ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ТА ПРАВИЛА ПРИВАТНОСТІ ПРИ ДОСЛІДЖЕННЯХ В ІНТЕРНЕТ

ВОЛОДИМИР КОЗАК,
Заступник Голови Державної служби України з питань захисту персональних даних
Volodymyr.kozak@zpd.gov.ua
044 517 85 86

Маркетинг є обов'язковою складовою сучасного ведення бізнесу. Питання: «Хто є Ваш споживач?» - це перше питання, відповідь на яке повинен знати будь-який підприємець. В свою чергу це вимагає проведення постійних досліджень з метою отримання інформацій про клієнта, його вподобань, особливостей його поведінки тощо. Як погодити це з вимогами невтручання в особисте життя людини, дотримання поваги до приватного інформаційного простору? Особливу гостроту це питання набрало останнім часом, коли все більше осіб почали користуватися Інтернетом, стрімко розвиватися соціальні мережі.

Уперше тема захисту особи прозвучала в Загальній декларації прав людини[1], прийнятій на третій сесії Генеральної Асамблеї ООН і підписаній 10 грудня 1948 року. У Декларації стверджувалося, що ніхто не може зазнавати безпідставного втручання в його особисте, сімейне життя, безпідставного посягання на недоторканність його житла, таємницю його кореспонденції або на його честь і репутацію; кожна людина має право на захист від такого втручання або таких посягань. У 1973 році Українська Радянська Соціалістична Республіка ратифікувала цю Декларацію. Хоча слід зауважити, що ця норма не особливо використовувалася громадянами для захисту своїх прав.

Згодом у Конвенції про захист прав людини і основоположних свобод[2], підписаній 4 листопада 1950 року (ратифікована Україною із заявами та застереженнями 17 липня 1997 року, набула чинності 11 вересня 1997 року), приблизно ті ж слова повторилися в статті 8 «Кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції. Органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві, в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб».

Європейські норми — це не певний перелік незмінних документів, а базові принципи, відображені в документах, що розвиваються відповідно до політичних

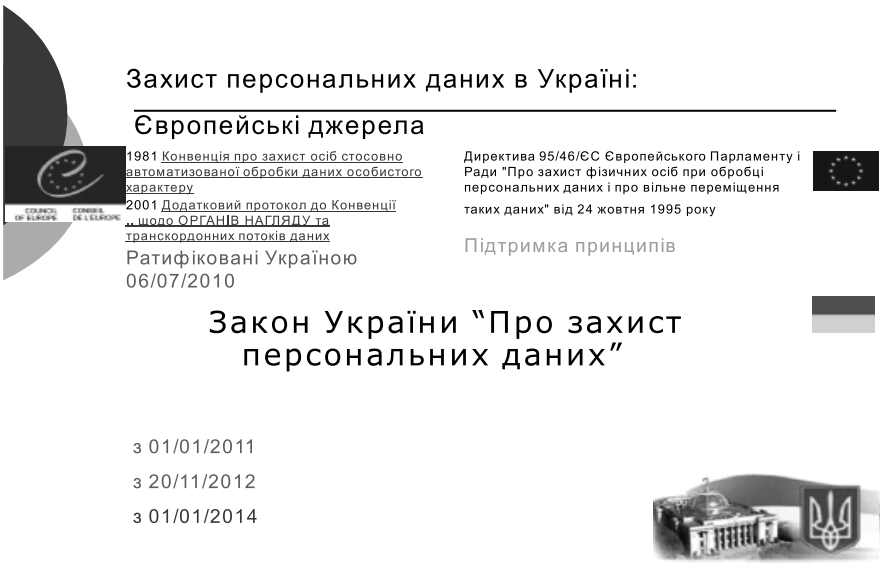
[1] http://zakon4.rada.gov.ua/laws/show/995_015
[2] http://zakon4.rada.gov.ua/laws/show/995_004

реалій та рівня розвитку технологій. Тому сказати, чи відповідають норми законодавства України нормам європейським, — цього мало. Треба аналізувати кожен аспект, який є в законодавстві.

Норми про захист прав людини містяться у статті 32 Конституції України[3]: «Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини».

Указана норма Конституції діяла увесь цей час і діє, звичайно, зараз. Крім того, різні закони тією чи іншою мірою були спрямовані на її імплементацію. Зокрема, є норма про лікарську таємницю, таємницю усиновлення, адвокатську таємницю і т. д. Тобто в різних законах відбивалась потреба захищати приватне життя. Не було лише спеціального закону. І такий закон з'явився. Ним став Закон «Про захист персональних даних»[4], який був прийнятий 1 червня 2010 року, практично одночасно із ратифікацією Конвенції про захист осіб стосовно автоматизованої обробки даних особистого характеру (далі – Конвеції 108). Вона була ратифікована Законом[5] від 6 липня 2010 року і є частиною українського законодавства. У принципі, все, що закладено в цій Конвенції, може використовуватися в нашому житті.

Чому був прийнятий Закон «Про захист персональних даних»? Насамперед тому, що Україна долучилася до процесу підписання документів з Європейським Союзом. А оскільки в Конституції України питання захисту персональних даних теж вирішувалося, то й не було жодних заперечень проти прийняття спеціального закону. Слід зауважити, що протягом минулого року, коли почав діяти Закон «Про захист персональних даних», було багато контраверсійних думок і пропозицій щодо внесення змін до нього.



[3] http://zakon4.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80
[4] http://zakon4.rada.gov.ua/laws/show/2297-17
[5] Закон України «Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних http://zakon2.rada.gov.ua/laws/show/2438-17/print1361278834285429

У Законі «Про захист персональних даних» використовуються положення, які існують у Директиві 95/46/ЄС[6] Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 року. Слід зазначити, що Директива 95/46/ЄС для країн ЄС є базовим документом, а у кожній країні її положення імплементуються національним законодавством. Тобто вона не є нормативним актом прямої дії.

І. Персональні дані[7]

Відповідно до статті 2 Закону України «Про захист персональних даних», «персональні дані - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована». Це визначення майже тотожне визначенню, поданому в Конвенції 108 і Директиві 95/46/ЄС.

Порівняйте визначення у Законі «Про захист персональних даних» та Директиві 95/46/ЄС. Вони практично не відрізняються.

«...відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована...»

Закон України «Про захист персональних даних»

«...будь-яка інформація, що стосується встановленої фізичної особи чи фізичної особи, яку можна встановити...»
Директива 95/46/ЄС

Визначення надзвичайно широке. Воно не є конкретним і бути таким не може. За 30 років з часу підписання 28 січня 1981 року Конвенції 108 багато чого змінилося. Те, що не було персональними даними, стало ними завдяки стрімкому розвитку інформаційних технологій.

Таким чином, поняття має бути настільки широким, щоб охопити всі процеси обробки відомостей про особу, які існують сьогодні, про які ми знаємо, і ті процеси, які настануть завтра і які підпадатимуть під це визначення.

Визначення поняття «персональні дані» розберемо більш детально. Воно складається з чотирьох частин:

1) «відомості чи сукупність відомостей»;
2) «про фізичну особу»;
3) «фізична особа»;
4) «ідентифікована або може бути конкретно ідентифікована».

«Відомості чи сукупність відомостей...»

За природою відомості чи сукупність відомостей про особу можуть мати об'єктивний або суб'єктивний характер.

Наприклад, об'єктивна інформація: аналіз крові особи, кардіограма, заробітна плата, зафіксована у відомості, та ін.

Суб'єктивна інформація, наприклад службова характеристика. Вона може відображати суб'єктивну точку зору того, хто її написав, скажімо, керівника, у якого може бути конфлікт з працівником. Але від цього інформація не перестає бути персональною інформацією, тому що вона стосується безпосередньо того, про кого написана характеристика.

За змістом відомості можуть відображати приватне чи сімейне життя або заняття особи. Тобто це можуть бути відомості, пов'язані з трудовими відносинами, соціальною поведінкою, або такі, що свідчать про те, замовником чи виконавцем є особа, і т. д.

Водночас, незалежно від того, у якій сфері виникають відносини, які вимагають обробки відомостей про особу, такі відомості є персональними даними.

[6] Директива 95/46/ЄС Європейського Парламенту і Ради" Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних" від 24 жовтня 1995 року. http://zakon4.rada.gov.ua/laws/show/994_242/print1360150843706940

[7] Використовуються рекомендації ARTICLE 29 - DATA PROTECTION WORKING PARTY WP 136 Opinion 4/2007 on the concept of personal data http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

Окремо виділяють так звану «чутливу інформацію». У Законі «Про захист персональних даних» встановлено особливі вимоги до обробки певних категорій персональних даних. Це відомості про расове, етнічне походження, політичні, релігійні, світоглядні переконання, здоров'я, статеве життя, членство у політичних партіях, профспілках.

Слід зауважити, що в Конвенції 108 до «чутливої інформації» відносять і «відомості про судимість».

Відомості про особу можуть бути будь-якими за формою. Очевидно, що найбільш часто використовується, чи зустрічається, алфавітно-цифровий формат: таблиці, тексти, повідомлення і т. д., тобто те, що зручно обробляти в такому вигляді засобами автоматизованої обробки.

Може бути графічний формат: графіки, шаржі, карикатури, фото, звукові записи, а також відеозаписи, кінозаписи і т. д.

Незалежно від того, в якому форматі інформація зберігається, в якому середовищі вона обробляється: чи це відеозображення, чи паперові носії, чи просто обробка файлів у комп'ютерній системі, — все одно ця інформація є персональними даними.

«...ПРО фізичну особу,...»

Відомості можуть стосуватися фізичної особи безпосередньо або опосередковано. Безпосередньо - це коли, наприклад,йдеться про чиюсь конкретну особову справу, скажімо, Іваненка Івана Івановича. Або, наприклад, про історію хвороби Петренка, або банківський рахунок з номером, ідентифікаційним кодом конкретної особи.

Однак часто бувають випадки, коли інформація стосується нас опосередковано. Наприклад, ведеться реєстр нерухомого майна, а з цим майном пов'язані особи, які є його власниками, які його обслуговували або робили ремонт. Опосередковано ці відомості стосуються і цих людей.

Або, скажімо, ведеться відеоспостереження у супермаркеті. Ніхто там не здійснює відеоспостереження за конкретною особою, а лише за торговим залом. Але якщо ми проходимо у торговому залі, то залишається не лише наше відеозображення, а й інформація про те, коли і з ким ми були в магазині, які товари купували, які роздивлялися, який у нас був настрій у цей час, який номер набирали по телефону, та багато іншої інформації.

«...про ФІЗИЧНУ ОСОБУ,...»

Відповідно до статті 24 Цивільного кодексу України «Людина як учасник цивільних відносин вважається фізичною особою».

Інформація про померлу людину не є її персональними даними.

Цивільна правоздатність фізичної особи виникає в момент її народження і припиняється в момент смерті.

«Інтереси зачатої, але ще не народженої дитини» можуть бути визнані як інтереси фізичної особи. Це означає, що персональні дані про протікання вагітності у деяких випадках можуть розглядатися не лише як персональні дані мами, а як персональні дані особи, яка потім виросла і досягла відповідного віку.

Приклад

Суд однієї з європейських країн визнав, що нанесено шкоду особі, дитячі малюнки якої залишились в дитячому садочку і були згодом використані. Особа виросла, знайшли її малюнки, роздрукували, і психологи за малюнками (проаналізувавши, де хатинка намальована – справа, зліва, зверху, яким шрифтами) зробили психологічний портрет цієї особи. Це було визнано незаконним втручанням у приватне життя.

«...Ідентифікована або може бути

конкретно ідентифікована»

Особа може бути ідентифікована прямо і опосередковано. Якщо на якомусь документі чи у файлі вказано прізвище, ім'я, по батькові або якась додаткова інформація, дата народження, фото, місце народження, то, зрозуміло, особу можна прямо ідентифікувати.

Закон «Про захист персональних даних» містить фразу: «може бути конкретно ідентифікована». Для визначення того, чи можна особу встановити, мають враховуватися всі засоби, використання яких ймовірно очікувати для її встановлення. До початку обробки персональних даних той, хто їх обробляє, зобов'язаний визначити, які дані будуть вважатися персональними.

Не слід забувати, що якщо до персональних даних відносити дуже багато інформації, то, відповідно, збільшаться затрати на їх обробку і захист, якщо ж перелік таких даних звести до мінімуму, то існуватимуть ризики, що можна випадково завдати шкоду фізичним особам.

Приклад:

Стосовно такого поняття, як «IP-адреса» в європейських країнах відбувалися суди, які визнавали, що IP-адреса— це персональні дані особи. Останній суд був у листопаді позаминулого року. Позов на користувача, який незаконно «завантажував» музику, подала компанія, яка захищає права власності на музичні твори. Щоб знайти цього користувача, треба було з'ясувати, яка у нього IP-адреса. Суд визнав, що нема підстав для видачі IP-адреси, оскільки це приватні персональні дані користувача. Тобто в черговий раз було визнано, що IP-адреса- це персональні дані.

В Україні більшість телекомунікаційних компаній погодилися, що номер телефону і номер мобільного абонента, навіть того, який не уклав письмову угоду, а використовує послуги передоплаченого зв'язку, придбавши стартовий пакет, - це персональні дані. У цьому випадку особа може бути досить просто ідентифікована. Найпростіший спосіб ідентифікації - зателефонувати за номером і запитати: «Ви хто?»

Можуть бути, звичайно, значно складніші процедури ідентифікації, але все ж при певних зусиллях особа може бути ідентифікована. Визначення персональних даних є сталим, але із змінами технологій змінюється відомості, які відносяться до персональних даних. Наприклад, обробка біометричних та генетичних даних, кілька десятків років тому вимагала значних ресурсів, ніхто не вважав генетичний код персональними даними. А на сьогодні застосування методів ідентифікації фізичних осіб з використанням генетичного коду є досить поширеним, і при цьому, безумовно здійснюється обробка персональних даних.

У Директиві 95/46/ЄС є таке положення: «Для визначення того, чи можна особу встановити, повинні враховуватися всі засоби, використання яким контролером (володільцем) чи будь-якою іншою особою ймовірно очікувати для встановлення вищезгаданої особи». Це означає, що різні суб'єкти мають можливість використовувати різні засоби для встановлення особи.

Тобто в різних ситуаціях підхід до процедури ідентифікації буде різний. У більшості випадків не викликає жодних сумнівів, що реєстрація на будь-якому сайті без конкретного прізвища, а лише за псевдонімом - є обробкою персональних даних.

В Україні сумлінне виконання Закону щодо захисту персональних даних для бізнесу є справою скоріше репутаційного характеру, ніж побоювання незначних штрафів у випадку порушення положень щодо обробки персональних даних.

Приклад В Україні провадяться дослідження лікарських засобів. У відповідних медичних документах є закодована інформація про особу, яка погодилася брати участь у дослідженні. Згодом інформація про перебіг її хвороби, про те, як ліки діяли на піддослідного, передається у компанію, яка замовила дослідження. І хоча в документах, переданих замовникові, не зазначено прізвищ та імен, але за кодом, назвою лікувального закладу при певних умовах можна ідентифікувати особу.

II. Принципи обробки та захисту персональних даних [28]

Закон України «Про захист персональних даних» встановлює вимоги до обробки та захисту персональних даних. Зазначені вимоги відображають положення, запроваджені Конвенцією 108 та розвинуті у Директиві 95/46/ЄС. Зручно представити всю сукупність вимог щодо захисту персональних даних у рамках восьми базових принципів обробки персональних даних. Персональні дані повинні:

- оброблятися сумлінно і законно (за наявності підстав та з дотриманням вимог);
- отримуватися із конкретними законними цілями та не оброблятися у способи, несумісні із цими цілями;
- бути адекватними, не надлишковими, відповідати цілям обробки;
- бути точними та своєчасно оновлюватися;
- не зберігатися довше, ніж це необхідно;
- оброблятися з дотриманням прав фізичної особи, включаючи право на доступ до даних;
- оброблятися з дотриманням вимог щодо захисту інформації;
- не передаватися за межі країни без відповідного захисту.

Розглянемо більш детально кожен із вищезазначених принципів.

1. Принцип законності обробки

Персональні дані повинні оброблятися сумлінно й законно, за наявності підстав та з дотриманням вимог. У Законі України «Про захист персональних даних» говориться, що персональні дані повинні оброблятися законно (п. 8 ст. 6). Слід зауважити, що європейські експерти вказують на відсутність у нашому Законі норми про те, що персональні дані мають оброблятися чесно. У Великій Британії, наприклад, чітко виписано критерії «чесності» обробки персональних даних. Від того, наскільки повно і детально в організації прописано й реалізовано процедури обробки персональних даних, залежить розмір штрафних санкцій у разі виявлення порушень.

Проект документу, який може замінити чинну нині Директиву 95/46/ЄС,- Генеральний регламент щодо захисту персональних даних, містить, вимоги про необхідність запровадження стандартизації, сертифікації у сфері захисту персональних даних, тобто елементів оцінки відповідності, з позначенням рівнів захисту. Вказаним Генеральним регламентом передбачається також необхідність розробки, спеціально для захисту персональних даних у тих чи інших інформаційних системах, технічних і програмних засобів (data protection by design) та налаштування за замовчуванням (by default) засобів загального користування, наприклад інтернет-оглядачів, таким чином, щоб персональні дані користувачів були максимально захищені. При цьому, звичайно, будуть запроваджуватися й процедури оцінки відповідності таких засобів установленим вимогам.

Закон України «Про захист персональних даних» вимагає обробляти персональні дані «законно», тобто на законних підставах. Закон визначає такі підстави обробки персональних даних:

- дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень;
- укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на користь суб'єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних;
- згода суб'єкта персональних даних на обробку його персональних даних;
- захист життєво важливих інтересів суб'єкта персональних даних;
- необхідність захисту законних інтересів володільців персональних даних, третіх осіб, крім випадків, коли суб'єкт персональних даних вимагає припинити обробку його персональних даних та потреби захисту персональних даних переважають такий інтерес.

Закони встановлюють випадки, коли обробка персональних даних може здійснюватися в інтересах національної безпеки, економічного добробуту та прав людини без згоди особи. Наприклад, Законом України «Про оперативно-розшукову діяльність»[8] передбачається у визначених випадках збирання та вивчення документів і даних, що характеризують спосіб життя окремих осіб, підозрюваних у підготовці або вчиненні злочину, джерело та розміри їх доходів.

Цивільним кодексом України (далі - ЦКУ) допускається використання без згоди особи її імені для висвітлення її діяльності або діяльності організації, в якій вона працює чи навчається, що ґрунтується на відповідних документах (стенограми, протоколи, аудіо-, відеозаписи, архівні матеріали тощо).

Без згоди фізичної особи - боржника, якщо інше не встановлено договором або законом, може здійснюватися, відповідно до ЦКУ, заміна кредитора у зобов'язанні, а отже, і передача первісним кредитором новому кредитору документів, які засвідчують права, що передаються, та інформації, яка є важливою для їх здійснення.

Виключно законами запроваджуються загальнодержавні реєстри, збір відомостей про осіб до яких є обов'язковим для встановлених категорій цих осіб.

Якщо в законі є конкретна підстава для обробки персональних даних, тоді не потрібна згода. Підзаконні акти повинні лише прописувати процедури збору та обробки персональних даних. На сьогодні низка чинних нормативно-правових актів органів державної влади, прийнятих до набуття чинності Закону України «Про захист персональних даних» установлюють не лише процедури обробки відомостей про фізичних осіб, а й подекуди визначають обов'язковість обробки персональних даних певних категорій осіб. Здійснюється приведення їх у відповідність до положень Закону України «Про захист персональних даних».

Іншою законною підставою для обробки персональних даних є згода особи, надана відповідно до сформульованої мети обробки; щодо обсягу персональних даних, які можуть бути включені до бази персональних даних; щодо доступу до персональних даних третіх осіб; щодо передачі персональних даних про фізич-

[8] http://zakon1.rada.gov.ua/laws/show/2135-12/print1374158310204843

ну особу з бази персональних даних і передачу персональних даних іноземним суб'єктам. Тобто згода - це не якийсь один документ, у якому написано, наприклад, «...даю згоду на обробку моїх персональних даних з будь-якою метою». Схожі формулювання на практиці інколи трапляються, але вони не відповідають жодним вимогам.

У Законі України «Про захист персональних даних» визначено, що згода повинна бути документована, зокрема письмова. Отже, вимога щодо виключно письмової згоди є необов'язковою. Документована процедура - це встановлений спосіб проведення певної діяльності чи процесу; процедура, визначена певним документом; процедура, яка встановленим порядком введена в дію.

Відповідно до статті 205 ЦКУ правочин, для якого законом не встановлена обов'язкова письмова форма, вважається вчиненим, якщо поведінка сторін засвідчує їхню волю до настання відповідних правових наслідків.

Тобто якщо на підприємстві, в організації, установі документовано встановлена процедура стосовно того, в яких випадках певні дії певного суб'єкта є згодою, то ця процедура може бути використана для констатації факту, що документовану згоду на обробку персональних даних цього суб'єкта було надано, а отже, обробка персональних даних є законною. Підтвердженням цього може бути такий приклад: отримуючи чеки у крамницях, ми ж не пишемо щоразу: «Я даю згоду на те, щоб мені виписали чек». Це і так абсолютно зрозуміло з наших дій.

Форми надання згоди можуть бути різними, зокрема, це можуть бути документи на паперових носіях з реквізитами або електронні документи, засвідчені електронно-цифровими підписами, або документи з реквізитами на будь-яких інших носіях. Наприклад, документи, створені з допомогою фото-, відео- або аудіофіксації. Останній вид документів широко використовується в банківській сфері.

Формою надання згоди може бути, наприклад, відмітка на електронній сторінці документа чи в електронному файлі, що обробляється в інформаційній системі на основі документованих програмно-технічних рішень, які не дозволяють обробку персональних даних до того часу, поки суб'єкт не виконає дії, щоб підтвердити надання їм згоди, і забезпечують реєстрацію дій суб'єкта персональних даних та цілісність протоколів реєстрації таких дій. У принципі, така процедура надання згоди певною мірою рекомендована Типовим порядком обробки персональних даних у базах персональних даних[9].Зазвичай, відвідувачі веб-ресурсів надають поінформовано згоду на збір та обробку відомостей про них, ознайомившись із політикою захисту персональних даних на сайті та зробивши відмітку про згоду з цією політикою.

Підстави для обробки «чутливих» даних:

1) однозначна згода суб'єкта;
2) обов'язки у сфері трудових правовідносин;
3) захист інтересів:
   - суб'єкта;
   - іншої особи у разі недієздатності суб'єкта;
4) обробка персональних даних членів (осіб, що підтримують контакти):
   - релігійними та громадськими організаціями;
   - політичними партіями та професійними спілками;
5) дані вже були оприлюднені суб'єктом;

[9] Типовий порядок обробки персональних даних у базах персональних даних. Затверджено наказом Міністерства юстиції України від 30.12.2011 N 3659/5. Зареєстровано в Міністерстві юстиції України 3 січня 2012 р. за N1/20314 http://zakon4.rada.gov.ua/laws/show/z0001-12/print1360150843706940

6) задоволення або захист правової вимоги;
7) дані стосуються:
   - звинувачень у вчиненні злочинів, вироків суду;
   - оперативно-розшукової чи контррозвідувальної діяльності;
   - боротьби з тероризмом;
8) забезпечення лікування (обробка медичним працівником)[28].

Обробка відомостей про расове, етнічне походження, політичні, релігійні, світоглядні переконання, здоров'я, статеве життя, членство в політичних партіях, профспілках (так звані «чутливі» дані) здійснюється за умов надання однозначної згоди на обробку персональних даних. Державна служба України з питань захисту персональних даних рекомендує обробляти такі «чутливі» персональні дані за умов надання письмової згоди.

Форми надання згоди:

- документ на паперовому носії з реквізитами, що дає змогу ідентифікувати цей документ та фізичну особу. Добровільне волевиявлення суб'єкта персональних даних засвідчується його підписом
- електронний документ, включаючи обов'язкові реквізити документа, що дають змогу ідентифікувати цей документа фізичну особу. Добровільне волевиявлення фізичної особи щодо надання дозволу на обробку її персональних даних засвідчується електронним підписом суб'єкта персональних даних
- документ з реквізитами на будь-якому іншому носії,зокрема фото - відео-, аудіофіксація добровільного волевиявлення суб'єкта персональних даних
- відмітка на електронній сторінці документа чи у електронному файлі,що обробляється в інформаційній системі на основі документованих програмно-технічних рішень, які, у свою чергу не дозволяють обробки персональних даних до того часу, поки суб'єкт персональних даних не виконає дії, що підтверджують надання ним відповідної згоди та забезпечують реєстрацію дій суб'єкта персональних даних та цілісність протоколів реєстрації таких дій.

2. Принцип конкретності мети обробки персональних даних

Персональні дані повинні отримуватися для конкретної законної мети і не оброблятися у спосіб, не сумісний із цією метою. Таким чином, з якою метою персональні дані збираються, з такою метою вони і повинні оброблятися. При цьому суб'єкт, по-перше, має знати, з якою метою він надає свою згоду. При наданні згоди суб'єкт має право зробити зауваження, що частіше всього на практиці зводиться до того, що суб'єкту надається якась альтернатива, він може вибрати якийсь варіант із загального переліку.

Якщо обробка персональних даних не відповідає конкретно визначеним при наданні згоди цілям, суб'єкт персональних даних може застосовувати засоби правового захисту.

3.Принцип пропорційності

Персональні дані повинні бути адекватними, не надмірними, відповідати меті обробки.

Що означає - бути «адекватними, не надмірними»? Наприклад, для чого житлово-експлуатаційному підприємству або готелю можуть знадобитися відомості про місце роботи осіб? Для чого в анкетах при отриманні дисконтних карт точно знати вік покупця, а то й дату його народження? Адже частіше використовується лише вікова категорія.

Зрозуміло, що під час прийняття на роботу треба надавати певні документи, відомості особистого характеру тощо. Але кількість оброблюваних персональних даних повинна відповідати меті обробки.

У будь-якому разі, якщо обробляються персональні дані, треба знати, для чого ті чи інші дані потрібні, та й спосіб обробки повинен відповідати цілям обробки.

4. Принцип якості даних

Персональні дані мають бути точними і своєчасно оновлюватися.

Це означає, що повинна бути встановлена процедура оновлення цих даних. Якщо це, наприклад, дисконтна програма, то відомості повинні періодично оновлюватися. Має бути встановлена процедура підтримки точності й оновлення персональних даних.

5. Принцип обмеження терміну обробки даних

Персональні дані повинні оброблятися у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, у строк, не більший, ніж це потрібно відповідно до їх законного призначення.

У деяких випадках законодавство визначає, який період часу зберігаються та обробляються персональні дані. Наприклад, копія паспорта, яку здають під час обміну валюти, зберігається, відповідно до банківської процедури, п'ять років, а тоді має бути знищена; певний час зберігаються відомості про відеоспостереження в магазині. А це означає, що має бути прописана процедура знищення цих відомостей. Якщо цієї процедури немає - це теж порушення.

6.Принцип прозорості та опозиції.

Закон України «Про захист персональних даних» установлює права суб'єктів персональних даних.

Кожен має право знати, хто і де обробляє його персональні дані (ст. 8 Закону України «Про захист персональних даних»). Здавалося б, це дуже просто, а насправді - це не зовсім так. Якщо проаналізувати будь-які анкети, у 30% з них не зазначається, хто збирає персональні дані. Така сама ситуація і з відеоспостереженням. Коли ми заходимо в супермаркет або в офіс, ми не знаємо, хто веде відеозапис. Це може бути охорона супермаркету або і фірми чи інша компанія, яка орендує тут приміщення. Коли ми відвідуємо інтерактивний сайт, то часто не знаємо, хто саме і для чого збирає у себе персональні дані. І таких прикладів безліч

Основним у таких випадках є те, що коли хтось узявся обробляти персональні дані, він має забезпечити, щоб особи, чиї дані обробляються, знали, хто це робить і де. З точки зору суб'єкта персональних: даних важливо, щоб він знав, до кого звернутися, щоб вимагати захисту своїх прав. Суб'єкт має право знати, кому передаються його персональні дані, з якою метою вони обробляються, він: повинен знати, як отримати доступ до своїх персональних даних, та мати можливість отримати цей доступ без пояснення причин. Доступ до персональних даних суб'єкта надається йому безкоштовно.

Ще раз нагадаємо, що кожен має право вимагати знищення чи виправлення своїх персональних даних, якщо вони обробляються незаконно чи є недостовірними. Кожен має право звертатися з питань захисту своїх персональних даних до уповноваженого органу з цього питання, а також застосовувати засоби правового захисту, тобто звертатися до суду.

7.Персональні дані повинні оброблятися з дотриманням вимог щодо захисту інформації.

Інформаційна система, в якій обробляються персональні дані, має бути належним чином захищена (п. 7 ст. 8 Закону України «Про захист персональних даних»).

У простих випадках - це забезпечення доступу до приміщень та до інформаційних систем лише осіб, які мають на це право, розмежування доступу з використанням паролів, реалізація мінімальних вимог щодо реєстрації подій в інформаційній системі відповідно до встановлених на підприємстві процедур. Для великих підприємств та й для малих підприємств, які ставлять за мету мінімізувати ризики, - це створення й незалежна оцінка системи управління інформаційною безпекою відповідно до міжнародних і національних стандартів, створення й оцінка комплексних систем захисту інформації в інформаційно-телекомунікаційних системах, застосування широкого переліку рекомендованих заходів. Це питання - складне і потребує окремого викладення.

8. Обмеження передачі даних іноземним суб'єктам.

Передача персональних даних іноземним суб'єктам відносин, пов'язаним із персональними даними, здійснюється лише за умов забезпечення належного захисту персональних даних.

Не всі країни, з якими співпрацюють українські підприємства, підписали і ратифікували Конвенцію 108, і не всі країни мають законодавство, спрямоване на захист персональних даних. У такому випадку передача персональних даних можлива лише за умов виконання імпортером персональних даних контрактних зобов'язань, визначених експортером даних. Відповідальність за дотримання вимог закону стосовно захисту персональних даних покладається на експортера даних, який у договорі з імпортером даних передбачає низку взаємних зобов'язань і процедур, спрямованих на дотримання цих зобов'язань.

У разі передачі персональних даних у країни, які ратифікували Конвенцію 108 і мають законодавство, спрямоване на захист персональних даних, також доцільно у договорі визначити низку важливих зобов'язань щодо дотримання кожною зі сторін вимог законодавства, чітко визначити процедури, спрямовані насамперед на забезпечення дотримання прав суб'єктів персональних даних.

Суб'єкт персональних даних має право отримувати інформацію про умови надання доступу до персональних даних, інформацію про третіх осіб, яким передаються персональні даних, а отже, і до контрактних положень, які визначають процедури передачі персональних даних про нього за кордон.

III. Суб'єкти відносин і база персональних даних

Хто є суб'єктами відносин, пов'язаних із персональними даними? Хто, власне, обробляє персональні дані? Закон України «Про захист персональних даних» вводить такі поняття:

володілець персональних даних — фізична або юридична особа, якій законом або за згодою суб'єкта персональних даних надано право на обробку цих даних, яка затверджує мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом.

- розпорядник персональних даних — фізична чи юридична особа, якій володільцем бази персональних

даних або законом надано право обробляти ці дані.

- третя особа — будь-яка особа, за винятком суб'єкта персональних даних, володільця чи розпорядника бази персональних даних та уповноваженого державного органу з питань захисту персональних даних, якій володільцем чи розпорядником бази персональних даних здійснюється передача персональних даних відповідно до закону.

Володілець (у документах з питань захисту персональних даних Ради Європи та Європейського Союзу — «контролер, англійською controller») — юридична або фізична особа, яка обробляє персональні дані від свого імені. Це може бути організація або приватна особа: підприємець, адвокат, лікар, хто завгодно, крім осіб, які обробляють персональні дані в особистих побутових цілях.

Важливо, що володілець встановлює мету, визначає склад персональних даних та процедури їх обробки.

Розпорядник (у документах з питань захисту персональних даних Ради Європи та Європейського Союзу — процесор, англійською- processor) не встановлює самостійно мету обробки персональних даних, не визначає їх склад та процедури обробки. Розпорядник діє від імені володільця, який визначив мету обробки персональних даних розпорядником, установив склад персональних даних та встановив розпоряднику процедури обробки.

Володільцем чи розпорядником бази персональних даних можуть бути підприємства, установи та організації усіх форм власності, органи державної влади чи органи місцевого самоврядування, фізичні особи — підприємці, які обробляють персональні дані відповідно до закону.

Як визначити, ким є та чи інша організація: володільцем чи розпорядником? У чому різниця? Розпорядник — це той, кому володілець доручив обробляти персональні дані відповідно до договору, це організація, яка обробляє персональні дані в інтересах володільця.

Якщо говорити про державного реєстратора, то найчастіше володільцем є орган державної влади, який є держателем реєстру, а розпорядником - підприємство або установа, яка визначена адміністратором реєстру.

Розпорядник не може визначати мету обробки персональних даних, а обробляти персональні дані може тільки з тою

СУБ'ЄКТИ ВІДНОСИН ВОЛОДІЛЬЦІ / РОЗПОРЯДНИКИ		
ВОЛОДІЛЕЦЬ		**РОЗПОРЯДНИК**
ПРАВО надано законом, договором або за **згодою**		ПРАВО надано **володільцем** або законом
затверджує мету обробки персональних даних встановлює склад персональних даних встановлює процедури обробки та захисту персональних даних		здійснює збір та обробку персональних даних від імені володільця з визначеними володільцем цілями
реєструє базу персональних даних		склад персональних даних встановлює володілець, розпорядник зазначається при реєстрації бази персональних
забезпечує захист персональних даних від незаконної обробки та доступу		забезпечує захист персональних даних від незаконної обробки та доступу
надає часткове або повне право обробки персональних даних іншим суб'єктам		

метою, яку йому визначив володілець. Розпорядник несе набагато менше відповідальності, ніж володілець.

Розпорядник може обробляти персональні дані лише з метою і в обсязі, визначеними у договорі. Якщо відсутній договір, яким організація, володілець, доручає обробляти персональних дані з визначеною володільцем метою та у визначених володільцем обсягах іншій організації, то ця інша організація не може бути розпорядником.

Не може бути розпорядником підрозділ юридичної особи або працівник організації — володільця персональних даних. Ним може бути лише окрема юридична особа або окремий приватний підприємець.

Існують ще деякі особливості. Конвенція 108 встановлює, що її вимоги розповсюджуються на групи осіб, які здійснюють діяльність без створення юридичної особи.

1. Профспілкові організації, деякі громадські об'єднання не є юридичними особами, але вони здійснюють обробку персональних даних.

2. Приватна особа здійснює обробку персональних даних, але робить вона це не для непрофесійних особистих чи побутових потреб. Наприклад, модератор працює у соціальній мережі, він визначає мету діяльності групи, має, відповідно до політики цієї соціальної мережі, можливість включити чи не включити інших осіб до складу групи, дозволити розмістити їхню точку зору чи не дозволити її розміщення. Тобто він встановлює склад персональних даних і процедури їх обробки. Отже, на ці дії поширюються вимоги Закону України «Про захист персональних даних» у частині, що такої обробки стосується.

Третя особа

Якщо якась організація не є володільцем, не є розпорядником і не є уповноваженим органом з питань захисту персональних даних, то її можна визначити як третю сторону. При цьому третя особа у більшості випадків теж може бути володільцем персональних даних або розпорядником, який діє від імені іншого володільця.

З точки зору підприємства, установи чи організації, яка є володільцем бази персональних даних та здійснює обробку персональних даних працівників, місцеві органи влади, виконавчі органи фондів соціального страхування від нещасних випадків, від тимчасової втрати працездатності, соціального захисту інвалідів, пенсійного, Державної інспекції з питань праці, служби зайнятості, податкової служби, органів прокуратури тощо є третіми особами, яким персональні працівників передаються у випадках, визначених законом. Зазначені органи зобов'язані вжити заходів щодо забезпечення вимог законодавства про захист персональних даних.

Тобто у відносинах стосовно обробки персональних даних беруть участь: володілець персональних даних, розпорядники, які діють в інтересах володільця, та уповноважений орган з питань захисту персональних даних, який здійснює нагляд за обробкою персональних даних. Якщо персональні дані передаються для обробки іншому, крім зазначених, суб'єкту, цей суб'єкт є третьою стороною і, як правило, - іншим володільцем персональних даних.

База персональних даних

Закон «Про захист персональних даних» вводить поняття бази персональних даних як іменованої сукупності упорядкованих персональних даних в електронній формі та/або у формі картотек. Із застосуванням цього поняття виникало багато складнощів унаслідок низки причин.

Різні цілі, склад персональних даних та

процедури - різні бази персональних даних

Конвенція 108 трактує як «файл даних для автоматизованої обробки», будь-який масив даних, що піддається автоматизованій обробці, і рекомендує кожній країні визначитися, чи буде вона застосовувати Конвенцію 108 до файлів персональних даних, які не обробляються автоматизовано.

Конвенцію 108 було прийнято у 1981 році, коли технології давали змогу автоматизовано обробляти лише певні категорії масивів даних. На сьогодні автоматизовано можуть оброблятися відомості про особу, які містяться у найрізноманітніших масивах даних: у цифровому, текстовому форматі, у графічній формі, у формі відеозображень. Зараз складно знайти процеси, де не використовується автоматизована обробка, навіть звичайні паперові документи готуються з використанням комп'ютерної техніки і піддаються автоматизованій обробці: скануванню, розпізнаванню тексту чи зображень, пошуку необхідних елементів даних тощо.

Термін «база персональних даних», що використовується у Законі «Про захист персональних даних», часто помилково ототожнюють з терміном «база даних», який передбачає конкретну технологію автоматизованої обробки.

База персональних даних не є базою даних.

Використання терміну «база персональних даних» передбачає, що володілець персональних даних визначає мету їх обробки у базі персональних даних, склад цих даних та процедури їх обробки з певною метою.

Різні цілі, склад персональних даних та процедури — різні бази персональних даних

Володільцем яких баз персональних даних є підприємство, установа чи організація?

Наприклад, мета обробки персональних даних пацієнтів лікувального закладу і працівників лікувального закладу різна. Одні — лікують, а інші — лікуються. Мета обробки персональних даних у цих двох різних персональних даних сформульована в різних законах. У першому випадку це можуть бути, наприклад, Закон України «Основи законодавства України про охорону здоров'я», у другому — Кодекс законів про працю України. Склад персональних даних, що обробляються в цих персональних даних теж різний.

Слід зазначити, що лікувальний заклад, крім зазначених цілей, імовірно, обробляє персональні дані з метою здійснення господарської діяльності для забезпечення функціонування — з метою закупівлі ліків, здійснення ремонту будівель, вивезення сміття, тощо. Персональні дані, які використовуються у цій сфері діяльності, можуть належати до іншої бази персональних даних.

Цей приклад є типовим і для інших категорій організацій. Зазвичай, визначення трьох баз персональних даних: клієнтів (користувачів, відвідувачів, пацієнтів, покупців, тощо), працівників та контрагентів,- достатньо в діяльності організації.

Приклад.

У телекомунікаційній компанії здійснюється обробка персональних даних працівників компанії, користувачів послуг зв'язку, а також обробка персональних даних у допоміжних бізнес-процесах. Можна обмежитися також трьома базами персональних даних.

Кількості баз персональних даних в організації законодавством не обмежена. Підприємство, установа чи організація самостійно визначають та відображають в організаційних документах в яких саме базах персональних даних здійснюється їх обробка.

Чи є обробка персональних даних у

системі відеоспостереження обробкою персональних даних в окремій базі даних? У цьому випадку персональні дані, отримані з допомогою системи відеоспостереження, можуть оброблятися в окремій базі персональних даних, або кількох базах, або існувати як складова частина обробки персональних даних у тій чи іншій базі персональних даних: відеоспостереження в робочих приміщеннях можна віднести до обробки персональних даних в базі персональних даних працівників, відеоспостереження чи реєстрація дій клієнтів – до іншої бази персональних даних.

Якщо йдеться про різні цілі, різний склад персональних даних і різні процедури - це означає, що мають існувати різні бази персональних даних.

Якщо, скажімо, у мобільному телефоні працівника є інформація про інших працівників цього підприємства, то можна говорити про елементи бази персональних даних працівників. При цьому метою обробки може бути організація функціонування підприємства, зокрема забезпечення виконання планових завдань.

Або якщо в мобільному телефоні працівника обробляються персональні дані клієнтів компанії, то це можна вважати елементом іншої бази персональних даних - бази персональних даних клієнтів компанії. Звичайно, у цьому випадку такі дії не є обробкою персональних даних працівником «для непрофесійних особистих чи побутових потреб», а отже, це потрапляє під застосування Конвенції 108 та законодавства про захист персональних даних. Таке використання персональних даних є окремими процедурами обробки персональних даних в інтересах підприємства, і кожен працівник зобов'язаний дотримуватись положень внутрішніх документів компанії і етичних норм при спілкуванні із клієнтами і працівниками.

Зрозуміло, що якщо у мобільному телефоні містяться номери телефонів працівників установи, в якій працює особа, і вона використовує їх не з метою організації виконання завдань установи, то це буде порушенням законодавства про захист персональних даних.

Відповідно до рекомендацій Ради Європи держава не повинна збирати в одну базу персональних даних інформацію, яка обробляється з різними цілями. Це робиться для того, щоб держава не мала можливості робити повний профайлінг фізичної особи, тобто відслідковувати всі події, пов'язані з конкретною особою та поєднувати відомості із різних джерел стосовно осіб, про яких обробляються відомості в державних установах.

IV. Орган нагляду, відповідальний за забезпечення законодавства про захист персональних даних

Кожна країна, яка приєдналася до Конвенції 108 створює уповноважений орган з питань захисту персоанльних даних даних. На який покладаються функції розслідування та втручання, участі у судовому розгляді, розгляд заяв суб'єктів про порушення їх прав та прийняття рішення.

Закон України «Про захист персональних даних» встановлює, що уповноважений орган з питань захисту персоанльних даних здійснює в межах своїх повноважень контроль за додержанням вимог законодавства про захист персональних даних шляхом проведення виїних та безвиїзних перевірок із забезпеченням відповідно до закону доступу до інформації, пов'язаної з обробкою персональних даних у базі персональних даних, та до приміщень, де здійснюється їх обробка.

Уповноваженим органом з питань захисту персональних даних є Державна служба України з питань захисту пер-

соанльних даних. З 1 січня 2014 року функції уповноваженого органу з питань захисту персоанльних даних покладаються на Уповноваженого Верховної Ради України з прав людини.

V. Обробка персональних даних з використанням веб-ресурсів

Веб-ресурс – сукупність сторінок в Інтернеті, яка може бути ідентифікована, адресована і супроводжувана в мережевій інформаційній системі.

У момент збору персональних даних суб'єкт персональних даних повідомляється про володільця персональних даних, склад та зміст зібраних персональних даних, права такого суб'єкта, визначені цим Законом, мету збору персональних даних та осіб, яким передаються його персональні дані.

Вимоги Закону України «Про захист персональних даних» та застосування його положень при обробці персональних даних з використанням веб-ресурсів повністю кореспондуються з рекомендаціями Комітету Міністрів Ради Європи щодо захисту недоторканості приватного життя в Інтернеті[10], рекомендаціями Робочої групи[11], що функціонує відповідно до статті 29 Директиви 95/46/ЄС та рекомендаціями Міжнародної робочої групи з питань захисту персональних даних в телекомунікаціях[12].

5.1. Категорії персональних даних що найчастіше обробляються в Інтеренет

Найчастіше персональні дані з використанням веб-ресурсів обробляються в рамках таких процесів як:

- заповнення відвідувачами веб-ресурсів анкет
- реєстрація та отримання логіна та пароля
- реєстрація з використанням облікового запису соціальної мережі
- надання електронної адреси відвідувача для зворотного зв'язку.

При цьому можуть оброблятися персональні дані надзвичайно широкого діапазону: від анкетних персональних даних, які явно є відомостями про особу яка ідентифікована, так і відомостей які можуть стосуватися особи опосередковано або які можуть використовуватися в процесі ідентифікації особи: відомостей про оплату послуг з використанням платіжних карт, логіни та паролі, записи в соціальній мережі, номери телефонів, електронні адреси, тощо.

Питання що стосуються таких специфічних категорій даних як IP-адреса, кукі, та інші відомості які часто використовуються як для технічного забезпечення надання якісних послуг користувачу, так і для відслідковування поведінки відвідувачів веб-сторінки вимагають окремого обговорення та коротко викладені в розділі 5.4.

5.2. Типові порушення законодавства з питань захисту персональних даних при обробці персональних даних з використанням веб-ресурсів та рекомендації щодо їх усунення

Під час виїзних та безвиїзних перевірок дотримання володільцями законодавства з питань захисту персональних

[10] Додаток до рекомендації № r (99) 5 комітету міністрів державам-членам ради європи по захисту недоторканності приватного життя в інтернеті
[11] http://www.medialaw.kiev.ua/laws/laws_international/105/
[12] Article 29 - data protection working party. WP 37. Working Document. Privacy on the Internet - An integrated EU Approach to On-line Data Protection-Adopted on 21st November 2000 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp37en.pdf
[13] International Working Group on Data Protection in Telecommunications. Report and Guidance on Data Protection and Privacy on the Internet "Budapest - Berlin Memorandum":1996http://www.datenschutz-berlin.de/attachments/138/bbmem_en.pdf?1200577389

даних до планів перевірок включалися також і питання дотримання законодавства про обробці персональних даних з використанням веб-ресурсів володільців.

Комісіям надавалась необхідна інформація - копії чи виписки з документів, письмові та усні пояснення. Як правило, комісіями не використовувалося право на безперешкодний доступ до комп'ютерів та магнітних носіїв, що передбачено законодавством.

Натомість, ефективно використовувався механізм огляду електронного документа для вивчення матеріалів, розміщених на сайті, процедур обробки персональних даних на сайті та механізмів функціонування веб-ресурсу володільця, про що складалися акти оглядів електронних документів за встановленою формою.

Найчастіше виявлялися такі порушення:

1. У момент збору персональних даних суб'єкт персональних даних НЕ ПОВІДОМЛЯЄТЬСЯ про володільця персональних даних (найменування юридичної особи – володільця та її адресу), склад та зміст зібраних персональних даних, права такого суб'єкта, визначені цим Законом, мету збору персональних даних та осіб, яким передаються його персональні дані.

2. Зміст персональних даних був явно НАДМІРНИМ відповідно до визначеної мети обробки персональних даних.

3. Процедури обробки персональних даних були визначені на сайті, але не були визначені розпорядчими документами володільця, як це передбачено законодавством.

Рзультатами перевірок Державної служби України з питань захисту персональних даних підготовлено обов'язкові до виконання ПРИПИСИ про усунення порушень.

Жодного припису не було оскаржено у судовому порядку.

Здійснено та здійснюється доопрацювання процедур обробки персональних даних в використанням веб-ресурсів, зокрема встановлено процедури повідомлення відвідувачів сайтів про свої права, про склад та зміст персональних даних, що збираються, про мету збору персональних даних та про осіб, яким передаються його персональні дані.

Як правило, таке повідомлення здійснюється у формі окремого розділу сайту («Політика обробки персональних даних», «політика приватності», чи «політика конфіденційності»).

Усуваються інші порушення, зокрема такі як надання безвідкличної чи безстрокової згоди на обробку персональних даних, передача персональних даних невстановленим третім особам, тощо.

Відновлено право суб'єкта персональних даних на знищення своїх даних, в разі відсутності підстав для їх обробки.

Окремі володільці призупинили функціонування своїх веб-ресурсів до усунення порушень.

5.3. Прозорість та відкритість забезпечення приватного життя в Інтернеті

Державна служба України з питань захисту персональних даних підтримує ініціативи, спрямовані на зростання обізнаності тих, хто обробляє персональні дані, та тих, чиї персональні дані обробляються з кращими практиками та стандартами обробки персональних даних.

За ініціативи ВГО «Українська асоціація захисту персональних даних» у жовтні 2012 року було прийнято Декларацію «За недоторканість приватного життя в Інтернеті»[13], до якої приєдналися провідні національні телекомунікаційні компанії.

У лютому 2013 року було проведено перше дослідження в рамках громадсько-

[13] http://uapdp.org/images/1016%202012%20.pdf

го моніторингу відкритості та прозорості обробки персональних даних в Інтернеті. Хоча використовувалися прості і доступні кожному методики, результати настороюють і варті уваги[14], адже, за результатами дослідження встановлено, що понад 75% веб-сайтів українського сегменту Інтернет, за явних ознак обробки персональних даних, не надають користувачам жодних відомостей про найменування володільця персональних даних. Це свідчить про те, що відвідувачі сайтів не мають можливостей на захист свої персональних даних.

Громадські ініціативи, спрямовані на забезпечення прозорості і відкритості обробки персональних даних є надзвичайно важливими.

5.4. Відслідковування поведінки відвідувачів веб-ресурсів (web-tracking)

За вкрай низького рівня правової культури володільців персональних даних, які здійснюють їх обробку з використанням веб-ресурсів українського сегменту Інтернет, коли ігноруються найпростіші вимоги закону при зборі та обробці персональних даних, важко говорити про небезпеку для приватного життя користувачів Інтернет некоректного використання автоматизованих засобів відслідковування особливостей поведінки користувачів Інтернет при відвідуванні веб-сайтів.

Але обговорювати це необхідно, адже цілком раціональні засоби, що використовуються для забезпечення кращого задоволення споживацьких потреб, за умов надмірного їх використання, надмірного збору відомостей про споживачів, фізичних осіб, які за певних обставин можуть бути ідентифікованими, можуть призвести до втручання в приватне життя. В країнах Європи цій проблемі надається значної уваги[15].

Для відслідковування особливостей поведінки відвідувачів веб-ресурсів використовуються такі технології як:

- надсилання до пристрою користувача кукі першої та кукі третьої сторони;
- збирання в базах веб-ресурсів детальної інформації протягом тривалого часу про відвідані сторінки, вибрані режими, натиснуті клавіші, тощо, та її подальша обробка;
- збирання в базах веб-ресурсів інформації про апаратні та програмні засоби, які встановлено у користувача, та ін.

Звичайно, в цій сфері заходів, що можуть вживатися Державною службою з питань захисту персональних даних, для забезпечення прогресу, мало. Адже ДСЗПД, в ході перевірок може лише зафіксувати незаконне надсилання кукі третьої сторони та вимагати, щоб такі операції здійснювалися лише за наявності законних підстав.

Володільці персональних даних, які здійснюють обробку персональних даних з використанням веб-ресурсів часто навіть не знають, які треті сторони отримують відомості про те, що користувач відвідав їх ресурс. Необхідно інформування як володільців персональних даних, так і суб'єктів персональних даних про механізми автоматизованого збору відомостей про поведінку відвідувачів в Інтернет, про законні підстави для обробки персональних даних про відвідування сайтів, про необхідність повідомлення відвідувачів про механізми автоматизованої обробки персональних даних та про їх права.

[14] http://uapdp.org/images/news/doslidzhennya/Research-results-v.2.2.pdf
[15] Article 29 data protection working party. WP 194. Opinion 04/2012 on Cookie Consent Exemption. Adopted on 7 June 2012 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf

VI. Дотримання законодавства про захист персональних даних при дослідженнях в інтернет

В залежності від різновиду опитування в Інтернет відносини між суб'єктами, пов'язаними з персональними даними також можуть бути різними, а отже застосовуються різні положення законодавства.

6.1. Дослідження, що передбачають активну взаємодію з респондентами

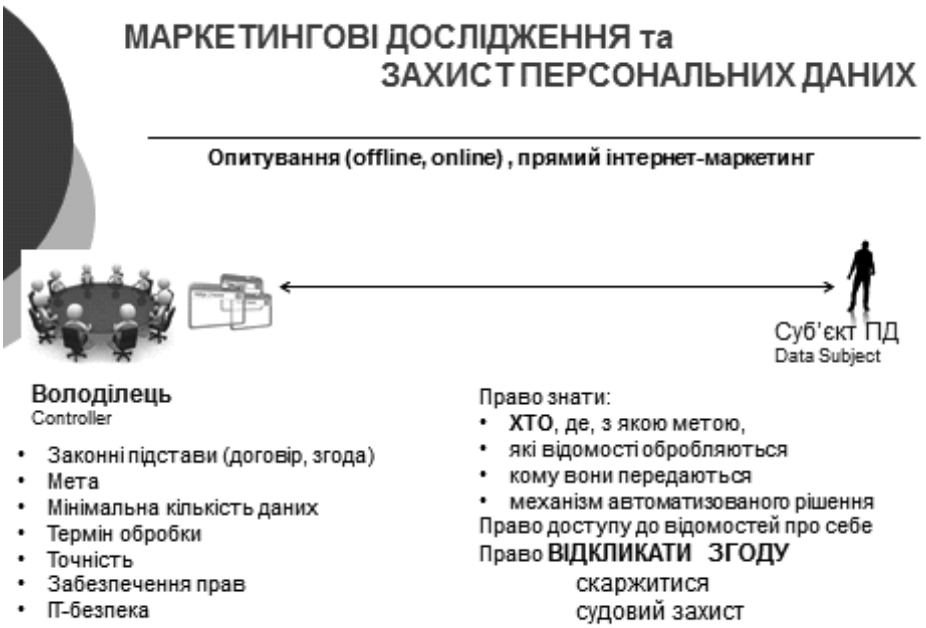
Перший різновид - дослідження, що передбачають активну взаємодію з респондентами[16]:

- offline – опитувальні листи респондент отримує по e-mail або скачує з сайта, заповнює відповідну форму й пересилає через e-mail;
- online (e-mail-опитування, Web-опитування) – респондент відповідає на поставлені запитання в режимі реального часу й може миттєво переглянути дійсні на поточний час, результати опитування.

Очевидно, що організація, яка здійснює опитування є володільцем персональних даних, а респондент є суб'єктом персональних даних (рис.6.1).

Дослідник необхідно звернути увагу на законні підстави для збору та обробки персональних даних та забезпечення прав суб'єкта персональних даних. Законними підставами у даному випадку може бути договір, укладений з респондентом (письмовий договір, чи договір приєднання згідно зі статтею 634 Цивільного кодексу України), або надана згода на обробку персональних даних. На дослідника покладається доведення факту наявності законних підстав для обробки персональних даних в разі звернення респондента зі скаргою до уповноваженого органу чи до суду.

Звичайно тут має бути чітко позначено мета дослідження, ваша процедура щодо захисту персональних даних, тобто які персональні дані ви збираєте, для чого ви їх зберігаєте, як довго вони будуть збері-



[16] Сучасні тенденції застосування інтернет-технологій у маркетингу, Ілляшенко С. М., в збірнику Маркетинг і менеджмент інновацій, 2011, № 4,Т.II, Сумськоий державноий університет. http://mmi.fem.sumdu.edu.ua/sites/default-files/mmi2011_4_2_64_74.pdf

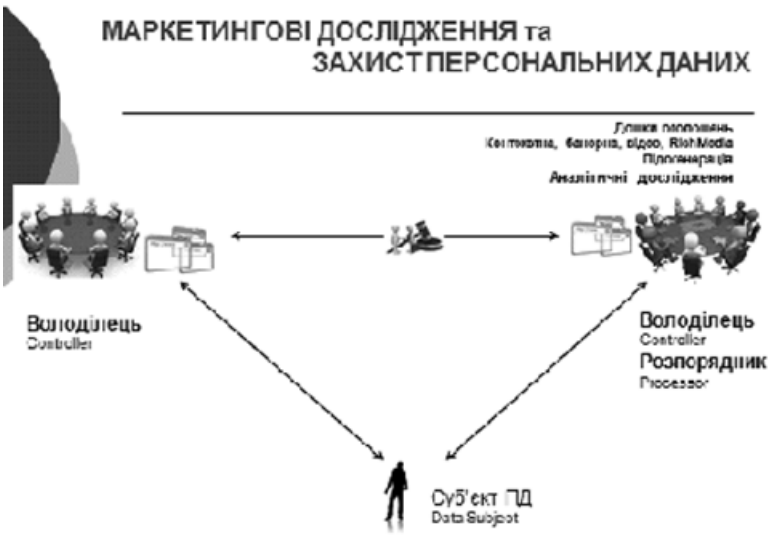
гатися. Мова йде про ретельно прописану політику вашого дослідження. Під час збору даних ви зобов'язані повідомити суб'єкта про його права, тобто чітко сказати, хто про що повинен знати, обов'язково повідомити респондента про його право приймати або не приймати участі в дослідженнях, на який стадії ваші дані стають анонімі, яка ступень псевдо анонімності даних у дослідженнях. Не обов'язково ваш респондент муси знати про всі етапи роботи з його даними, але лише до того етапу, коли його дані агрегуються та стають анонімними, неможливими для ідентифікації.

Навіть при опитуванні, яке не передбачає ідентифікацію респондента, зазвичай обробка персональних даних (логін, пароль, відповіді на запитання та ін..) здійснюється. В разі виплати респондентам винагороди, при розігруванні призів здійснюється ідентифікація респондентів.

6.2. Дослідження, що не передбачають прямої взаємодії з суб'єктами персональних даних

Інший різновид досліджень в Інтернеті – збір та аналіз інформації про відвідування певних сторінок сайтів компаній-партнерів, що не передбачає прямої взаємодії з респондентами: надання послуг компаніям партнерам щодо вивчення аудиторії їх сайту. При цьому можуть застосовуватися різні технології, але часто,згідно з позицією Державної служби України з питань захисту персональних даних[17] такі технології пов'язані з обробкою персональних даних[18], зокрема:

- здійснюється обробка IP-адрес та унікальних ідентифікаторів Cookies, що дозволяє відстежувати суб'єктів - користувачів конкретного комп'ютер, навіть якщо їх справжні імена невідомі;
- аналізуються відомості про тип інтернет-браузерів, які використовуються відвідувачами сайта (наприклад, Microsoft Internet Explorer, Mozilla Firefox, Google Chrome або Opera); операційна система (ОС), яку вони використовують (наприклад, Windows XP); розширення екрану монітора; глибина кольору екрану монітора, активні



[17] Корпоративний Кодекс поведінки/Маркетинг в Україні, №2, 2013- с. 58
[18] WP 171. Opinion 2/2010 On online behavioural advertising, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

процеси в комп'ютері відвідувачів сайту та ін.

Зазвичай компанія дослідник, у цьому випадку, є розпорядником персональних даних, а компанія—партнер є володільцем персональних даних. Підставою для обробки персональних даних компанією партнером є згода відвідувача сайту, умови якої визначено політикою захисту персональних даних компанії партнера.

Що є підставою для обробки персональних даних компанією дослідником при здійсненні такого різновиду досліджень в Інтернет? Зазвичай це згода, надана компанії-партнеру щодо обробки персональних даних компанією-дослідником як розпорядником персональних даних. Тобто компанії досліднику дуже важливо працювати з компанією партнером, в інтересах якого здійснюються дослідження для того, щоб погодити положення політики приватності та відповідні юридичні рішення щодо згоди.

В разі якщо компанія партнер ігнорує положення законодавства про захист персональних даних, якщо юридичні рішення щодо згоди не погоджені, або взагалі, відсутні, компанія дослідник не має законних підстав для здійснення досліджень, а отже несе ризики звернення відвідувачів сайту компанії партнера зі скаргою до уповноваженого органу з питань захисту персональних даних або до суду.

Яку стратегію обробки ризиків, пов'язаних із обробкою персональних даних обирати компанії досліднику: уникати ризиків відслідковуючи політики приватності партнерів та наявність обґрунтованих юридичних рішень щодо згоди, чи приймати такі ризики вважаючи їх нікчемними – вибирати компанії досліднику.

В разі відсутності правочинів, які встановлюють відносини між компанією-дослідником та компаніями партнерами в сфері захисту персональних даних такі партнери є третіми сторонами.

Однак, історія може продовжуватись. Компанії-дослідники часто збирають інформацію багатьох сайтів компаній партнерів, і в результаті компанії-дослідники обробляють отримані відомості не лише в інтересах компаній партнерів, а в своїх власних інтересах. Де закінчується дослідження в інтересах партнерів,, а де починаються дослідження в своїх цілях? І це також потрібно позначати в своїй політиці приватності.

6.3 Аспекти відносин між компаніями дослідниками та їх партнерами

Відносини стосовно персональних даних вимагають формулювання політики, визначення процедур, спрямованих на дотримання цієї політики, підтримки політики і процедур в актуальному стані. Адже без цього неможливо оцінити ризики обробки персональних даних.

Що потрібно враховувати при укладанні договорів з компаніями партнерами?

Якщо мова йде про відносини між володільцем та володільцем даних, то кожна сторона оцінює свої ризики самостійно. Сторона, яка поширює персональні дані, зобов'язана забезпечити їх захист відповідно до законодавства.

Сторона, яка поширює персональні дані зацікавлена в тому, щоб договірні положення зобов'язували сторону, яка персональні дані отримує, дотримуватися визначених умов обробки персональних даних.

Сторона, яка отримує персональні дані, зацікавлена в тому, щоб врегулювати юридичні аспекти щодо підстави для отримання та подальшої обробки персональних даних, найменше – встановити, що сторона яка поширює персональні дані має підстави для їх обробки та поширення.

В разі, якщо компанія дослідник та компанії-партнери знаходяться в різних юрисдикціях необхідно враховувати таке. Законодавство України не забороняє і не обумовлює спеціальними дозволами передачу персональних даних іноземним суб'єктам відносин. Водночас, в разі якщо країна партнера не приєдналася до Конвенції 108, передача персональних даних можлива за умов, коли партнер бере на себе зобов'язання щодо забезпечення захисту персональних даних визначені законодавством України. Типові контракті положення, рекомендовані уповноваженим органом з питань захисту персональних даних ви можете знайти на сайті ДСЗПД або Американської торговельної палати в Україні[19].

ПІСЛЯМОВА

Дослідження ВГО «Українська асоціація захисту персональних даних» виявили вкрай низький рівень відкритості та прозорості обробки персональних даних в Інтернет. Водночас, дослідження компанії GfK Ukraine показують, що користувачі українського сегменту Інтернет в 85% випадків ознайомлюються з політикою приватності Інтернет-ресурсу, який вони відвідують.

Понад 30% користувачів знають про існування Cookies та досить добре обізнані щодо механізму їх роботи. понад 54% учасників дослідження підтвердили, що не мають достатньо знань для того, щоб управляти ними. 22% опитаних відповіли, що уважно прочитали інформацію щодо захисту персональних даних на сайті GfK Ukraine.

Росте обізнаність користувачів українського сегменту мережі Інтернет щодо вимог законодавства про захист персональних даних, що прав користувачів на недоторканість приватного життя та гарантованих законом способів вимагати відновлення своїх порушених прав. Це значить, що ризики компаній, які здійснюють дослідження в Інтернет зростають, а отже необхідні нові знання, кваліфіковані фахівці та обґрунтовані рекомендації в сфері захисту персональних даних при проведенні досліджень в Інтернет.

[19] Угода про передачу персональних даних (в країни, що не приєднались до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ETS №108) та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордоннихпотоків даних (далі – Конвенція №108 та Додатковий протокол)) http://zpd.gov.ua/dszpd/doccatalog/document?id=56163 або http://www.chamber.ua/personal-data