Органи внутрішніх справ – правоохоронні органи, які виконують такі функції:

– економічні – діяльність щодо захисту власності, економіки в цілому від злочинних посягань та ін.;

– екологічні

– охорони правопорядку – патрульної поліції;

– співробітництва у забезпеченні світового порядку – участь у діяльності Інтерполу.

Органи юстиції – органи виконавчої влади, призначенням яких є організація здійснення державної правової політики:

– розробка проектів законів, здійснення систематизації законодавства;

– забезпечення організаційної діяльності судів;

– керівництво нотаріатом, судово-експертними установами, державною виконавчою службою та ін.;

– організація правового навчання населення;

– реєстрація політичних партій та інших об'єднань громадян, а також нормативних актів міністерств та відомств.

Отже, можемо констатувати, що в умовах перехідного періоду робота правоохоронних органів стає одним з пріоритетних напрямків державної діяльності. Виражаючи сутність сучасної держави, вона спрямована на вирішення завдань щодо забезпечення охорони конституційного ладу, прав і свобод громадян, усіх установлених та врегульованих правом суспільних відносин. Тому належна її реалізація повинна стати запорукою гармонійного розвитку суспільства та побудови правової держави.

Одержано 12.10.2017

УДК 342.72

Віталій Олександрович СЕРЬОГІН,
професор кафедри конституційного і муніципального права юридичного факультету Харківського національного університету імені В. Н. Каразіна, доктор юридичних наук, професор

ГРУПОВИЙ ПРОФАЙЛІНГ ЯК ЗАГРОЗА ІНФОРМАЦІЙНОМУ ПРАЙВЕСІ

Використання інтернет-сайтів, як правило, є безкоштовним, тобто інформація на них зазвичай доступна без будь-яких витрат. Проте останнім часом існує тенденція до того, що багато компаній, котрі працюють в Інтернеті, надають доступ до своїх веб-сайтів

лише тоді, коли користувач заповнить електронну форму заявки, де вказується ім'я, адреса, адреса електронної пошти тощо. Інформація, яку користувач надає про себе, реєструється і використовується для певних цілей. Ці дані іноді поєднуються з даними про інтернет-серфінг і потім використовуються для виявлення певних характеристик методами так званого добування даних (англ. Data Mining) – виявлення прихованих закономірностей або взаємозв'язків між змінними у великих масивах необроблених даних. З отриманих результатів виводяться групові профілі, котрі показують властивість або комплекс властивостей певної групи людей.

Групові профілі є дуже корисними й ефективними для прямого маркетингу, втім вони можуть мати негативні наслідки для інформаційного прайвесі долучених до таких профілів людей.

Для споживача такий підхід може бути цікавим, адже він більше не повинен отримувати пропозиції на продукти, в яких не зацікавлений, тоді як збільшення пропозицій на товари, в яких він насправді зацікавлений, полегшує порівняння цін. Однак у цьому є й певні недоліки. Коли люди розглядаються як члени групи, вони більше не можуть контролювати інформацію про себе. Інформація про більшість учасників групи може бути використана для прогнозування характеристик членів групи, про яких немає інформації. Натомість люди, які належать до групи, котра для маркетингу є нецікавою, взагалі не отримують жодних пропозицій. Адреса електронної пошти користувача розміщується в списках розсилки, в результаті він починає отримувати всі види спеціальних пропозицій електронною поштою. Інша, навіть більша, загроза полягає в тому, що особа може бути позбавлена можливості користування певними продуктами або послугами. У суспільстві, в якому більшість покупок здійснюється через Інтернет, це може стати проблемою для значних груп людей.

Звичайно, існують закони та правила конфіденційності, які допомагають уникнути деяких проблем. Одна, існує кілька випадків, коли ці закони є неефективними навіть для держав ЄС, де рівень захисту інформаційного прайвесі вважається найвищим у світі. Принципи захисту інформаційного прайвесі, закріплені в Європейській директиві 95/46/EG від 24 жовтня 1995 р., відповідають Керівним принципам Організації економічного співробітництва та розвитку і зводяться до таких вимог: 1) всі дані повинні бути отримані на законних підставах за згодою суб'єкта; 2) дані повинні бути актуальними, точними та повними; 3) мета

зібраних даних має бути розкрита, і дані можуть використовуватися лише для цієї мети; 4) дані не можуть бути розкриті стороннім особам без згоди суб'єкта; 5) необхідно вживати розумних запобіжних заходів щодо втрати, розкриття інформації, її знищення тощо; 6) суб'єкт повинен мати можливість знати про використання та цілі своїх даних; 7) суб'єкт має право виправити чи видалити свої дані; 8) збирач даних несе відповідальність за дотримання вищезазначених принципів.

Як бачимо, Європейська директива 95/46/EG захищає, як і попереднє законодавство, лише особисті дані, тобто ті, що містять відомості стосовно ідентифікованої чи такої, що може бути ідентифікована, фізичної особи. Це явно виключає дані щодо юридичних осіб та осіб, які не можуть бути ідентифіковані. Як наслідок, проблемними залишаються питання, коли дані вважаються ідентифікуючими. Дані про неідентифікованих осіб на сьогодні не захищені законодавством про інформаційне прайвесі. Звичайно, захистити анонімні дані досить важко. Проте деякі засоби захисту повинні бути введені. Річ у тім, що створення групових профілів, тобто вибір, стигматизація та конфронтація, суперечать принципам справедливого правосуддя та поводження щодо груп людей.

Не слід шукати вирішення даної проблеми з точки зору колективної конфіденційності, оскільки групи, залучені до групових профілів, не мають структури та організації. На сьогодні більш прогресивною виглядає концепція так званого «категоричного прайвесі». Це новий аспект інформаційного прайвесі, що в основному ґрунтується на концепціях особистої конфіденційності, але включає конфіденційність інформації, яка більше не може слугувати ідентифікатором людини, але може мати негативні наслідки для членів групи. «Категоричне прайвесі» стосується інформації, до якої застосовуються наступні умови:

1. Інформація була спочатку взята з особистої сфери фізичних осіб, але більше не слугує ідентифікатором окремих фізичних осіб, але, замість цього, використовується як ідентифікатор груп осіб.

2. При додаванні до ідентифікаторів груп і при розголошенні така інформація може призвести до таких самих негативних наслідків для членів групи, як це було б для окремої фізичної особи, якби інформація супроводжувалась ідентифікаторами цієї особи.

Такий підхід, на наш погляд, може слугувати підвищенню ефективності захисту інформаційного прайвесі і як такий потребує закріплення на законодавчому рівні.

Одержано 12.10.2017