавні репресивні режими – таким чином, має величезну соціальну і політичну важливість. Такі архіви, які були основою для виконання репресивної діяльності, перетворені за нового політичного режиму (який приніс свободи і відповідальність, проголошені Загальною декларацією прав людини) у важливий засіб надання можливості встановлення нових соціальних зв'язків. У цьому розумінні ефект бумеранга, що демонструється документами, які уціліли, є як нетиповим, так і унікальним, і вимагає, з професійної точки зору, обережної концепції управління цими архівними фондами. У той же час він приніс цілком нові обов'язки для архівних інституцій.

Архіви мають вирішальний вплив на життя людей. Ніщо не слугує цьому кращим прикладом, ніж спосіб, у який використовувалися документи, щоб послужити припиненню репресій. Образ архівів служб безпеки у репресивних режимах ясно ілюструє наскільки важливими вони є. Протягом життя таких режимів, жертви політичних інформаційних служб могли відчувати важливість архівів, але тільки з настанням демократії і відкриття джерел сталося те, що громадяни стали повністю обізнані у їхньому впливі на життя людей.

Основна роль, яку відіграють архіви, характеризується не лише їхніми функціями, на кшталт ключів до нашого недавнього минулого, але також їхнім адміністративним значенням у дотриманні прав особи. Це проявляється тоді, коли демократичні режими бажають, наприклад, проголосити амністію за так звані думкозлочини або видати компенсацію жертвам репресій чи їхнім родинам. Досвід Німеччини та Іспанії добре це ілюструє. Немає сумнівів, що історичний вимір є надзвичайно важливим, але соціальний вплив, який архіви можуть мати, надає їм найважливішу публічну роль. Серед найбільш знаних архівів Іспанії є без сумніву Секція Громадянської війни Національного Історичного архіву у Саламанці,

що надала десятки тисяч сертифікатів громадянам, які колись були членами армій і органів безпеки Республіки чи адміністрації Республіки і стали пізніше жертвами франкістських репресій. Іншим важливим прикладом є архіви колишнього Штазі у Берліні.

ЗАГАЛЬНІ РОЗДУМИ І РЕКОМЕНДАЦІЇ

Причини зберігання документальних джерел вивчення репресій

Першим питанням у кожному обговоренні, що стосується архівів колишніх державних інституцій безпеки, у країнах, які знаходяться в процесі переходу до демократії, є: зберігати їх чи ні. Всі пізніші дискусії про їхній архівний обіг, про їхнє використання громадянами і новою адміністрацією чи про професійну етику стосовно їхнього змісту залежить від відповіді на це перше питання.

Існують приклади країн, у яких всі типи архівів служб безпеки, створених режимами, що передували демократичним, збережені майже цілковито. Існують також протилежні приклади, коли не залишалося жодного документального свідчення репресій чи, принаймні, ніхто не знає про їхнє існування. Середній шлях пройшли країни, які спершу використали документи з адміністративними цілями, а тоді знищили їх з етичних міркувань.

Прикладом другого типу в іспаномовній Південній Америці є Чилі. Невідомий жоден документ основних репресивних інституцій військової диктатури, чиєю основною складовою була DINA, а її наступником CNI. Таким чином на початку процесу переходу, коли очевидною була потреба знати правду про політичне насильство, зникнення і убивства, скоєні режимом Піночета, існувала величезна перешкода, спричинена браком документальних доказів. Комісія з Правди і Примирення – перший орган свого типу, створений у 1990 році, зіткнувся з завданням реконструкції 15 років історії країни майже виключно на основі персональних свідчень, базованих на словесних чи письмових спогадах тих, хто був залучений до цих подій. Комісія, яка досягла зростання рівня обізнаності щодо зловживань владою колишнім режимом, не в змозі пролити світло на долю багатьох зниклих осіб чи назвати осіб, відповідальних за звірства. Досвід Чилі є повчальним: тими, хто поніс найбільші втрати від зникнення документів, були чилійці, а тими, хто найбільше виграв, були агенти, які проводили репресії, а особливо їхні керівники. Безсумнівно, чилійський шлях до демократії проходить через примирення, однак можливість притягнення злочинців до відповідальності за їхні злочини значною мірою зникла.

Подібний випадок можна знайти у Південній Африці, де Національне Розвідувальне Агентство продовжує залишатися організацією, відповідальною за документи, вироблені ним самим у минулому.

В Іспанії одне з документарних джерел, чиє місцезнаходження невідоме (якщо вони не знищені) стверджує, що служба охорони голови уряду під контролем полковника Сан Мартіна працювала як служба розвідки в останні роки диктатури.

Чилійський випадок не є виключним. В Африці у період 1979 – 1980 років уряд Родезії знищив документи, створені чотирма найбільш важливими і спеціалізованими організаціями безпеки в останні роки репресивного режиму: Центральна Розвідувальна Організація, підрозділ Спеціальної Поліції, спеціальні суди і армійський підрозділ, знаний як «Зулуські розвідники».

Спадкування у колишній Німецькій Демократичній Республіці (НДР) після падіння Берлінської Стіни і возз'єднання є прикладом протилежного типу. Хоча архіви Штазі в усій повноті не були отримані, принаймні, значну більшість цих архівів було передано. Це стало можливим, попри все, через припущення, що німецький народ збереже їх, якщо знатиме про начала їхньої важливості. Таким чином, негайна передача архівів Штазі в руки нових органів влади, стала можливою для того, щоб слідувати бажанням представників народу, і серед інших завдань – очистити від тих, хто відповідальний за репресії, нову адміністрацію. Архіви було використано як для того, щоб звільнити тих, хто відповідальний за репресії, так і для компенсації жертвам репресій. Зразковими були паралельні процесуальні дії. Це проявилося у двох законах: один у НДР перед об'єднанням і кінцевий закон в об'єднаній Німеччині. Найбільшим прихильником цього був народ. Роль, яку відіграли групи, на кшталт групи преподобного Ґаука, були визначальним фактором. Можливо, німці пам'ятали долю нацистських архівів в кінці Другої світової війни. Потрібно нагадати, що їхнє первинне використання було здійснене суддями Нюрнберзького процесу, хоча у цьому випадку не німецький народ був прихильником процесу, а збройні сили союзників.

Поміж цими двома видами досвіду лежить досвід Греції, яка використала документи репресивних органів протягом кількох років, відразу після диктатури, для виконання адміністративних завдань, на кшталт компенсацій і усунення від влади тих, хто був відповідальним за репресії. Архіви було пізніше знищено згідно з новим законодавством, яке визнало їх, імовірно виходячи з етичних міркувань, небажаним для зберігання в канцеляріях і архівах нагадуванням для людей, діяльність чи позиція яких, визнані незаконними попереднім режимом, і які були реабілітовані. Хоча вони й полегшують усунення від влади осіб, відповідальних за репресії чи виплату компенсацій їхнім жертвам. Це рішення зробило можливим підведення риски під періодом Диктатури і періодом Полковників, але не може бути визнане задовільним з точки зору історичного і документального спадку.

В Іспанії пройшло обговорення: чи знищувати досьє поліцейських архівів, що проливають світло на політичну, профспілкову та ідеологічну

приналежність осіб, які вважались незадоволеними франкістським режимом. Внаслідок анекдотичної події (затримання в аеропорту Мадрида комуністичного депутата Енріке К'юріель через те, що він згадувався в комп'ютерних записах поліції як «таємний активіст»), Парламент Іспанії розглянув пропозицію знищити ці досьє. В результаті було прийнято рішення анулювати комп'ютерні файли поліції щодо політико-соціальної діяльності, які існували з днів колишнього режиму, незважаючи на передачу (у той самий час) всіх файлів політичної природи, що містилися в поліцейських архівах, до Національного Історичного Архіву. Це досягнення стало можливим завдяки Міністрові внутрішніх справ, який був відповідальним за Центральний поліцейський архів, і Міністрові культури, який був відповідальним за Національний Історичний Архів, які підписали разом зобов'язуючу угоду. Таким чином було збережено нерухомою збірку документів щодо вивчення опозиційних соціальних рухів протягом 40 років режиму Франко.

Часто говорилося, що архіви нерідко є найбільш достовірним відображенням історії народу і таким чином визначають найбільш точну пам'ять націй. Це безсумнівно щодо тоталітарного, диктаторського чи репресивного режиму. В таких режимах бракує будь-яких юридичних засобів відображення багатоманітності ідей і поведінки. Тільки архіви, особливо архіви поліції і розвідувальних служб, які контролювали народ, можуть відобразити приховані соціальні конфлікти, притаманні цим режимам. На відміну від публічного образу, який такі режими намагалися представити, їхня справжня природа може бути розкрита у файлах і реєстрах служб безпеки. Існування значних поліцейських архівів є загальною характеристикою таких режимів. Репресивний апарат був загалом дуже великим і характеризувався значним обсягом документів. Через це інформація і про осіб, і про групи збиралася майже щоденно. Це був у багатьох випадках єдиний шлях цього режиму забезпечити свою владу.

У всіх країнах, які пережили періоди політичних репресій, величезний інтерес породжували архіви цих репресій. Історики і журналісти мали законне бажання знати про репресії якомога глибше. Необхідно було забезпечити ці вимоги юридичними гарантіями, що судовий процес не зазнає втручань, у той же час захищаючи приватність жертв репресій, включно з прийняттям закону «останньої крапки» (про амністію[46]).

Аргументи на користь зберігання цих документів мають ясний вигляд. Однак, залишаються значні сумніви стосовно можливості повторного використання документів з репресивними цілями. Коли немає впевненості, що документи було знищено чи передано органам влади, явно відмінних від органів колишнього режиму, як у випадку Чилі, потрібно вважати, що вони можуть знову бути використані проти прав людини. У гіпотетичному випадку повернення репресивного режиму документи мо-

[46] З точки зору українського законодавства краще говорити про реабілітацію. – *Ред.*

гли б бути використаними з негідною метою. В усіх випадках, найкраще, щоб документи згідно із законом знаходилися в демократичній державі і в руках професійних архівних працівників.

На завершення слід сказати, що документи, накопичені органами репресій, важливі для пам'яті народу і служать непорушним свідченням. Але найбільш вагомий аргумент на користь зберігання репресивних архівів новими демократичними державами полягає у важливості, яку такі документальні джерела мають для осіб, що постраждали від колишнього режиму, як для прямих, так і для непрямих жертв. Документи періоду репресій є суттєвими для використання індивідуальних прав: на амністію, на компенсацію, на пенсію і загальні громадянські права (на спадок, на власність...) у новій політичній ситуації.

Ключова роль архівів у політичних змінах

Залежно від шляху, яким рухається демократія, існує декілька альтернативних образів архівів служб безпеки репресивних режимів. Шлях, яким репресивний режим припинив існування, визначає значною мірою майбутнє своїх архівів. У процесі «переговорних змін» чи «національного примирення» аргументи про компенсацію жертв стоять вище від усього іншого. У декількох випадках вони навіть вивищуються над вимогами назвати імена осіб, відповідальних за репресії, через так звані закони «останньої крапки» в ім'я гаданого бажання соціального миру. У випадку революційного вибуху чи швидкого колапсу системи перша вимога стосується тих, хто винен. У цьому випадку завдання архівних працівників набагато легше через те, що руйнування системи вимагає нового планування і через зміни в установленому порядку і в особах. Однак у ситуації, коли демократичні процеси вже були розпочаті в часи репресивного режиму, можливо, наприкінці тривалого еволюційного процесу, завжди залишається ряд значних перешкод. Це трапляється, наприклад, коли відповідальні особи з попереднього режиму активно сприяли процесу репресій, але продовжують займати свої посади.

Як уже зазначалося, жодні два випадки змін не є повністю схожими, але як ілюстрацію може бути розглянуто дві альтернативи: німецький випадок з архівами Штазі та іспанський випадок з архівами репресивних інституцій періоду Франко. Це цілком відмінні типи змін із різних вихідних позицій. Німецький випадок був результатом тотального колапсу режиму, а іспанський – результатом тривалого періоду змін, розпочатих в період самого режиму Франко, уникнувши повного руйнування «законності».

Під час політичних змін архіви є основним засобом втілення в життя колективних та індивідуальних прав. Успіх методів відшкодування і компенсацій жертвам репресій, так само як і усунення відповідальних осіб колишнього режиму, буде значною мірою зумовлений використанням документів репресивних інституцій. Підтримка їхнього збереження і створення інституцій, відповідальних за їхню охорону в новій політичній державі, є визначальними факторами у процесі зміцнення демократії. Серед

фундаментальних функцій архівів у зміцненні як колективних, так і індивідуальних прав виділяють наступні:

КОЛЕКТИВНІ ПРАВА

1. Право народів і націй обирати свій власний шлях політичних змін значним чином визначається доступністю документів. Без архівів немає справжньої свободи вибору. Комісії Правди, як показує досвід Польщі, Чилі чи Південної Африки, тільки тоді можуть задовільно завершити свою роботу, якщо збереглися документальні джерела репресивних інституцій.

У німецькому випадку громадськість визнала важливість архівів Штазі як для планування майбутнього, так і для розуміння того, як минуле зумовлюється діяльністю інформаційних і репресивних служб. На цю позицію значний вплив вчинив спосіб, яким після Другої світової війни управлялися нацистські архіви, коли стало видно важливість їхнього збирання і зберігання у Центрі Порівняльної Документації в Берліні.

2. Право народів на цілісність їхньої писаної пам'яті повинно бути незаперечним. Якщо спільнота обирає прощення як засіб досягнення політичних змін, результатом цього не повинно стати зникнення документального спадку минулого. Нації мають як права, так і обов'язки зберігати свою пам'ять шляхом передачі їх до архівів. Хоча кожне покоління повинно бути вільним обирати політичні процеси, за які вони відповідальні, вони не можуть обрати за інші покоління. Право на вибір шляху політичних змін виключає право знищувати документи.

3. Право на правду. Громадяни мають тісно пов'язане з цими обома правами право на найповніше можливу інформацію про дії попереднього режиму чи через їхніх парламентських представників, чи через будь-яку іншу систему, які можуть вважатися адекватними цим представникам. Це є основою, на якій працюють усі так звані Комісії Правди, на кшталт Комісії за Правду і Примирення у Чилі, Комісія Правди і Примирення Південної Африки чи Верховна Комісія з досліджень злочинів проти польської нації у Польщі.

4. Право визначати осіб, відповідальних за злочини проти прав людини. Право визначати агентів репресій повинно визнаватися незалежно від будь-яких інших рішень стосовно відповідальних осіб чи можливе продовження їхньої праці в якості державних службовців. Політика амністії чи прощення щодо посадових осіб, відповідальних за порушення прав людини, була прийнята різними країнами у процесі переходу до демократії з метою досягнення національного примирення. Однак, у демократичній державі народ має право знати імена посадових осіб, відповідальних за порушення прав людини у колишніх режимах, для того, щоб гарантувати, що вони не робитимуть політичну кар'єру. Вже згадуване законодавство Німеччини врегульовує, яким чином це повинно здійснюватися. Закон про записи Штазі дозволяє громадськості чи приватним орга-

нізаціям розслідувати [інформацію про] органи влади, публічних осіб і громадянських представників щодо можливих зв'язків з колишньою репресивною машиною. Сфера розслідування обмежена для того, щоб уникнути можливого залишення при владі агентів і співробітників Міністерства внутрішніх справ через незнання. З іншого боку законодавство обмежує використання цього права, якщо ті, щодо кого проводиться розслідування мали менше ніж вісімнадцять років на момент, коли, як припускається, правопорушення мало місце. Рівною мірою існує обмеження розслідування в часі, яке складає п'ятнадцять років з моменту оприлюднення закону (до 2006 року).

ІНДИВІДУАЛЬНІ ПРАВА

1.Право досліджувати долю родичів, які зникли під час періоду репресій. Одним з найгірших наслідків репресій є незнання долі родичів чи друзів, які зникли. Архіви репресій повинні дозволяти розслідування, і якщо можливо – прояснення таких випадків.

2. Право знати, яка інформація про осіб зберігається в архівах: відомі як «habeas data» (судовий наказ про представлення даних), який гарантує право знати, чи будь-яка інформація про особу знаходилася в поліції або розвідувальних службах колишнього репресивного режиму і оцінювати, у який спосіб можуть вплинути політичні, ідеологічні, етнічні чи расові упередження на персональне, сімейне чи професійне життя. Саме право може також застосовуватися від імені агентів і службовців інституцій репресивного режиму.

3.Право на історичні й наукові дослідження: усі громадяни мають право доступу до джерел вивчення їхньої національної історії. Доступ до таких документів повинен враховувати потребу захисту приватності жертв і третіх сторін, згадуваних у документах.

4. Право реабілітації для ув'язнених і репресованих з політичних мотивів: у кожному процесі переходу до демократії, ті, хто був засуджений судами чи звільнений з їхньої роботи суто з політичних, релігійних, етнічних чи расових причин, повинні бути звільнені з-під ув'язнення, поновлені на їхній роботі чи повинні отримати компенсацію. Часто існує ситуація, що тільки серед архівів колишніх репресивних режимів можуть бути знайдені докази політичної, релігійної, етнічної чи расової природи засудження чи звільнення.

5. Право на компенсацію і відшкодування збитків, завданих жертвам репресій. Коли органи влади нових демократичних режимів вирішать надати компенсацію жертвам репресій, документи, вироблені інституціями колишнього режиму, забезпечать їх необхідними доказами.

6. Право реституції конфіскованого майна. Коли громадяни нової демократичної держави мають юридичне право повернути особисте майно, конфісковане попереднім режимом за їхні переконання чи ідеологію,

документи в архівах репресивних органів дадуть детальний опис такого майна, так само як і інформацію про їхнє місцезнаходження чи місце призначення. Якщо реституція неможлива через те, що майно зникло чи має нових, законних власників, архіви доведуть їхнє право на відповідну компенсацію.

Необхідність законодавчої бази для архівів репресій

У процесі політичних змін законодавець повинен узяти до уваги архіви і інструментальну роль, яку вони відіграють у створенні нового законодавства. Приклад Іспанії свідчить про те, як практичне застосування законодавства про амністію, виплати і компенсації тісно пов'язане з документальними свідченнями, які створюють підстави для застосування цих законів. У процесі, що відбувається відразу після краху репресивного режиму, архівні працівники повинні брати до уваги законодавство, а також зміни, що сталися, для того щоб гарантувати, що права є життєздатними в новій ситуації.

Будучи свідомими цієї необхідності і вагомої ролі документів репресій, архівні працівники всіх країн, від найвищих органів влади архівів до простого архівного працівника, повинні виявити ініціативу в юридичному процесі в їхніх власних країнах для охорони вищезгаданих колективних та індивідуальних прав і будь-яких інших, які можуть з'явитися, через наступні юридичні засоби:

Записи, створені чи накопичені репресивними органами, повинні бути передані під контроль нових демократичних органів влади за першої-ліпшої можливості, і ці органи влади повинні детально регламентувати їхнє зберігання. Демократичні органи влади повинні створити комісії, відповідальні за управління цими сховищами, і архівні працівники повинні бути тісно залучені до роботи комісій. Комісії повинні також нести відповідальність за архіви розвідувальних служб, які продовжують діяти при новому режимі. Комісії повинні обрати досьє, які поліція, органи безпеки чи розвідки більше не вимагають зберігати для виконання своїх обов'язків при демократичному режимі. Органи безпеки повинні забезпечити передачу обраних досьє і документів чи то до національних архівів, чи то до інституцій, що мають справу з компенсаціями або виплатами жертвам репресій, або усуненням колишніх посадових осіб, чи то до Комісій Правди.

Документи колишніх репресивних органів повинні зберігатися в архівних установах національної системи архівів або в інституціях, створених для ідентифікації колишніх посадових осіб, компенсації жертвам репресій чи забезпечення колективних та індивідуальних прав. Другий спосіб вирішення є більш бажаним, ніж перший, як про це свідчать німецька і португальська моделі, на противагу одній іспанській. Висока кількість запитів може призвести до краху традиційної діяльності архівів, які зага-

лом не дуже добре забезпечуються коштами чи персоналом. Саме тому тимчасові інституції, на які покладається ця відповідальність, мають формуватися із спеціально призначеного для цих спеціальних завдань персоналу. Це поліпшить якість забезпечення цих служб, у той час даючи можливість постійно діючим архівам виконувати свої традиційні обов'язки. Той факт, що ці установи є тимчасовими, повинен бути ясно встановленим. Кінцевим місцем знаходження документів, як частини національної пам'яті, повинно бути національне сховище (репозиторій) історичних записів.

Може бути необхідним встановлення спеціального законодавства для захисту документів колишніх репресивних організацій в якості культурної власності. Якщо законодавство, що захищає культурний спадок, уже існує, то ці документи повинні ними охоплюватися. Якщо чинні норми охоплюють зберігання документального спадку в архівних установах, то передача записів до цих установ гарантує, що вони стануть культурною власністю, що захищається. В будь-якому випадку характер документів як культурної власності повинен бути чітко визначеним.

Для того, щоб гарантувати права осіб засобами архівів, необхідні відповідні юридичні ініціативи – чи то новий загальний закон про державні архіви, чи то внесення відповідних змін до існуючого закону. Права, що мають бути таким чином гарантовані, охоплюють:

право всіх осіб вимагати доступу до архівів для того, щоб дістати інформацію про існування чи неіснування будь-якої інформації чи документів стосовно них, завжди передбачаючи, що приватність третьої сторони гарантується;

право для осіб, що не були на службі в репресивних органах, визначати, чи записи, що містять персональну інформацію, можуть враховуватися третьою стороною. Персональні досьє жертв репресій повинні бути закриті від публічного доступу протягом законно встановленого періоду, за винятком спеціального дозволу особам, яких вони стосуються, чи їхніх спадкоємців. Особи повинні мати можливість внести зміни чи заяву щодо інформації, яка міститься про них у персональних досьє. Вони повинні бути включені в досьє, але чітко відділені від документів, що зберігалися репресивним режимом, і які не повинні змінюватися;

право вимагати доступ до файлів агентів репресій на основі гарантій безпеки, встановлених законодавством.

Необхідність розголошення інформації про архіви репресивних режимів

Кульмінацією процесу є складання повного звіту з наданням деталей прав, встановлених новими державами, так само як поширеність архівів та інституцій, з ними пов'язаних. Необхідно залучати не тільки відповідні інституції державної адміністрації, але повинні бути запрошені до уча-

сті також усі ті, кого це стосується: політичні партії, профспілки, релігійні організації, фонди і правозахисні організації. Також важливим є залучення ЗМІ, переважно радіо і телебачення.

Необхідність прийняття Етичного Кодексу для архівних працівників, які наглядають за документами репресій

Складання Етичного Кодексу може бути великою допомогою, якщо відображає управління записами, що обговорювалися в цьому звіті. Архіви, відповідальні за переховування цих записів, повинні встановлювати такі кодекси. Особливо важливим є те, щоб архівний персонал, який продовжує службу з часів колишнього режиму, чітко погодився з цими принципами. Етичний Кодекс повинен включати наступні пункти:

документи репресій є частиною спадку нації; вони повинні бути збережені в їхній цілісності, слугуючи нагадуванням про нетерпимість, расизм і політичний тоталітаризм;

архівні працівники є виконавцями волі народу в юридичних процесах, обраних для змін; вони самі повинні повністю дотримуватися закону;

індивідуальні права жертв політичних репресій мають першість перед історичним розслідуванням;

архіви не повинні розміщати будь-які документи на підставі критерію відбору, що базується на їхній цінності для історичного дослідження;

архівні працівники не є цензорами; закон визначає, які документи повинні бути доступними і як це повинно відбуватися;

якщо законодавство недостатньо конкретизоване, архівні працівники можуть тлумачити його на підставі юридичних коментарів експертів адміністративного права; у випадках, коли приватність особи і право на історичне розслідування протистоять одне одному, може бути передбачено рішення щодо використання копії оригінального документа з видаленим іменем жертви чи третьої сторони;

архівні працівники повинні поводитися з найбільш можливою обережністю з усіма запитами щодо посвідчення чи легалізації фотокопій, що використовуються для того, щоб надати юридичну силу скарзі жертв репресій чи інших осіб;

архівні працівники повинні встановити контроль, необхідний для захисту документів, що містять вразливу інформацію. Документи репресій повинні зберігатися в загальних архівах, але в окремих спецсховищах і з спеціальними заходами безпеки; тільки персонал архіву повинен мати доступ до цих документів;

архівні працівники повинні обмежити використання автоматизованих баз даних стосовно жертв репресій тією мірою, якою це необхідно для використання «habeas data». Ці бази даних повинні використовуватися лише як допомога при пошуку. Не повинно дозволятися жодне адміністративне чи урядове їх використання.

ЗАГАЛЬНІ ЗАУВАЖЕННЯ І РЕКОМЕНДАЦІЇ

В якості загального правила основні архівні принципи також чинні для архівів репресій. Архівні працівники можуть бути схильні встановити нову класифікацію записів репресивних інституцій, особливо таємних служб, які можуть видаватися неорганізованими. Однак за видимою відсутністю організованості може бути приховано логіку організації, відображену в специфічній структурі документальних фондів. У цих справах повинні підтримуватися принципи «поваги фондів» («respect des fonds») і зберігатися початковий порядок. Основним обов'язком архівних працівників є, в цьому разі, розуміння динаміки функціонування цих інституцій і відображення їх у класифікаційних схемах та описах архівів.

Ідентифікація фондів

Найперше архівне завдання – ідентифікація фондів. Архівні працівники повинні знати, яка агенція, організація чи орган створили збірку документів, з якою вони мають справу. Історична еволюція організаційних структур і обов'язків повинна бути проаналізована разом з її органічною і адміністративною залежностями .

Ключ до організації архівів будь-якої інституції лежить у правильному аналізі її структур і юрисдикції. Класифікація документів без такого попереднього аналізу була б важкою і невідповідною. Первісний порядок документів був відповідним для самої організації, тобто для виконання нею репресивного завдання. Парадоксально, але найбільш дієвою була організація документів з політичною метою, найбільш ефективним є використання архівів для реабілітації і компенсації щодо громадянських прав за нового політичного порядку, якщо збережено їхній первісний порядок. Саме тому ідентифікація фондів починається з вивчення положень і внутрішніх норм, які регулювали діяльність організації протягом усього періоду її існування.

Рекомендується, щоб ідентифікація фондів проводилась архівними працівниками, які є членами вже згадуваних комісій ліквідацій (дивись загальні рекомендації), перед тим як їх буде передано до архівних установ. Неконтрольована передача документів може непоправно спотворити первісний порядок архівів.

Різноманітність репресивних органів настільки велика, що визначити обсяг терміна «репресії» нелегко. Поняття репресій стосується не лише політичних ідей, але також охоплює ідеологію і персональну поведінку, релігію, філософські погляди, сексуальну поведінку та інші сфери, які Загальна декларація прав людини відносить до сфери свободи. З огляду на це робоча група ЮНЕСКО – Міжнародної Ради Архівів встановила наступні категорії репресивних органів: (a) розвідувальні служби, (b) воєнізовані органи, (c) спеціальні трибунали, (d) концентраційні табори, (e) спеціальні в'язниці, (f) психіатричні центри з «перевиховання».

Ці заклади спеціально створювались як інструменти репресій. На додаток, репресивні структури можна також знайти в більш традиційних частинах адміністративного апарату, які продовжують існувати після падіння тоталітарного режиму. Для цих випадків експертна група встановила наступні категорії: (a) збройні сили, (b) поліція і органи безпеки, (c) цивільні суди, (d) інші підрозділи цивільної адміністрації.

Розвідувальні служби представляють найбільш характерний тип документації, який значно відрізняється від традиційної організації документів у державних адміністративних органах. Архіви розвідувальних служб особливо багаті на інформації щодо людей і репресивних організацій.

Архіви розвідувальних служб репресивних режимів загалом організовані навколо великої картотеки чи автоматизованого каталогу. Такі каталоги були створені для того, щоб швидко надати інформацію про осіб. Картки в каталозі часто містять детальний опис даних, що містяться в документах. Ці картки, які інколи називаються «такими, що не потребують пояснення», наприклад, у Державному архіві Ріо-де-Жанейро, відрізняються від звичайних карток каталогу, які звичайно тільки ідентифікують документ чи файл у сховищі і не дають додаткової інформації або не відсилають до інших каталогів чи файлів.

Доцільно зберігати файли каталогів в їхньому первісному форматі після передачі документів новим архівним установам. Якщо процес інтеграції цих фондів не дозволяє збереження первісної структури, архівні працівники повинні забезпечити, щоб зв'язок між старим і новим каталогами був ясним.

Часто інформація, що використовується розвідувальними службами, надходить з інших установ чи органів. Використання конфіскованих документів репресивними органами було дуже поширеним. Важливо визначити ті документи, які потрапили до фондів репресивних організацій, але їх не потрібно виділяти в окремий фонд. Автоматизований опис документів може допомогти представити такі матеріали найкращим чином, щоб сприяти історичним дослідженням щодо організацій чи осіб, які вилучили цей матеріал. Комп'ютерне «перетворення» цих документів повинно здійснюватися не згідно з логікою поліції, а слідувати структурі й організації самої інституції.

Особи є основними об'єктами досьє розвідувальних служб репресивних режимів. Інформація про цих осіб може міститися в простих чи складних досьє. Однак, інформація про ту ж саму особу, наприклад, короткий опис у картках, «що не потребують пояснення», там де вони існують, чи картки з посиланнями, повинна завжди зберігатися разом. Документи, на які ці картки посилаються, складають документальний доказ будь-якої скарги чи адміністративного або судового рішення. Таким чином, дуже важливо, щоб зв'язок між картками і документами не розрива-

вся; повне розуміння організації документів розвідувальних служб залежатиме від карток чи автоматизованих каталогів.

Визначення серій документів репресивного характеру, які можуть все ще існувати в адміністративному апараті демократичної держави-спадкоємиці, є набагато важчим. У таких випадках досьє, пов'язані з репресіями, повинні бути відділені від решти шляхом їхньої чіткої ідентифікації. Будучи раз виділеними, ці файли чи їхня група можуть бути визнані закритим фондом, і може бути гарантовано їхню передачу і постійне зберігання в архівах державних адміністративних органів. Дуже важливо підкреслити, що ця процедура не рекомендується для інших фондів. Вона рекомендується лише тут через те, що у цих файлах міститься делікатна інформація політичної і соціальної природи. Дані повинні визначатися відновленням цілісності фондів, маючи за довгострокову мету, щоб у майбутньому цілісність фондів було відновлено і щоб усі файли репресивних організацій зберігалися в одному сховищі. Якщо це не зроблено, для наступних поколінь залишиться враження, що ці інституції непричетні до політичних репресій у недемократичні періоди.

ОЦІНКА

Існує два основних оціночних завдання для архівних працівників, які працюють із записами репресивних організацій:

вивчення різних документальних груп для того, щоб визначити їхню цінність для захисту прав особи і їхню цінність як доказ для історії репресивного режиму і країни загалом;

вибір файлів, пов'язаних із порушеннями прав людини з метою відділення їх від решти документів нейтральних агенцій, які продовжують існувати при демократичному режимі.

Ці завдання можуть бути описані як оцінка закритих фондів і оцінка відкритих фондів.

У випадку оцінки закритих фондів різні серії повинні спершу бути ідентифіковані, а тоді необхідно визначити їхню цінність, беручи до уваги юридичний, адміністративний та інформаційний критерії. Стосовно юридичної цінності документів, основним критерієм повинні бути автентичність і точність. Багато документальних серій, створених протягом періодів репресій характеризувалися відсутністю легалізації (підписів чи печаток). Саме так, наприклад, сталося з уже згадуваними «картками, що не потребують пояснення». Значна кількість звітів і документів у цих досьє, можливо, не мають юридичної цінності як доказ у демократичному судовому процесі. Немає сумніву, що інформація, яка в них міститься, є в багатьох випадках чистим вимислом. Однак вони є автентичними документами. В демократичний період документи колишніх режимів стануть автентичним і точним доказом дій, що застосовувалися проти людей з політичних, ідеологічних, релігійних, етнічних і расових мотивів. Таким

чином вони будуть чинними документами для використання таких прав як амністія, відшкодування чи компенсація жертвам репресій.

Але в деяких випадках докази переслідування, підтверджені документами, не визнаються достатніми для отримання відшкодування чи компенсації. Можуть існувати закони, як, наприклад, в Іспанії, що встановлюють, що право на компенсацію буде визнано лише тим особам, які були ув'язнені більше ніж протягом трьох років. Для виконання цих юридичних вимог тільки юридичні документи, що дають доказ анулювання вироку, можуть надати право на доступ до компенсації, яка забезпечується законодавством. Саме тому архівні працівники повинні бути обізнані із законами, які регулюють права громадян, для того, щоб визначити найбільш відповідні записи в кожній індивідуальній справі. Це також впливає на рішення про те, які записи повинні описуватися більш детально і який порядок пріоритетів повинен бути в описовій роботі.

Персональні файли агентів і службовців адміністративних органів і служб репресивних режимів, особливо служба записів військових кадрів, мають особливе значення, тому що вони містять біографічну інформацію, яка могла б бути критичною у визначенні їхньої відповідальності під час репресій.

Усі файли, що містять інформацію про осіб, які були жертвами репресій повинні бути збережені через їхню первинну цінність як доказ у питанні щодо прав людини протягом, принаймні, 75 років від дати створення. Оскільки ці записи мають також значну історичну цінність для знання про дійсний обсяг репресій, вони повинні розглядатися як записи для постійного зберігання.

У випадку оцінки відкритих фондів критерій відбору для відділення досьє від чинних документів організації повинен базуватися на типі злочину. Досьє щодо осіб, підозрюваних чи звинувачених у злочинах, які вони ніколи не скоювали чи які юридично не були визнані злочинами в новій демократичній державі, повинні бути передані до загальних архівів. Критерій відбору має бути настільки загальним, наскільки це можливо, і якщо виникають сумніви щодо їхнього включення, досьє повинні бути передані до загальних архівів. В Іспанії досьє центрального поліцейського архіву цієї категорії були передані до Національного Історичного Архіву. Для того, щоб це зробити, необхідно чітко визначити, які типи звинувачень політичних опонентів чи звичайних громадян були пред'явлені репресивними режимами і які відсутні в судовій практиці демократичних країн. У досьє фігурують такі «злочини», як: загроза органам влади, загроза особам, потурання тероризму, участь у недозволеному об'єднанні, терористичний акт, співпраця з бандами, участь у незаконній організації, опір особливому законодавству, опір внутрішній службі державної безпеки, завдання шкоди, зберігання зброї і боєприпасів, непокора, незаконне затримання осіб, керівництво воєнізованою організацією, організація

заколоту, втеча з-під варти, страйк, друк, стрілянина, порушення військового статуту, виступи проти уряду, порушення громадського порядку, завдання шкоди органам влади, незаконний збір інформації, відмова від військової служби, таємний перетин кордону, участь у банді, незаконне видання і пропаганда, порушення відбування вироку, повстання, опір, незаконні мітинги, заклики до повстання, зберігання зброї і вибухових речовин, тероризм і образа країни (нації), її символів і прапора.

Щодо відкритих фондів також потрібно врахувати документи з обмеженим доступом, пов'язані з репресіями прав людини, визнані таємними. Це буде можливим тільки в тому разі, якщо Комісії, які займаються аналізом документів цих інституцій, не будуть зустрічатися з перешкодами в них. Очевидно, всіх членів Комісії стосується законодавство про державну таємницю стосовно їхньої свободи дій у використанні державних таємниць, для якого вони повинні мати відповідний дозвіл.

Принцип джерела

Нетиповий характер документів розвідувальних служб, у порівнянні з іншими репресивними інституціями, на кшталт трибуналів, в'язниць, лікарень тощо, вже підкреслювався. Вони часто містять вилучені документи, що стосуються осіб, цивільних інституцій чи політиків, які були об'єднані з матеріалами інших джерел, на кшталт газет, звітів агентів тощо, в одному досьє. Коли документи розвідувальних служб передаються до загальних архівів нової демократичної держави, необхідно поважати це джерело розвідувальної агенції.

Цілісність фондів

Не тільки джерело, але і цілісність фондів має поважатися. Якщо закон передбачає повернення особистого майна особи, це право може вступити у протиріччя з принципом цілісності фондів. Якщо особи вимагатимуть досьє у значній кількості, це може піддати небезпеці існування фондів, загрожуючи частині національного спадку.

Компромісне рішення може бути прийняте шляхом розрізнення суто особистих документів, що повинні бути повернуті їхнім власникам чи їхнім нащадкам, і документів, що стосуються діяльності осіб у їхній громадській або політичній ролі, які повинні постійно залишатися в архівах. Повинно бути визнано право на фінансову компенсацію власникам цих документів чи їхнім нащадкам, забезпечивши, щоб такі документи не було розміщено в публічних архівах. У той же час можна рекомендувати, що в разі, якщо особи, яким повернуто майно, вирішать їх передати третій стороні, держава повинна отримати право пріоритетного набуття.

Концепція «фондів» також повинна бути визнана у випадку з підрозділами поліції та армії спеціального призначення репресивного апарату. Доцільно розглядати записи цих спеціальних органів в якості окремих фондів, і саме тому передати їх до загальних архівів.

Існує лише одне виключення з принципу збереження цілісності фондів. Це відбувається там, де досьє репресій знаходяться разом з досьє, які потрібні для продовження діяльності органу. У цих випадках досьє мають бути тимчасово розділені.

Опис

Опис архівів колишніх репресивних режимів подібний до опису традиційних досьє. Мета – в помірні строки створити описові списки загального характеру, на кшталт путівників і реєстрів, які б сприяли тому, що зміст збірок буде широко відомим. Не рекомендується, щоб архівні працівники створювали каталоги, які містять детальну інформацію про осіб, через те, що вони можуть зачепити їхнє право на приватність. У випадку з документами, які колись оцінювалися і були визнані такими, що містять факти, пов'язані з приватністю осіб, рівень опису не повинен виходити за межі реєстру, який подає заголовок серії, охоплювані періоди і посилання на елементи, що зберігаються. Індекси до цих документів повинні містити тільки ім'я особи і каталожне посилання. З іншого боку, система індексів, створена репресивними режимами, якщо вона корисна архівним працівникам, не повинна визнаватися допомогою у пошуку і ставати доступною відвідувачам. Навпаки, вони повинні розглядатися як документи і зберігатися з основною частиною архівів у сховищах без публічного доступу. Ці старі інструменти контролю таким чином залишаться під виключним управлінням архівних працівників. Таким же чином використання комп'ютерів у описі повинно бути обмежене для створення списків, що відповідають правовим нормам щодо захисту приватності.

Адміністрація архівів

Одним із важливих положень, яке потрібно врахувати архівним працівникам, що працюють з документами колишніх репресивних режимів, є питання безпеки зберігання. Ці документи стосуються багатьох з них, особливо колишніх службовців цих організацій, і вони можуть бути зацікавлені в знищенні документів. Рекомендується, щоб для їхнього зберігання були впроваджені заходи безпеки, які повинні бути, принаймні, настільки ж суворими, як і ті, що існували в їхньому колишньому місці зберігання.

Управління користувачами є рівноважливим завданням. Рекомендується, щоб в архіві було створено кімнату публічного читання. Цей офіс повинен бути відповідальним за створення путівника про колективні та індивідуальні права, які гарантовані законом і які в сутності поширюються на архів. Цей путівник повинен також забезпечити основну інформацію про зберігання архівів і про умови доступу та послуги, що надаються користувачам.

У напрямку до путівника про джерела репресій: огляд архівів колишніх репресивних режимів у нових демократичних державах, 1974-1994.

Один факт, який ясно проявився у межах цього дослідження, є необхідність невідкладно брати на себе обов'язки щодо заходів, аби гарантувати збереження документів так само, як і їхнє легітимне використання. В процесі їхньої роботи експертна група зібрала інформацію тільки про 13 країн з 25, в які було надіслано повні запитальники щодо архівів репресій. З 13 отриманих відповідей дві не забезпечували інформації. про зберігання документів; у Зімбабве документи були знищені, а в Чилі не була доступна будь-яка інформація про статус архівів. Також відомо, що документи в Греції були знищені з етичних мотивів, хоча запитальник не було повернуто. В результаті з 14 країн в 3 архіви репресивних органів колишнього режиму відсутні, складаючи еквівалент 28,5%. Дві країни (Угорщина і Південна Африка) повідомили про недоступність фондів важливих репресивних інституцій колишніх режимів. Той факт, що декілька країн вирішили не відповідати на запитальник, не призводить до значного оптимізму щодо зберігання їхніх архівів репресій.

Кількість записів, про які повідомлялося (більше ніж 100.000 лінійних метрів з 11 країн) яскраво висвітлює кількість проблем, з якими зіткнулися нові органи влади.

Шість з цих 11 країн (Бразилія, Іспанія, Німеччина, Парагвай, Португалія і Росія) використовують документи для того, щоб виплатити компенсації жертвам репресій, і 4 (Німеччина, Латвія, Парагвай і Португалія) використовують документи для того, щоб звільнити відповідальних осіб колишнього режиму. В трьох країнах (Польща, Бразилія і Португалія) документи репресій використовуються Комісіями Правди.

Майже всі архіви обмежують доступ для того, щоб гарантувати захист честі і приватності осіб. Період закритості фондів коливається в межах 50 років у Іспанії, 75 років у Португалії і Росії і 100 років у Бразилії. У Німеччині період закритості фондів не встановлювався. У Латвії не існує такого загального обмеження, тут наявна політика контрастів: вільний доступ до документів певних органів (Міністерство внутрішніх справ) і обмежений доступ до інших (КДБ Латвійської республіки). Сім держав (Бразилія, Іспанія, Латвія, Німеччина, Росія, Парагвай і Португалія) встановили порядок надання документів для ознайомлення з метою наукових і історичних досліджень.

І, нарешті, у двох країнах (ПАР і Угорщина) найбільш важливі збірки документів не використовуються ні для компенсації жертвам, ні для звільнення осіб, відповідальних за репресії, ні для історичних досліджень. Чіткі рішення або нормативні документи стосовно цих записів відсутні. Однак в обох країнах були докладені значні зусилля для розкриття цих фондів.

ВИСНОВКИ

Робота експертної групи повинна розглядатися як перший етап міжнародної акції, яка повинна бути розширена і включити не тільки згадувані країни, але і організації захисту прав людини.

Необхідно створити Конституцію широкого міжнародного форуму щодо документів колишнього репресивного режиму за участі архівних працівників, правників, представників політичних партій, правозахисних організацій та інших.

Повинно бути вивчено можливість надання допомоги в управлінні записами колишніх репресивних режимів країнам у процесі переходу до демократії для того, щоб уникнути колапсу архівних установ і не дозволити знищення записів. Відповідно, середньостроковою метою могло б бути створення *фонду допомоги архівам на службі у прав людини* (колишні архіви служб репресій).

Робота з ідентифікації архівів репресій повинна продовжуватися – завдання, для якого програма «Пам'ять Світу» надає відповідні рамки, роблячи можливим включення до Реєстру всіх даних, зібраних дотепер.

Анджей Жеплінський, професор права Варшавського університету

ПРАВО НА ЗНАННЯ АРХІВНИХ ДАНИХ ПРО СЕБЕ

АРХІВИ КОЛИШНІХ СПЕЦСЛУЖБ

Архіви є безцінним джерелом для вивчення й осмислення минулого будь-якого народу. Це особливо важливо у випадку тоталітарних режимів з лівим ухилом або вкрай консервативних режимів, оскільки при цих режимах спецслужби були для уряду єдиним достовірним джерелом інформації про суспільну думку і стан в державі. Інші джерела менш повні, оскільки такі режими переслідували будь-які прояви відкритого і плюралістичного мислення і наукового аналізу. Тепер, після повалення таких режимів, стан і вміст архівів викликає, природно, великий інтерес до архівів з боку істориків, соціологів і журналістів. Крім того, політики намагаються використовувати їх у політичних цілях. Архіви повинні задовольнити всім цим потребам, однак, закон обов'язково повинний гарантувати нерозголошення конфіденційної інформації, особливо про жертви режиму.

Крім політиків, істориків, юристів і організацій, що поєднують жертв репресій, вплив у цьому питанні повинні мати також професійні архівісти. На конференції 1993 року в Мехіко Міжнародна Рада по архівах (ICA – International Council for Archives) ухвалив створення групи експертів для підготовки звіту по архівах репресивних режимів і розробки рекомендацій з роботи з цими архівами.

Поняття «репресивні режими» викликає гостру дискусію серед фахівців. Це поняття повинне включати всі режими, яким не вистачає законних демократичних основ і які змушені прибігати до різних поліцейських обмежень для збереження влади. Таке визначення, однак, неприйнятне для архівістів, істориків і правозахисників, наприклад, із прибалтійських держав, які стверджують, що правління в їхніх країнах німецьких нацистів і радянських комуністів у 1940-1991 роках було, по суті, окупацією. Тобто, режими були не тільки злочинними, але й іноземними. Це також відноситься до режимів Східного Тімора (індонезійська окупація) і Тібету (китайська окупація). З іншого боку, поняття «репресивний режим» добре відображає ситуацію в країнах третього світу, особливо в Латинській Америці, де вкрай консервативні режими існують десятиліттями.

Проект ICA, що фінансується ЮНЕСКО, має своєю метою забезпечувати архівістів у країнах, що скинули ярмо диктатури, інформацією про найкращі способи збору і виявлення документів, створених при репресивному режимі.

У лютому 1994 р. ІСА були призначені сім експертів-архівістів з Чилі, Іспанії, Німеччини, Південно-Африканської Республіки, Росії і США. Головою був призначений Антоніо Гонзалес Квінтана, глава Мадридського Військового Архіву (і начальник Відділу Громадянської Війни Національного Історичного Архіву Саламанки в 1984-1994 р.р.). Експерти добре усвідомлювали особливу делікатність документів, з якими працюють архівісти. Унаслідок цього, при роботі з такими документами, архівісти повинні керуватися спеціальним кодексом, проект якого був у свій час підготовлений.

Щоб зосередитися на останніх подіях, питання про архівізацію і виявлення документів, створених фашистськими режимами першої половини цього століття, не розглядалося.

Фахівці, що працюють над проектом ІСА, вирішили, що термін «репресивні інститути» варто використовувати стосовно до:

- служб розвідки і контррозвідки;
- воєнізованих організацій;
- спеціальних судів;
- концентраційних таборів;
- спеціальних в'язниць;
- центрів психіатричного перевиховання.

Крім того, репресивні структури можуть входити до складу таких традиційних суспільних інститутів, як:

- армія;
- поліція, у тому числі таємна поліція;
- звичайні суди;
- інші адміністративні органи.

У цей список, всупереч запереченням двох архівістів з колишніх комуністичних країн, не включений самий головний, на мій погляд, репресивний інститут у нашому регіоні – Комуністична партія і партійний апарат. Крім того, спеціальної уваги заслуговують архіви іноземного відділу. У таких країнах, як Польща, більшість дій дипломатичної і консульської служби були спрямовані проти груп політичних емігрантів, що відігравали важливу роль в опозиції й антикомуністичному опорі. Архіви таких «дипломатичних» служб також варто розглядати як архіви спецслужб.

Першою організацією, що практикувала масові репресії для збереження влади і для боротьби із супротивниками, була іспанська інквізиція. Архіви, що стосуються цієї організації, є моделлю, яку можна використовувати при роботі з документами, що залишилися від тоталітарних і автократичних режимів другої половини нашого століття. Документи Верховної й Універсальної рад інквізиції, а також велика частина документів її районних трибуналів, що зберігаються в Національному Історичному Музеї в Мадриді, є безцінними джерелами не тільки для вивчення способів підтримки королівської влади в той час, але і для розуміння менталітету і культури Ренесансу в Європі. Це доводить необхідність дбайливого

збереження такого роду документів для майбутніх поколінь істориків архівістами з посттоталітарних країн Центральної та Східної Європи кінця 80-х.

* * *

Як показує досвід, архіви спецслужб дуже багато значать для таких організацій. Це ясно видно з архівів східнонімецької Штазі (дванадцяте управління). Якими би секретними не були їхні дії і як би вони не хотіли сховати свої злочини, збільшені і сильно бюрократизовані інститути цих служб не могли протистояти спокусі реєструвати і записувати кожен крок.

Усе йде добре, поки беззаконна держава, жертви якої із захопленням перемелюються спецслужбами, знаходиться в повному розквіті. Ситуація може драматично змінитися ще до реального падіння режиму, коли посадові особи спецслужб намагаються не тільки уникнути відповідальності, але і знайти зручну фінансову позицію в новій обстановці.

Ми занадто рідко усвідомлюємо, що у вирішальні моменти нашого життя дані архівів (особливо офіційних архівів) можуть відігравати велику роль у долі кожного з нас. Це стає особливо ясним у ті моменти історії нації, коли беззаконна держава валиться, і люди одержують можливість ознайомитися хоча б з частиною документів, зібраних спецслужбами полеглого режиму. Важливість архівів складається не тільки в їхній корисності для вивчення і розуміння сучасної історії, а також у їхній ролі в захисті прав людини. Наприклад, у згаданому вище Архіві Громадянської Війни, що зберігається в Саламанці, містяться десятки тисяч досьє на республіканців, що переслідувалися режимом Франко. Іншим прикладом можуть служити 65.000 судових рішень про реабілітацію жертв комуністичних репресій у Польщі, прийнятих після 1988 р. Така реабілітація була б неможлива, якби документи про репресії не збереглися. Усі зацікавлені особи добре знають, яке значення може мати посвідчення статусу жертви сталінських репресій при одержанні допомоги: ці посвідчення видаються на підставі документів, що збереглися в російських архівах.

Експерти ІСА провели в десятку країн, у тому числі в Польщі, соціологічне дослідження. Архів Польського Міністерства Внутрішніх справ запитальник не повернув. У кінцевому рахунку, звіт був складений на підставі відповідей, отриманих із Бразилії, Чилі, Іспанії, Литви, Латвії, Німеччини, Парагваю, Португалії, Південно-Африканської Республіки, Росії, Угорщини і Зімбабве. Зібрані матеріали були використані в документі «Огляд архівів колишніх репресивних режимів у нових демократичних країнах (1974-1994)». Перша зі згаданих дат (квітень 1974 р.) – час падіння режиму Салазара в Португалії; друга дата (квітень 1994 р.) – час, коли чорношкіра більшість перемогла в загальнонародних виборах у Південно-Африканській Республіці. Звіт був довершений у грудні 1995 року.

* * *

Майбутнє архівів у більшості випадків залежить від того, як репресивний режим заміняється правовою державою. Навіть у випадку «м'якої революції» чи при прагненні до «національного примирення», аргументи про компенсацію збитків жертвам повинні мати пріоритет при рішенні долі архівів. У деяких випадках це має більше значення, ніж з'ясування імен осіб, винних у політичних репресіях, і осіб, що передали владу в перехідний період. У такій ситуації ситуація з архівами буде залежати від того, чи зберегли представники колишнього режиму політичний вплив.

Перше питання, яке повинне виникнути щодо архівів колишніх спецслужб після падіння диктатури, такий: що робити з цими архівами? Це, звичайно, відноситься тільки до тих режимів, документи про діяльність спецслужб яких збереглися. Може статися і зворотне: так, DINA і CNI, яка замінила її, – чилійські спецслужби періоду диктатури Піночета – стверджують, що вони знищили усі свої архіви ще до того, як у країні був організований цивільний уряд. Комісія зі Справедливості і Примирення, створена тут у 1990 році, зіштовхнулася з проблемою відновлення 15 років національної історії, що включає кілька тисяч політичних убивств, за повідомленнями і спогадами окремих осіб. В міру усвідомлення масштабів репресій DINA, виявлення винних у цих звірствах здається майже неможливим. Додаткових труднощів додає той факт, що Чилі пробиває шлях до демократії через примусове національне примирення, гарантоване законом, створеним Піночетом і його оточенням, що також забезпечили для себе закони, які їх амністують. Це сильно ускладнює всяку ідентифікацію осіб, винних у злочинах. Ситуація в Південно-Африканській Республіці аналогічна. Дотепер невідома доля архівів іспанської SD, однієї з місцевих спецслужб. В Родезії, у 1979-1980, перед переходом влади до чорношкірих, місцеві спецслужби знищили усі свої архіви.

Подібні спроби знищити документи, що свідчать про беззаконня і репресії, були розпочаті спецслужбами комуністичних країн у період переходу до демократії. Багатьом з них удалося знищити частину даних, що відносяться до найбільш ганебних випадків.

Однак, можливо тільки часткове знищення документів. Архіви були занадто великі, щоб можна було організувати їхнє швидке знищення, не привертаючи уваги громадськості. Громадськість Східного Берліна організувала активний захист місцевих архівів; однак, незважаючи на це, багато архівів Штазі, що зберігаються в столицях земель Східної Німеччини, були знищені. Ці дії східних німців були викликані усвідомленням важливості архівів у справі переслідування нацистських злочинців і реабілітації їхніх жертв. У Польщі відомості про спалення документів працівниками комуністичних спецслужб, у той час ще функціонуючих, стали відомі узимку 1989/90 р., що дозволило зупинити знищення цих документів.

Падіння репресивної системи відбувається не моментально. Звичайно йому передує безліч симптомів. І, звичайно, найкраще про ці симптоми бувають інформовані працівники спецслужб. Крім того, між переходом влади до політиків-демократів і встановленням контролю над спецслужбами проходить кілька місяців. Протягом цього досить тривалого періоду офіційні особи можуть спробувати вилучати з архівів деякі документи. Будучи викраденими, такі документи можуть у майбутньому захистити цих осіб від судового переслідування, а також можуть бути використані для шантажу колишніх співробітників з метою одержання економічної чи політичної вигоди. Це відбулося в Польщі, Чехії й Угорщині.

Зовсім інша ситуація спостерігається в Прибалтиці й Україні. Уже наприкінці вісімдесятих років центральні органи комуністичної влади почали вилучати документи з місцевих архівів КДБ і КПРС і перевозити їх у Москву. Таким чином, ці нації були позбавлені можливості зберегти документи про найбільш трагічний період своєї історії, а жертви злочинів комуністів – надії одержати хоча б часткову компенсацію. Тому серед перших законів, створених урядами незалежних Балтійських країн, були постанови про захист збережених залишків місцевих архівів партії і КДБ.

Ситуація в Москві нагадує ситуацію, наприклад, в Аргентині. КДБ був органом незалежної держави. Перед переходом влади його працівники подбали про власну безпеку. Їхнє положення було набагато більш вигідним у порівнянні з положенням працівників таємної поліції при інших латиноамериканських репресивних режимах. Падіння комуністичного режиму відкрило широкі можливості для безкарного розграбування величезної державної власності. У цій своєрідній приватизації брали участь працівники КДБ, партійні і комсомольські діячі і лідери організованих злочинних груп. Це сильно збільшило шанси КДБ на збереження колишніх привілеїв. Таким чином, діють два фактори: у минулому працівники КДБ мали привілеї, оскільки вони працювали на державу, а в сьогоденні вони стали керівним класом. Тому не було необхідності знищувати або вилучати документи.

* * *

Що стосується поводження з архівами колишніх спецслужб, то двох однакових чи хоча б схожих рішень не існує.

Найчастіше архіви, що залишилися від колишніх спецслужб, зберігаються. В іншому випадку, такі документи знищуються після їхнього використання в адміністративних цілях (ідентифікації, реабілітації і відшкодування збитку жертвам).

Це останнє рішення було прийнято в Греції, де законодавці зневажили історичною цінністю архівів, мотивуючи своє рішення знищити ці архіви необхідністю захисту жертв режиму чорних полковників. Можливість такого рішення обговорювалася також в Іспанії. Після одного інциденту (у Мадридському аеропорті був арештований депутат-комуніст,

досьє на якого містилося в старих архівах і було використано поліцією), кортесами обговорювалася пропозиція знищити всі архіви режиму Франко. У кінцевому рахунку, іспанські депутати ухвалили вилучити з поліцейських архівів усі згадування про соціально-політичних активістів, що діяли проти режиму Франко, а також передати всі документи політичної поліції, що відносяться до цього періоду, у Національний Історичний Музей. Це було почато по взаємній згоді міністрів внутрішніх справ і культури.

Необхідно розуміти, що, у випадку скинення правлячого режиму, дані архівів спецслужб можуть бути використані для репресій. Крім того, оскільки невідомо напевно, які документи були знищені (і чи знищувалися вони взагалі), а також хто володіє документами, що залишилися, такі документи в будь-який час можуть стати інструментом беззаконня. Тому не слід знищувати або розосереджувати архіви колишніх спецслужб: їхнє збереження в архівах, окремо від поточних архівів спецслужб, повинне визначатися законом і контролюватися професійними архівістами. Це – єдиний спосіб гарантувати при новому політичному ладі права жертв репресивних режимів, включаючи індивідуальну амністію, законну реабілітацію, відновлення власності і компенсацію збитку. Чесне дотримання цього правила доводить поступове зближення влади закону і плюралістичної демократії.

Досвід показує, і Іспанія є тільки одним прикладом, що найбільш ефективним способом захисту прав жертв є законна ізоляція архівів спецслужб і їхня передача незалежним від цих служб професійним архівістам. У світлі звіту ICA, професіоналам повинні передаватися документи, створені спецслужбами, розвідкою і контррозвідкою, а також досьє щодо політичних справ, що велися таємною поліцією. Перераховані вище служби повинні якомога швидше передати документи в національні архіви чи в спеціальні архіви, що займаються реабілітацією.

Закон про передачу документів колишніх спецслужб повинний гарантувати збереження цих архівів як частини культурної спадщини нації.

* * *

На думку міжнародних суспільств архівістів, істориків і захисників прав людини, основні принципи законів, що відносяться до архівів, у яких зберігаються документи, створені спецслужбами репресивних режимів, такі:

1) Кожна нація має право пам'ятати свою історію в такому вигляді, як вона записана в документах. Документи, по суті, є історичною спадщиною.

2) Кожна нація має право на правду. Громадяни мають право на максимум інформації (наскільки це можливо) про діяльність скинутого режиму.

3) Кожна нація має право на ідентифікацію осіб, винних у порушеннях прав людини. Це право не залежить ні від яких політичних рішень, що стосуються цих осіб, у тому числі можливості їхньої подальшої участі в суспільному житті. Політика помилування й амністування осіб, винних у порушеннях прав людини, проводилася в деяких молодих демократичних країнах з метою сприяння національному примиренню. Однак у демократичній правовій державі право знати імена осіб, відповідальних за порушення прав людини, повинне бути збережено, щоб ці особи не могли використовувати своє минуле для отримання політичної вигоди. Це рішення було прийнято в Німеччині, де архіви Штазі використовуються суспільними і приватними організаціями для з'ясування ступеня відповідальності різних органів і осіб за їхні зв'язки з колишнім режимом ГДР. Це робиться, щоб не допустити ситуації, коли працівники і співробітники комуністичної таємної поліції, як і раніше, будуть займати керівні посади. З іншого боку, німецьке законодавство обмежує термін такого використання архівів Штазі п'ятнадцятирічним періодом (до 2006 р.).

4) Кожна особа має право знати, яка стосовна до нього інформація міститься в архівах спецслужб (якщо така є). Це право називається «**правом на знання особистістю архівних даних про себе**». Це право дозволяє жертві спецслужб довідатися, до якого ступеня політичні, ідеологічні, етнічні чи расові упередження вплинули на її особисте, сімейне і професійне життя. Таке ж право доступу до своїх досьє мають працівники колишніх спецслужб.

5) Кожна особа має право на проведення наукових пошуків в архівах колишніх спецслужб. У цьому випадку право доступу до архівів обов'язково повинне розглядатися з обліком права на недоторканність приватного життя жертв репресій. Крім того, права третіх осіб, що згадуються в документах, також повинні бути захищені. Постраждалі особи повинні зберігати право доступу до їх документів, що стосуються, протягом часу, визначеного законом. Такі особи також повинні мати право вносити виправлення в ці документи, однак, зміна їхнього основного змісту повинна бути заборонена.

6) Кожна жертва має право на законну реабілітацію, на відшкодування збитків, понесених в результаті дій працівників колишніх спецслужб, а також на відновлення конфіскованої власності. Свідчення, необхідні для таких компенсацій, містяться в документах, створених спецслужбами.

7) Кожна особа має право наводити довідки про долю своїх родичів, що пропали в результаті діяльності спецслужб.

8) Кожна жертва має право знати імена осіб, що брали участь в її переслідуваннях.

* * *

Моральний кодекс архівістів, що працюють з документами колишніх спецслужб:

- документи про репресії є частиною національної спадщини. Усі ці документи повинні бути збережені як нагадування про нетерпимість, расизм, а також політичний й ідеологічний тоталітаризм;
- архівіст є виконавцем волі нації в період переходу до демократії;
- права жертв політичних репресій превалюють над історичними дослідженнями;
- архіви колишніх спецслужб не повинні відбиратися ні за яким критерієм, крім критерію історичного дослідження;
- архівіст – не цензор; поняття архівних даних і процедура їх розкриття визначені законом;
- якщо вказівки закону недостатньо точні, архівіст може інтерпретувати їх у світлі офіційних думок фахівців із суспільних законів. У випадку виникнення конфлікту між правом особи на недоторканність приватного життя і правом на проведення історичних досліджень, рекомендується створення копій документів з вилученими з них іменами жертв чи третіх осіб;
- архівіст зобов'язаний задовольняти всі запити жертв репресій чи інших осіб на створення копій чи документів підтвердження дійсності документів;

архівіст зобов'язаний організувати систему контролю, що забезпечує захист документів, які містять конфіденційні дані. Документи про репресії повинні зберігатися в спеціальних, ізольованих відділах національних архівів, їхня безпека повинна ретельно дотримуватися. Доступ до таких документів можуть мати тільки працівники архівів.

Євген Захаров, Харківська правозахисна група

ХРЕСТОМАТІЙНА СПРАВА КОСТЯНТИНА УСТИМЕНКА

Однією з цілей семінару «Свобода висловлювань в Україні. Доступ до інформації», який проводила Харківська правозахисна група в Києві 28 лютого – 1 березня 2002 року за підтримки фонду МакАртурів, було намагання привернути увагу громадськості, зокрема, юридичної, до справи Костянтина Устименка. З самих різних точок зору ця справа заслуговує на широке суспільне обговорення.

В історичній площині справа Устименка пов'язана з практикою політичних репресій в СРСР. Будучи щирим комуністом, віряч в рівність усіх членів КПРС, Устименко звертався з листами в партійні органи, в яких критикував керівництво Дніпропетровського обкому КПРС. Саме це стало причиною заочної постановки його на психіатричний облік в міському психоневродиспансері: з точки зору верхівки КПРС люди, які критикували їхні дії, були божевільними. Це була усталена практика. Чимало людей, обвинувачуваних в антирадянській агітації і пропаганді, отримували від психіатрів «вялотекущую шизофренію» або інший діагноз і потрапляли за судовими рішеннями на примусове лікування в закриту психлікарню до тих пір, поки не давали підписку про відмову від суспільної активності. Відомо також, що левову долю авторів анонімних антирадянських листівок, яких КДБ вдавалося виявити (а таких антирадянщиків було приблизно 100 на рік), клали в психлікарні без будь-якого суду. Досі деякі люди, які потрапили під прес каральної психіатрії, знаходяться в лікарнях: їх би вже й відпустили, але просто нема куди йти. Якось, коли я відвідував одного такого свого підопічного, його лікар розповів, як йому, коли він працював районним психіатром в сільському районі, телефонував перший секретар райкому: «Слухай, забери Н. – він скаржиться на мене усюди, лає мене, він хворий!» І, каже, ми забирали! У цьому сенсі Устименку ще повезло. Він не потрапив в лікарню за свої листи, як, наприклад, харків'янин Володимир Кравченко, його «просто» виключили з КПРС і звільнили з роботи (будучи радіоінженером, Устименко працював викладачем в технікумі) і не давали змоги працювати будь-де, аж поки не працевлаштували за прямою вказівкою Володимира Щербицького, якого Устименко побачив рано-вранці 26 квітня 1986 року (перші години після початку Чорнобильської катастрофи!) разом з першим секретарем Дніпропетровського обкому в центрі Дніпропетровська і попросив про допомогу. Так він і працює зараз кочегаром.

Дізнавшись, що він був заочно поставлений на психіатричний облік і знятий з нього, Устименко вирішив домогтися ознайомлення зі своїм досьє: як сталося, що він був взятий на облік, а потім знятий з нього, хто приймав ці рішення і за чиєю вказівкою, куди надсилали довідки про його стан здоров'я і за чими запитами, як і на підстави яких нормативних актів обмежували його право на працевлаштування тощо. І почався новий багатолітній етап ходіння по муках – юридичний. Борючись за своє право знати інформацію про себе, Устименко дійшов до Конституційного Суду України, який прийняв дуже важливе рішення по його заяві. Рішення, яке стало предметом гордості Конституційного Суду, яке вивчають в юридичних вузах, багато разів друкувалося в різних виданнях, здавалося б, повністю мало задовольнити позивача. Але це рішення нічого не дало самому Устименку: воно просто не було виконане. І, на жаль, не вбачається правових можливостей для зрушення цієї справи з мертвої точки. Проте, може, якійсь світлий правовий розум знайде вихід з цього положення?

Пропонуємо увазі читачів виклад обставин справи самим Костянтином Устименком і коментар фахівця-конституціоналіста Станіслава Шевчука.

Костянтин Устименко, м. Дніпропетровськ

ЗДІЙСНЕННЯ ПРАВА НА ІНФОРМАЦІЙНУ ПРИВАТНІСТЬ ТА ПРАКТИКА СУДОВОГО ЗАХИСТУ ЦЬОГО ПРАВА

(виступ на семінарі «Свобода висловлювань в Україні. Доступ до інформації» в Києві, 28 лютого – 1 березня 2002 р.)

Першою справою, розглянутою Конституційним Судом України (КСУ) за зверненням громадянина України, була справа К.Г. Устименка стосовно тлумачення положень Законів України «Про інформацію» та «Про прокуратуру».

Рішення КСУ по цій справі від 30.10.97 стало хрестоматійним прикладом судового захисту конституційного права громадянина на інформацію про особу. Цей приклад неодноразово наводився у засобах масової інформації, у виступах керівництва КСУ, у звітній доповіді Уповноваженого з прав людини Верховної Ради, у посиланнях відомого в Україні американського судді Богдана Футея.

При цьому ні один з дописувачів чи промовців про «справу Устименка» не звернувся до самого Устименка хоча б для одержання формального дозволу використовувати його повне прізвище та ім'я, які належать до персональної інформації про особу і не можуть використовуватися без її дозволу, якщо ця особа не є публічною особою.[47]

Більше того, оскільки мотивувальна частина вказаного рішення КСУ через певні обставини не була оприлюднена негайно, деякі дописувачі керувались усними поясненнями на прес-конференції доповідача по справі в КСУ та опублікованою в листопаді 1997 р. в «Урядовому кур'єрі» та в «Юридичному віснику України» резолютивною частиною рішення, що призвело до деякого викривлення інформації щодо Устименка в публікаціях.

Виходячи з цього, я щиро вдячний організаторам даного поважного зібрання за надану мені можливість поінформувати широкий загал про наслідки судового захисту права на доступ до персональної інформації про громадянина Устименка для самого Устименка.

Перед тим, як викласти обставини справи та мотиви рішення КСУ, вважаю доцільним звернути увагу на юридичне підгрунтя, на якому базувалось звернення до судових органів.

---

[47] Ми не можемо погодитися в цьому з шановним автором – з моменту прийняття рішення Конституційним Судом України по справі Устименка він став публічною, а точніше, квазі-публічною особою. – Ред.

Згідно Закону України «Про інформацію» від 02.10.92:

«дія цього Закону поширюється на інформативні відносини, які виникають у всіх сферах життя і діяльності суспільства і держави при одержанні, використанні, поширенні та зберіганні інформації» (ст. 3).

«Кожному громадянину забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законами України» (ст. 9).

«Інформація про особу – це сукупність документованих або публічно оголошених відомостей про особу... Кожна особа має право на ознайомлення з інформацію, зібраною про неї» (ст. 23).

«Громадяни мають право доступу до інформації про них, заперечувати її правильність, повноту, доречність, тощо». Відмова в доступі до такої інформації, або приховування її, або незаконні збирання, використання, зберігання чи поширення можуть бути оскаржені до суду» (ст. 31).

«В разі вчинення державними органами... та їх посадовими особами,... державними організаціями, які є юридичними особами, та окремими громадянами протиправних діянь, передбачених цим Законом, ці дії підлягають оскарженню до органів вищого рівня або до суду» (ст. 48).

Звертаючись до суду загальної юрисдикції в 1989 р., Устименко посилався на Закон СРСР «О порядке обжалования в суд неправомерных действий органов госуправления и должностных лиц...», порушуючи який головлікар психоневродиспансеру відмовлявся надати інформацію щодо підстав заочних взяття й зняття з психіатричного обліку Устименка.

Перше рішення суду – відмовити в задоволенні скарги Устименка – грунтувалось на лікарській таємниці. Потім, після втручання Прокуратури України, після депутатських звернень до Генерального Прокурора М. О. Потебенька депутата Л.Д. Кучми, суд поступово став змінювати свою позицію по справі.

Одночасно, у зв'язку з набранням в листопаді 1992 р. чинності Закону України «Про інформацію» претензії були оформлені у вигляді інформаційного запиту, а після отримання відмови головлікаря було змінено підстави судової скарги, тобто оскаржувалось порушення Закону «Про інформацію».

Після скасування за протестами прокуратури двох рішень суду, третім рішенням дії головлікаря в частині надання Устименку інформації, що не відповідає дійсності та приховуванні інформації, визнані неправомірними й зобов'язано посадову особу надати Устименку письмову відповідь на такі питання:

1. Ким, коли і на якій підставі Устименка було поставлено на облік у психоневродиспансері?

2. За якими адресами розсилались довідки про стан здоров'я Устименка?

3. Ким Устименка було знято з обліку, на якій підставі та чи був він при цьому присутнім?

4. На підставі якого нормативного акту психіатри в 1988-90 рр. обмежували працевлаштування Устименка?

В 1994 р. Дніпропетровський обласний суд задовольнив скаргу головлікаря, скасував вказані рішення райсуду й провадження по цій справі закрив, оскільки її розгляд не є компетенцією суду.

Намагаючись якимось чином отримати персональну інформацію про себе і знаючи, що прокуратура має матеріали перевірки скарги на дії головлікаря, Устименко направляв з цього питання інформаційний запит і до прокуратури, а відмову в наданні інформації прокурора оскаржив до суду. Суд відмовив у розгляді скарги на тій підставі, що громадянин може оскаржити дії прокурора тільки у випадках, передбачених Кримінально-процесуальним кодексом. Таким чином, судами загальної юрисдикції у 1994 р. відмовлено Устименку в захисті його права на отримання інформації про себе, гарантоване ст. ст. 3, 23, 31, 48 Закону «Про інформацію».

Перевіривши останні судові рішення в порядку нагляду, Голова Верховного Суду В.Ф. Бойко 18.11.96 підтвердив їх законність і обгрунтованість, хоч на цей час право на інформацію про особу та на судовий захист цього права вже гарантувалось ст. 32 Конституції України.

З приводу неоднозначного застосування судами загальної юрисдикції Закону України «Про інформацію» Устименко звернувся до КСУ.

Рішенням по справі Устименка № 18/гоз-97 від 30.10.97 КСУ вирішив в резолютивній частині:

1. Частину 4 статті 23 Закону України «Про інформацію» треба розуміти так, що забороняється не лише збирання, а й зберігання, використання та поширення конфіденційної інформації про особу без її попередньої згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту, прав та свобод людини. До конфіденційної інформації, зокрема, належать свідчення про особу (освіта, сімейний стан, релігійність, стан здоров'я, дата і місце народження, майновий стан та інші персональні дані).

Згода на збирання, зберігання, використання і поширення відомостей щодо недієздатної особи надається членам її сім'ї або законним представником. У період збирання інформації про нього кожний дієздатний, члени сім'ї або законні представники недієздатного мають право знати, які відомості і з якою метою збираються, як, ким і з якою метою вони використовуються. У період зберігання і поширення персональних даних ці ж особи мають право доступу до такого роду інформації, заперечувати її правильність, повноту, тощо.

2. Частину 5 статті 23 Закону «Про інформацію» треба розуміти так, що кожна особа має право знайомитись з зібраною про неї інфор-

мацією в органах державної влади, органах місцевого самоврядування, установах і організаціях, якщо ці відомості не є державною або іншою, захищеною законом, таємницею.

Медична інформація, тобто свідчення про стан здоров'я людини, історію її хвороби, про мету запропонованих досліджень і лікувальних заходів, прогноз можливого розвитку захворювання, в тому числі і про наявність ризику для життя і здоров'я, за своїм правовим режимом належить до конфіденційної, тобто інформації з обмеженим доступом. Лікар зобов'язаний на вимогу пацієнта, членів його сім'ї або законних представників надати їм таку інформацію повністю і в доступній формі.

В особливих випадках, як і передбачає ч. 3 ст. 39 Основ законодавства України про охорону здоров'я, коли повна інформація може завдати шкоди здоров'ю пацієнта, лікар може її обмежити. У цьому разі він інформує членів сім'ї або законного представника пацієнта, враховуючи особисті інтереси хворого. Таким же чином лікар діє, коли пацієнт перебуває у непритомному стані.

У випадках відмови у наданні або навмисного приховування медичної інформації від пацієнта, членів його сім'ї або законного представника вони можуть оскаржити дії чи бездіяльність лікаря безпосередньо до суду або, за власним вибором, до медичного закладу чи органу охорони здоров'я.

Правила використання відомостей, що стосуються лікарської таємниці – інформації про пацієнта, ні відміну від медичної інформації – інформації для пацієнта, встановлюються статтею 40 Основ законодавства України про охорону здоров'я та ч. 3 ст. 46 Закону України «Про інформацію».

3. У ст. 48 Закону України «Про інформацію» визначальними є норми, сформульовані у ч. 1 цієї статті, які передбачають оскарження встановлених Законом «Про інформацію» протиправних діянь, вчинених органами державної влади, органами місцевого самоврядування та їх посадовими особами, а також політичними партіями, іншими об'єднаннями громадян, засобами масової інформації, державними організаціями, які є юридичними особами, та окремими громадянами, або до органів вищого рівня, або до суду, тобто за вибором того, хто подає скаргу. Частина друга ст. 48 Закону «Про інформацію» лише встановлює порядок оскарження протиправних дій посадових осіб у разі звернення до органів вищого рівня, а ч. 3 цієї статті акцентує на тому, що й оскарження, подане до органів вищого рівня, не є перепоною для подальшого звернення громадянина чи юридичної особи до суду. Частину третю у контексті всієї ст. 48 Закону «Про інформацію» не можна розуміти як вимогу обов'язкового оскарження протиправних дій посадових осіб спочатку до органів вищого рівня, а потім – до суду.

Безпосереднє звернення до суду є конституційним правом кожного.

4. Визнати неконституційним положення частини четвертої статті 12 Закону України «Про прокуратуру» щодо можливості оскарження прийнятого прокурором рішення до суду лиш у передбачених законом випадках, оскільки винятки з конституційних норм встановлюються самою Конституцією, а не іншими нормативними актами.

5. Прийняття рішення Генеральним прокурором України по скарзі (ч. 5 ст. 12 Закону «Про прокуратуру») припиняє провадження по таких скаргах в органах прокуратури, але не може стати перешкодою для подальшого звернення до суду.

6. Рішення КСУ є обов'язковим до виконання на території України, остаточним і не може бути оскарженим. Рішення КСУ підлягає опублікуванню у «Віснику КСУ» та в інших офіційних виданнях України.

Роз'яснюючи ці рішення КСУ на прес-конференції, матеріали якої опубліковано в «Юридичному віснику України» №47 за 1997 р., доповідач по справі суддя КСУ Олександр Мироненко на питання: «Тепер, після винесення КСУ рішення у цій справі, громадянин Устименко може розраховувати на її перегляд у судах загальної юрисдикції?», відповів: «безперечно, такі суди прийматимуть відповідні рішення, виходячи з нашого тлумачення закону».

З надією я чекав одержання повного тексту рішення КСУ. Отримавши його поштою і ознайомившись з мотивувальною частиною, яка ще ніде не була опублікована, я звернувся до Голови КСУ з листом, в якому, зокрема, повідомляв:

«Всупереч вимогам ст. 55 Закону «Про Конституційний Суд України» мене було позбавлено права участі в розгляді мого звернення, що призвело до перекручення інформації в мотивувальній частині рішення КСУ...

Вказаний на стор. 4 рішення КСУ, як діючий сьогодні в Україні, наказ МОЗ СРСР від 29.12.79 № 1333 «Про порядок надання відомостей про психічний стан громадян» з 1 березня 1991 р. вже в СРСР був нечинним відповідно до п. 2 Висновку Комітету конституційного нагляду СРСР від 29. 11. 90 № 17 «О правилах, допускающих применение неопубликованных нормативных актов о правах, свободах и обязанностях граждан». Розповсюдження інформації від імені КСУ про дію в Україні цього наказу матиме негативні правові наслідки.

Керуючись ст. 40 Конституції, прошу Вас, як посадову особу державного органу, письмово повідомити мене про можливі засоби обмеження розповсюдження недостовірної інформації з рішення КСУ від 30.10.97 по справі Устименка».

Всупереч вимогам ст. 40 Конституції Голова КСУ на це моє звернення не відповів, але опубліковані в листопаді 1997 р. в «Урядовому кур'єрі» та в «Юридичному віснику» рішення КСУ містили лише резолютивну частину без мотивувальної. До речі, мої спроби в цьому році знайти в

будь-якій бібліотеці м. Дніпропетровська «Вісник КСУ» з опублікованим повним рішенням КСУ по справі Устименка не мали успіху, бо підписка проводилась з 1998 р., а перший номер «Вісника КСУ» за 1998 р. був третім по рахунку. Тому, якщо повні рішення опубліковано в першому чи другому номері «Вісника КСУ», у Дніпропетровські, як і в інших містах України, публічне ознайомлення з ним обмежене, про що я й просив Голову КСУ.

Керуючись рішенням КСУ та діючим законодавством Устименко й прокуратура області звернулись до Дніпропетровського обласного суду з поданням про перегляд ухвали облсуду від 21.02.94 про закриття провадження по справі Устименка за непідвідомчістю суду за новими обставинами.

Ухвалою облсуду від 30.01.98, постановленою під головуванням судді А.П. Приходченко, яка брала участь у проголошенні ухвали 1994 року, подання прокуратури і заява Устименка відхилені.

Підставою відмови в перегляді справи суд назвав те, що офіційне тлумачення Конституційним Судом Закону «Про інформацію» по справі Устименка не може бути визнаним нововиявленими обставинами, оскільки це тлумачення не містить відомостей, про які на день проголошення ухвали від 21.02.94 не знали і не могли знати сторони і суд.

Тим самим суд визнав, що він свідомо не застосував у 1994 році по справі Устименка положення Закону «Про інформацію», які повинні бути застосовані.

Розуміючи такий підтекст, в ухвалі від 30.01.98 зазначено можливість перегляду ухвали 1994 року в порядку судового нагляду. Але внесений після цього протест прокуратури в порядку судового нагляду відхилено постановою президії Дніпропетровського облсуду від 08.04.98.

Законність і обгрунтованість судових рішень про відмову в перегляді справи Устименка на основі рішення КСУ підтвердив 29.12.2000 Голова Верховного Суду В.Ф. Бойко. При цьому він повідомив, що провадження з цього питання у Верховному Суді України закрите.

Звернення з скаргою на порушення права на судовий захист та права на особисту інформацію до Європейского суду з прав людини залишено без розгляду у зв'язку неприйнятністю скарги до розгляду рішенням від 26.10.99. В чому полягала ця неприйнятність в рішенні Європейського суду, не пояснюється і не повинно пояснюватися згідно п. 4 ст. 35 Конвенції про захист прав людини.

Після внесення змін до Цивільно-процесуального кодексу відносно права касаційного оскарження у Верховному Суді рішень суду, які були прийняті протягом часу дії Конституції України 1996 року, на ухвалу облсуду від 30.01.98 була подана касаційна скарга до Верховного Суду.

Жевріла надія, що персональне рішення Голови Верховного Суду про закриття провадження з цього питання у Верховному Суді може ви-

явитися залежним від норм закону і сумління. В скарзі наводились аргументи про порушення в ухвалі від 30.01.98 норм матеріального права – статей 3, 19, 32, 55 Конституції України, статей 23, 48 Закону «Про інформацію» та ст. 69 Закону «Про Конституційний Суд України».

В скарзі ставилось питання про скасування ухвали облсуду від 30.01.98 та про перегляд Верховним Судом ухвали облсуду від 21.02.94 у зв'язку з виключними обставинами на основі рішення КСУ по справі Устименко від 30.10.97.

Ухвалою Верховного Суду від 12.10.01 в задоволенні касаційної скарги Устименку відмовлено.

На підтвердження особистої думки по справі Голови Верховного Суду, висловленої двічі, у 1996 і у 2000 році, підлеглі судді в цій ухвалі умудрились навіть не згадати про рішення КСУ. Всупереч вимогам ст. 343 ЦПК (Цивільно-процесуального Кодексу) в ухвалі не наведено касаційної скарги про порушення норм права і, відповідно, не вказано, чому ці доводи не взяті до уваги.

Ухвала Верховного суду від 12.10.01 є остаточною і оскарженню не підлягає.

Які можна зробити з наведених фактів порушення протягом майже десяти років права на інформацію про особу громадянина України?

Дотримання Конституції і Законів України не є обов'язковим у свідомості тих посадовців, які повинні опікуватися законності в Україні. Таке становище обумовлено відсутністю конкретних санкцій за порушення високими посадовцями своїх обов'язків та визначеного законом механізму дійового застосування цих санкцій.

На сьогодні в Україні відсутній механізм взаємоконтролю діяльності законодавчої, судової та виконавчої гілок влади, не визначений механізм відкликання виборцями народного депутата, немає визначеної законом ініціативи громадських правозахисних організацій в розслідуванні зловживань високими посадовцями своїми посадами.

Порушення законності суддями оцінюється самими ж суддями у виборних кваліфікаційних комісіях, а члени незалежного органу контролю діяльності суддів – Вищої Ради Юстиції – в повній мірі не застосовують своє право відповідно до ст. 38 Закону України «Про Вищу Раду Юстиції» проводити перевірки зловживань суддями за зверненнями звичайних громадян України.

В свою чергу народні депутати Верховної Ради, які є суб'єктами звернення до Вищої ради Юстиції про відкриття дисциплінарного провадження з приводу порушення присяги суддями Верховного Суду, недостатньо використовують свої права за матеріалами звернень виборців.

Відсутність відповідальності посадовців зумовлює типове порушення права на інформацію про особу, а саме на заборону поширення інформації про особу без її згоди, коли з екрану телевізора прокурор чи слідчий на основі обвинувачувального висновку називає прізвище підозрю-

ваного як злочинця, хоча це можна зробити лише після набрання чинності вироку суду.

На жаль, законодавець не завжди користується вже визначеними Законом «Про інформацію» дефініціями. Так, у ст. 1 цього Закону визначено, що під інформацією розуміються документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі.

В прийнятій Верховною Радою 03.03.98 редакції Закону «Про обмеження монополізму та недопущення недобросовісної конкуренції у підприємницькій діяльності» стаття перша визначає, що інформація – це відомості в будь-якій формі та вигляді, на будь-яких носіях, у тому числі листування, книги, помітки, ілюстрації, карти, малюнки, схеми, фотографії, кіно- і відеофільми... Тобто дається розширене тлумачення поняття «інформація» з віднесенням до неї можливих об'єктів права інтелектуальної власності, що може призвести до колізії норм права про особисту інформацію та норм про авторське право і інтелектуальну власність.

Як бачимо, відсутність бажання виконувати Закон поєднується з колізіями законодавчих актів, з безвідповідальністю посадових осіб і все це, на мій погляд, зумовлено рівнем культури діючих осіб, які не напевно відрізняють добре і зле.

Тому завдання неурядових правозахисних організацій полягає, насамперед, у просвітницькій роботі не тільки для підвищення рівня правової культури громадян, але й для підвищення рівня моральної культури посадовців, що сприятиме сумлінності виконання ними своїх обов’язків.

Станіслав Шевчук, кандидат юридичних наук

СПРАВА К. Г. УСТИМЕНКА ТА ДЕЯКІ ПРОБЛЕМИ ВИКОНАННЯ РІШЕНЬ КОНСТИТУЦІЙНОГО СУДУ УКРАЇНИ

Рішення Конституційного Суду України (далі – КСУ) у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «ро інформацію»та статті 12 Закону України «ро прокуратуру» (справа К. Г. Устименка) від 30 жовтня 1997 року має велике значення для становлення вітчизняного конституційного судочинства. На це вказують наступні характеристики цього Рішення:

1. По суті, воно є першим прикладом захисту єдиним органом конституційної юрисдикції конституційних прав окремої фізичної особи шляхом реалізації конституційних повноважень щодо офіційного тлумачення Конституції та Законів України. Важливість цього рішення значно підсилюється фактом відсутності закріплених в Конституції України та у Законі України «Про Конституційних Суд України» від 16 жовтня 1996 року повноважень щодо безпосереднього звернення фізичної або юридичної особи для захисту конституційних прав та свобод (права на конституційну скаргу). Ці особи можуть звертатися до КСУ за цим захистом лише опосередковано, використовуючи послуги «політичних посередників» – суб`єктів права на конституційне подання (Президента України, не менш як 45 народних депутатів України, Верховного Суду України, Уповноваженого Верховної Ради України з прав людини, Верховної Ради Автономної Республіки Крим). Після звернення фізичної або юридичної особи зазначені суб`єкти права на конституційне подання вивчають порушені заявником питання, їх юридичну обгрунтованість та можливість звернення до КСУ.

Як свідчить відповідна практика, для захисту цих прав та свобод окремих осіб до КСУ звертався лише Уповноважений Верховної Ради України у деяких випадках. Найбільш відомим є Рішення Конституційного Суду України у справі за конституційним поданням Уповноваженого Верховної Ради України з прав людини щодо відповідності Конституції України (конституційності) положень статей 7, 8 Закону України "Про державні гарантії відновлення заощаджень громадян України", за конституційним зверненням Воробйова В. Ю., Лосєва С.В. та інших громадян щодо офіційного тлумачення положень статей 22, 41, 64 Конституції України (справа про заощадження громадян) від 10 жовтня 2001 року. Але навіть у цих випадках конституційне подання Уповноваженого до КСУ носить абстрактний (від імені всіх осіб), а не конкретний (в інтере-

сах конкретних осіб) характер, що не може не впливати на якість та ефективність конституційного судочинства.

Як свідчить практика західних демократій у сфері конституційного судочинства, саме через інститут індивідуальної конституційної скарги досягається найбільш максимальний рівень захисту з урахуванням особливості кожної справи та специфіки порушення конституційного права окремої особи.

З іншого боку, відповідно до чинного українського законодавства, єдиною можливістю безпосереднього захисту конституційних прав та свобод залишається використання інституту конституційного звернення з метою офіційного тлумачення Конституції України та законів України, «якщо суб'єкт права на конституційне звернення вважає, що це може призвести або призвело до порушення його конституційних прав і свобод» (стаття 94 Закону «Про Конституційний Суд України»). Ця можливість якраз й була використана фізичною особою – К. Устименком для прийняття відповідного рішення.

Отже, перше рішення КСУ щодо захисту прав людини – це рішення по справі Устименка.

2. У Рішенні наводиться офіційне тлумачення деяких положень Закону України «Про інформацію», що має велике значення у правотворчості та у правозастосуванні, шляхом тлумачення персональні дані відносяться до конфіденційної інформації, наголошується на важливості конституційного права на безпосереднє звернення до суду, розкривається обсяг регулювання операцій з інформацією медичного характеру тощо.

3. У пункті 3 резолютивної частини Рішення формулюється важливий конституційний принцип «винятки з конституційних норм встановлюються самою Конституцією, а не іншими нормативними актами», який має вирішальний вплив на порядок мотивації Рішення КСУ про скасування смертної кари 29 грудня 1999 року. Як зазначив КСУ у пункті 4 мотивувальної частини цього Рішення: «Конституційне забезпечення невід'ємного права на життя кожної людини, як і всіх інших прав і свобод людини і громадянина в Україні, базується на засаді: винятки стосовно прав і свобод людини і громадянина встановлюються самою Конституцією України, а не законами чи іншими нормативними актами».

Незважаючи на свою важливість, та певною мірою «канонічність», це Рішення є показовим щодо відсутності належного механізму його виконання, тобто являє собою «негативний» приклад відсутності в Україні цього механізму, що дозволяє вести розмову лише про наукове-практичне значення цього Рішення. По відношенню до громадянина К. Устименка це Рішення не має ніякого практичного ефекту. Тобто, знов таки, єдина можливість безпосереднього звернення до КСУ з метою захисту конституційних прав та свобод не має ніякого практичного ефекту саме через відсутність чітких положень процесуального законодавства, що дозволяє

переглянути попередні судові рішення з урахуванням рішення КСУ щодо офіційного тлумачення.

Відповідно до пункту 6 резолютивної частини: «Рішення Конституційного Суду України є обов'язковим до виконання на території України, остаточним і не може бути оскарженим». З позицій передової теорії конституційного права та відповідної практики не виникає сумнівів, що воно є обов`язковим для всіх суб`єктів права (йдеться про ту його частину, де дається офіційне тлумачення), а не тільки для громадянина К. Устименка. Останній звертався до КСУ не з метою задоволення наукового інтересу (хоча це також можна припустити), а для розв`язання конкретної правової колізії, необхідність у чому існувала поза яких сумнівів.

Тобто обов`язковість цього Рішення характеризується двома ознаками: 1) обов`язковість загальна – для всіх суб`єктів права, але не всього рішення, а його резолютивної частини, де надається тлумачення або формулюється правовий принцип, тобто КСУ, коли приймав рішення по конкретній справі – К. Устименка, сформулював певні правоположення, яким належить певна ступінь загальнообов`язковості; 2) обов`язковість особлива – для органів державної влади, у тому числі судових, які відповідно до Закону України «Про Конституційний Суд України», та, зокрема, статті 70, зобов`язані виконати це рішення на користь К.Устименка.

Як же суди виконують рішення КСУ щодо офіційного тлумачення по відношенню до фізичних та юридичних осіб, за ініціативою яких проблемні правові питання стали предметом розгляду єдиного органу конституційної юрисдикції? Відповідь не видається такою простою, оскільки у процесі виконання рішення по справі К.Устименка виявились внутрішні вади нашої судової системи:

«Ухвалою облсуду від 30.01.98, постановленою під головуванням судді А.П. Приходченко, яка брала участь у проголошенні ухвали 1994 року, подання прокуратури і заява Устименка відхилені.

Підставою відмови в перегляді справи суд назвав те, що офіційне тлумачення Конституційним Судом Закону «Про інформацію» по справі Устименка не може бути визнаним нововиявленими обставинами, оскільки це тлумачення не містить відомостей, про які на день проголошення ухвали від 21.02.94 не знали і не могли знати сторони і суд».

Відповідно до статті 343 Цивільного процесуального кодексу України 1963 року, що були чинними на момент проголошення ухвали (21.02.94):

«Рішення, ухвали і постанови, що набрали законної сили, можуть бути переглянуті у зв'язку з нововиявленими обставинами.

Підставами для перегляду рішень, ухвал і постанов у зв'язку з нововиявленими обставинами є:

1) істотні для справи обставини, що не були і не могли бути відомі заявникові;

2) встановлені вироком суду, що набрав законної сили, завідомо неправдиві показання свідка, завідомо неправильний висновок експерта, завідомо неправильний переклад, фальшивість документів або речових доказів, що потягли за собою постановлення незаконного або необгрунтованого рішення;

3) встановлені вироком суду, що набрав законної сили, злочинні дії сторін, інших осіб, які беруть участь у справі, або їх представників чи злочинні діяння суддів, вчинені при розгляді даної справи;

4) скасування рішення, вироку, ухвали або постанови суду чи постанови іншого органу, що стали підставою для постановлення даного рішення, ухвали чи постанови.»

Як ми бачимо, прийняття рішення КСУ щодо офіційного тлумачення не було підставою для перегляду судового рішення на той момент, оскільки воно не є нововиявленою обставиною у сенсі статті 343. Рішення також не є, зокрема, «істотною для справи обставиною». Ці положення були чинними й на момент винесення ухвали облсудом (30.01.98). Враховуючи традиційний позитивістський менталітет більшості українських суддів та виходячи з їх традиційної юридичної освіти, було важко очікувати від них певної сміливості заповнити існуючу прогалину у процесуальному законодавстві та виконати рішення КСУ шляхом перегляду попереднього рішення по справі К. Устименка судами загальної юрисдикції.

Ситуація суттєво не змінилась й після проведення «малої судової реформи», коли 21 червня 2001 року процесуальні кодекси України зазнали суттєвих змін. Так, наприклад, у Цивільному процесуальному кодексі України перегляду рішень, ухвал, що набрали законної сили, у зв'язку з нововиявленими та винятковими обставинами присвячується 42 глава. Так, у статті 347-2 цієї глави зазначається:

«Підставами для перегляду рішень і ухвал у зв'язку з нововиявленими обставинами є:

1) істотні для справи обставини, що не були і не могли бути відомі заявникові;

2) завідомо неправдиві показання свідка, завідомо неправильні висновки експертів, завідомо неправильний переклад, фальшивість документів або речових доказів, що потягло за собою ухвалення незаконного рішення, що встановлено вироком суду, який набрав законної сили;

3) злочинні дії сторін, інших осіб, які брали участь у справі, чи злочинні діяння суддів, вчинені при розгляді даної справи, встановлені вироком суду, що набрав законної сили;

4) скасування рішення, вироку або ухвали (постанови) суду чи постанови іншого органу, що стали підставою для постановлення цього рішення, цієї ухвали;

5) визнання неконституційним закону, який був застосований судом при вирішенні справи.

Підставами для перегляду справи за винятковими обставинами є виявлене після касаційного розгляду справи неоднозначне застосування (курсив автора – С.Ш.) судами загальної юрисдикції одного і того ж положення закону або його застосування всупереч нормам Конституції України, а також якщо у зв'язку з цими рішеннями міжнародна судова установа, юрисдикція якої визнана Україною, встановила факт порушення Україною міжнародних зобов'язань».

Причому, відповідно до статті 347-3 «заяви про перегляд рішень і ухвал у зв'язку з нововиявленими та винятковими обставинами можуть бути подані сторонами, іншими особами, які беруть участь у справі, та прокурором протягом трьох місяців з дня встановлення обставини, що є підставою для їх перегляду». Рішення чи ухвали переглядаються у зв'язку з нововиявленими обставинами судом, який їх постановив, а за винятковими обставинами – колегією суддів у складі суддів Верховного Суду України (стаття 347-4).

Отже, ми бачимо, що протягом майже 6-річного існування Конституційного Суду України, його рішення щодо офіційного тлумачення за конституційним зверненням фізичних та юридичних осіб не можуть бути належно виконані, якщо для цього необхідно додаткове рішення судів загальної юрисдикції. Відсутність такого положення можна знайти й у інших процесуальних кодексах України.

На мою думку, виходячи з аналогії закону, рішення КСУ щодо офіційного тлумачення є винятковою обставиною для перегляду справи судами загальної юрисдикції, оскільки неоднозначне застосування є підставою для конституційного звернення щодо офіційного тлумачення Конституції України та законів України відповідно до статті 94 Закону «Про Конституційний Суд України» від 16 жовтня 1996 року. Але, скоріше за все, судова практика України не розвивається за цим напрямком.

Отже, рішення КСУ по справі К. Устименка актуалізує величезну проблему виконання рішень КСУ щодо офіційного тлумачення за конституційним зверненням окремих осіб. Слід мати на увазі, що вони звертаються до КСУ не задля наукового або »спортивного» інтересу, а для вирішення конкретної життєвої проблеми правничими засобами. Якщо це проблемне питання не буде вирішено у найближчий час, діяльність КСУ щодо захисту конституційних прав та свобод матиме мінімальний ефект. Що й практично доведено у процесі невиконання рішення КСУ по справі К. Устименка.

ЗМІСТ

Наукове видання

СВОБОДА ІНФОРМАЦІЇ ТА ПРАВО НА ПРИВАТНІСТЬ В УКРАЇНІ

ТОМ 2

ПРАВО НА ПРИВАТНІСТЬ: CONDITIO SINE QUA NON

34(75)

Спеціальний випуск № 75 інформаційно-аналітичного
бюлетеня «Права людини»
Свідоцтво про реєстрацію Міністерства у справах друку та інформації
ХК №425 від 23.01.97.

Відповідальний за випуск та редактор *Євген Захаров*
Комп'ютерна верстка *Олександр Агєєв*

Підписано до друку 20.08.2004
Формат 60 х 84 1/16. Папір офсетний. Гарнітура Тип Таймс
Друк офсетний. Умов. друк. арк. 12,07 Умов. фарб.-від. 7,16
Умов.- вид. арк. 12,4 Наклад 1000 прим.

Харківська правозахисна група
61002, Харків, а/с 10430
http://www.khpg.org

«Фоліо»
61057, Харків, вул. Донець-Захаржевського, 6/8

Надруковано на обладнанні Харківської правозахисної групи
61002, Харків, вул. Іванова, 27, кв. 4