УДК 342.721:681.3.02

ПРОЦЕНКО В.А., науковий співробітник Науково-дослідного центру
Національної академії правових наук України

ОСОБЛИВОСТІ МЕХАНІЗМІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ЗАКОНОДАВСТВІ ЄС

Анотація. *Про сучасні проблеми захисту персональних даних та про механізми ЄС по забезпеченню захищеності даних, закріплені на законодавчому рівні.*

Ключові слова: *захист даних, обробка інформації, персональні дані, захист персональних даних, права і свободи людини, передача даних, “хмарні обчислювання”, “безпечна гавань”.*

Аннотация. *О современных проблемах защиты персональных данных и о механизмах ЕС по обеспечению защищенности данных, заложенных на законодательном уровне.*

Ключевые слова: *защита данных, обработка информации, персональные данные, защита персональных данных, права и свободы человека, передача данных, “облачные вычисления”, “безопасная гавань”.*

Summary. *Modern issues of personal data security and EU data security safeguarding mechanisms provided by law.*

Keywords: *data security, information processing, personal data, personal data security, human rights and freedom, data transfer, “cloud computing”, “safe harbor ”.*

Постановка проблеми. Персональні дані – це будь-яка інформація, що стосується особи, незалежно від того, до якої сфери життєдіяльності вона відноситься – особистої, професійної чи громадської. Це може бути що завгодно, від імені особи, фото та адреси електронної пошти, до банківських реквізитів, повідомлень в соціальних мережах, медичної інформації або IP-адреси комп’ютера.

Хартія ЄС “Про основні права” встановлює, що кожна людина має право на захист персональних даних вдома, на роботі, в торговельних відносинах, лікарні, поліцейському відділку або в Інтернеті [1]. 74 % європейців вважають, що розкриття персональних даних стає неминучим у сучасному житті, але в той же час, 72 % Інтернет-користувачів стурбовані тим, що вони надають надто багато особистої інформації. Вони відчувають, що не мають повного контролю над своїми даними. Це руйнує їхню довіру до мережі Інтернет і стримує зростання цифрової економіки в цілому.

Значного розголосу, наприклад, набула справа австрійського студента-юриста Макса Шремса. Він спробував з’ясувати стан безпеки його особистих даних, звернувшись до соцмережі Facebook. Він був здивований, коли представники Facebook погодилися надіслати йому більше ніж 1200 сторінок інформації про нього, навіть за умови, що він вже давно видалив свій профіль в цій соцмережі.

М. Шремс надіслав 22 скарги уповноваженому із захисту даних в Дубліні, де знаходиться головний офіс Facebook в Європі. За його словами, були вилучені всі його повідомлення в Facebook. І простий пошук за окремими словами може дати значний обсяг особистої інформації. Наприклад, можна ввести всі політичні партії, які існують в Австрії, і через мить дізнатися, за яку він голосував, тому що студент обговорював їх в приватних чатах з іншими людьми. І все це зберігається протягом трьох, чотирьох, п’яти, а подекуди, і 10 років.

В результаті розслідування, проведеного в Дубліні, компанія Facebook погодилася внести ряд змін на сайт, які б відповідали правилам конфіденційності. Представники

компанії наголошують, що в їх мережі особи добровільно розкривають інформацію. Користувачі, розміщуючи інформацію, повністю усвідомлюють, що вони роблять, тому що детально інформуються системою про те, які дані вони залишають і хто матиме доступ до них, а також компанія забезпечує користувачеві можливість видалити дані про себе. Таким чином, представники Facebook вважають, що їх послуги абсолютно відповідають принципам, на яких базується захист даних Європейського Союзу [2].

Новим явищем сучасного інформаційного світу є Cloud computing (“Хмарні обчислення”), мається на увазі, що дані можуть бути оброблені в Пекіні, зберігатися в Бостоні і скачані в Будапешті [3].

Особисті дані все частіше переміщуються через кордони – як віртуальні, так і географічні – і зберігаються на серверах кількох країн всередині і за межами ЄС. Глобальний характер інформаційних потоків робить виклик для зміцнення захисту особистих даних на міжнародному рівні. Це вимагає вживання заходів посилення засобів захисту даних фізичних осіб та зменшення їх потоку через кордони.

Реформа захисту даних, запропонована Європейською Комісією, дозволить спростити загальноєвропейські корпоративні правила та оптимізувати процес їх затвердження, адже затвердженням загальних правил захисту даних буде займатися вже єдиний орган, а не кілька.

Метою статті є дослідження законодавчих норм Європейського Союзу щодо захисту персональних даних в сучасних умовах.

Виклад основних положень. Трохи більше чверті користувачів соціальних мереж (26 %) і ще менше покупців он-лайн (18 %) вважають свої персональні дані повністю захищеними.

74 % європейців вважають, що розкриття особистої інформації стає невід’ємною частиною сучасного життя.

43 % Інтернет-користувачів вважають, що в них запитують більше особистої інформації, ніж це необхідно.

Тільки одна третина європейців знають про існування державних органів влади, що відповідають за захист даних (33 %).

90 % європейців бажають мати однаково високий рівень захисту даних в усіх країнах ЄС.

Законодавство ЄС про захист даних. Захист особистих даних ніколи не був більш важливим на тлі зростаючої загрози кіберзлочинності та фактів витоку особистої інформації. Велика кількість людей відчуває, що вони втратили контроль над тим, хто може довідатися про них в Інтернеті. Точне місце розташування кожного може вже зараз бути відслідковано. Поняття особистого життя змінилося за умов, що сотні мільйонів людей сьогодні зареєстровані на сайтах соціальних мереж.

Відповідно до законодавства ЄС, персональні дані можуть бути зібрані законно при дотриманні суворих вимог та для законної мети. Крім того, особи чи організації, що займаються збором та обробкою особистої інформації людей, повинні захистити її від зловживань і дотримуватися певних прав власників даних, які гарантовані законом ЄС.

Кожен день в Європейському Союзі підприємствами, органами державної влади та приватними особами передаються через кордони величезні обсяги персональних даних. Суперечливі правила захисту даних в різних країнах можуть порушити процес міжнародного обміну. Окремі особи також можуть відмовлятися від передачі персональних даних за кордон, якщо вони не впевнені в рівні захисту даних в інших країнах.

Таким чином, були встановлені загальні правила ЄС, що дають змогу громадянам держав-членів ЄС переконатися, що їх персональні дані мають високий рівень захисту в усьому ЄС. Адже особа має право подати скаргу і отримати відшкодування, якщо її дані неправомірно використані в будь-якій країні Співтовариства [4].

Директива 95/46/ЄС Європейського Парламенту та Ради Європи від 24 жовтня 1995 року про захист фізичних осіб у зв’язку з обробкою персональних даних і вільним обігом цих даних спрямована на захист прав і свобод людини у зв’язку з обробкою її персональних даних. Директива вимагає від держав-членів гарантувати право осіб на недоторканність приватного життя та забезпечити вільний потік особистих даних в рамках Співтовариства [5].

Ці правила захисту особистих даних були введені, коли Інтернет був ще в зародковому стані. Швидкий технологічний розвиток і глобалізація принесли нові виклики для захисту даних. Користуючись сайтами соціальних мереж, будь-якими Інтернет-послугами та смарт-картами, ми залишаємо цифрові сліди у мережі. Отже нові виклики безпеці даних вимагають реформ, які забезпечили б чітке регулювання сучасного цифрового середовища.

З метою забезпечення ефективного механізму захисту даних пізніше органами Євросоюзу були прийняті:

- Рішення Європейської Комісії 2001/497/ЄС від 15 червня 2001 року про набір стандартних договірних пропозицій для передачі особистих даних до третіх країн в рамках Директиви 95/46/ЄС [6]. Це Рішення встановлює типові договори, щоб гарантувати відповідний рівень захисту особистих даних, які переміщуються з ЄС до третіх країн. Рішення вимагає, щоб держави-члени слідкували за тим, щоб компанії або державні органи, які мають відношення до передачі особистих даних до третіх країн, гарантували “відповідний рівень захисту” даних;
- Рішення Європейської Комісії 2004/915/ЄС від 27 грудня 2004 року про внесення поправок до Рішення 2001/497/ЄС стосовно введення альтернативного набору стандартних договірних пропозицій для передачі особистих даних до третіх країн [7]. Затверджує нові типові договори, які бізнес-структури можуть використовувати для гарантування відповідного рівня захисту, коли дані переміщуються з ЄС до третіх країн. Нові договори додаються до тих, які вже існують за Рішенням Комісії 2001 року;
- Постанова 45/2001 Європейського Парламенту та Ради Європи від 18 грудня 2000 року про захист фізичних осіб у зв’язку з обробкою персональних даних органами Співтовариства та про вільний обіг цих даних [8]. Мета постанови – забезпечити захист персональних даних в межах установ та органів Євросоюзу. Це включає умови, які гарантують високий рівень захисту особистих даних, оброблених установами та органами Співтовариства, а також передбачає створення незалежного контрольного органу, щоб контролювати виконання цих умов;
- Директива 2002/58/ЄС Європейського Парламенту та Ради Європи від 12 липня 2002 року у зв’язку з обробкою персональних даних та захисту особистого життя в секторі електронних комунікацій [9]. Директиву було прийнято в 2002 році, одночасно із розробкою нової структури європейського законодавства у сфері електронних комунікацій. В директиві викладені умови зберігання даних державами-членами з метою поліцейського нагляду, розглянуті питання розсилки небажаної електронної пошти, використання файлів типу “cookies” і оприлюднення особистих даних [10].

25 січня 2012 року в Брюсселі Європейська Комісія запропонувала всеосяжну реформу правил ЄС щодо захисту даних 1995 року, щоб зміцнити он-лайн права на конфіденційність і підвищити ефективність цифрової економіки в Європі.

Технологічний прогрес і глобалізація значною мірою змінили спосіб збору даних, доступу до них та їх використання. Крім того, 27 держав-членів ЄС у 1995 році імплементували Доктрину по-різному, в результаті виникли розбіжності в правозастосовній діяльності. Новий єдиний закон захисту даних має покінчити із нинішніми правозастосовними розбіжностями і скоротити адміністративні витрати, пов’язані із захистом особистих даних, що дасть змогу європейським компаніям економити сукупно близько € 2,3 млрд. на рік. Ця ініціатива має сприяти зміцненню довіри споживачів до он-лайн сервісів, забезпечуючи необхідний імпульс для економічного зростання, створення робочих місць та впровадження інновацій в Європі. Нова Директива також передбачає конкретні правила для передачі персональних даних за межі ЄС для забезпечення їх найефективнішого захисту.

Основні зміни, закладені у новій Директиві захисту даних ЄС:

✓ “Право бути забутим” – має допомогти людям краще керувати своїми ризиками в Інтернеті. Коли особа не хоче, щоб її дані могли використовуватися, і немає законної підстави для їх обов’язкового збереження, дані можуть бути повністю видалені.

✓ Запит на згоду щодо обробки даних особи має бути явним та зрозумілим.

✓ Спрощений доступ до власних даних і підвищена їх мобільність для простішої передачі даних з однієї служби до іншої.

✓ Компанії та організації повинні будуть повідомляти про серйозні порушення захисту даних протягом 24 годин, за умов, що не виникло виправданої затримки.

✓ Єдині правила захисту даних, дійсні на всій території ЄС.

✓ Компанії будуть мати справу тільки з одним національним органом із захисту даних, що знаходиться в країні ЄС, де розташовані їх основні установи.

✓ Фізичні особи матимуть право звертатися в усіх випадках щодо захисту даних в національний орган в країні їх проживання, навіть якщо їх персональні дані обробляються за межами своєї країни.

✓ Правила ЄС будуть також застосовуватися до компаній, що не належать до країн ЄС, але пропонують товари або послуги в ЄС.

✓ Підвищення відповідальності та звітності усіх, хто займається обробкою персональних даних.

✓ Непотрібні адміністративні труднощі, такі як повідомлення про вимоги до компаній, пов’язаних із обробкою персональних даних, будуть вилучені.

✓ Національні служби із захисту даних будуть посилені та дадуть змогу краще забезпечити дотримання правил ЄС всередині країн.

Передача персональних даних до третіх країн. Треті країни – це термін, що використовується в законодавстві ЄС для позначення країн за межами Європейського Союзу. Персональні дані можуть бути передані в третю країну, якщо ця країна забезпечує достатній рівень захисту даних. Деякі винятки з цього правила передбачені, наприклад, коли контролер сам може гарантувати, що одержувач буде дотримуватися правил захисту даних.

Стаття 29 Директиви створила “Робочу групу із захисту осіб у зв’язку з обробкою персональних даних”. Робоча група дає рекомендації щодо рівня захисту в Європейському Союзі та в третіх країнах. Група проводила переговори з представниками США про захист персональних даних, результатом яких було створення принципів *“Безпечної гавані”* [11].

“Безпечна гавань” – це налагоджений процес, який дозволяє американським компаніям відповідати вимогам Директиви 95/46/ЄС про захист персональних даних. Він призначений для організацій на території ЄС та США, які займаються зберіганням

даних про клієнтів та спрямовані на запобігання випадковому розкриттю інформації або її втраті. Американські компанії можуть брати участь в програмі лише за умови, що вони дотримуються 7 принципів, викладених у Директиві ЄС. Цей механізм був розроблений Міністерством торгівлі США у співробітництві з ЄС.

Головні принципи “Безпечної гавані”:

- Сповіщення – фізичні особи повинні бути проінформовані про те, що їхні дані будуть зібрані і як вони будуть використовуватися.
- Вибору – фізичні особи повинні мати можливість відмовитися від того, щоб їх інформація була зібрана та передавалася третім особам.
- Подальшої передачі – передача даних третім особам може відбуватися тільки з організаціями, які дотримуються відповідних принципів захисту даних.
- Безпеки – зобов’язання компаній докласти відповідних зусиль, щоб запобігти втраті зібраної інформації.
- Цілісності даних – дані повинні бути достовірними та відповідати меті їх збору.
- Доступності – особи повинні мати доступ до інформації про себе і мати можливість виправити або видалити її, якщо вона є неточною.
- Виконуваності – необхідна наявність ефективних засобів реалізації цих правил [12].

Порівняння з американським законом про захист даних. США надають перевагу так званому “секторальному” підходу до законодавства про захист даних, який ґрунтується на поєднанні законодавства, регулювання та саморегулювання. Колишній Президент США Білл Клінтон і колишній віце-президент Альберт Гор в “Основах глобальної електронної торгівлі” наполягають, що приватний сектор має бути провідним і компанії повинні реагувати відповідно до нових викликів Інтернет-технологій. На сьогодні в США не має єдиного закону про захист даних, який можна було б порівняти із Директивою ЄС про захист даних.

Законодавству США більш притаманний галузевий розвиток, закони приймаються для врегулювання конкретних, вузьких питань у сфері захисту даних. Наприклад, Акт “Про захист приватного відео” 1988 року, Акт “Про захист і конкуренцію кабельного телебачення” 1992 р., Акт “Про кредитну звітність” та Акт “Про захист персональних даних штату Массачусетс”. Таким чином, у той час як деякі сектори вже відповідають директиві ЄС, принаймні частково, більшість – ні.

Висновки.

28 січня проголошено європейським Днем захисту даних. Це спільна ініціатива Європейської Комісії та Ради Європи спрямована на підвищення обізнаності європейців в тому, як можуть збиратися та використовуватися їх особисті дані та які вони мають права на їх захист.

Європейський Союз вже протягом багатьох років має формалізовану систему законодавства у сфері конфіденційності, яка є більш суворою, ніж у багатьох інших регіонах світу.

Компаніям, що діють на території Європейського Союзу, не дозволяється посилати особисті дані за межі Європейської економічної зони, якщо неможливо гарантувати відповідний рівень захисту зовні. Такий захист може здійснюватися як на державному рівні (якщо закони країни передбачають рівний рівень захисту), так і на рівні організацій (міжнародна організація проводить свій внутрішній контроль за персональними даними).

Сьогодні в рамках Євросоюзу розпочато процес глибокого реформування законодавства у сфері захисту даних. Директива 95/46/ЄС “Про захист фізичних осіб у зв’язку з обробкою персональних даних і вільним обігом цих даних”, спрямована на захист прав і свобод людини у зв’язку з обробкою її персональних даних, вже значною

мірою застаріла, так як її було розроблено на самому початку динамічного процесу становлення Інтернет-технологій. Розробка нової Директиви дасть змогу відповідати сучасним викликам та загрозам безпеці персональних даних. Окрім того, дуже важливим є аспект інформаційної взаємодії держав та компаній ЄС із “третіми країнами”. Щоб не опинитися “за бортом” європейського інформаційного потоку, Україні теж необхідно здійснити ряд реформ у сфері захисту даних, докласти великих зусиль для боротьби із мультимедійним та програмним піратством та належно забезпечити відповідальність за злочини в інформаційній сфері.

Використана література

1. Charter of Fundamental Rights of the European Union of 7 December 2002. – Режим доступу : //www.europarl.europa.eu/charter/pdf/text_en.pdf

2. Max Schrems: The Austrian Thorn In Facebook's Side. – Режим доступу : http://www.forbes.com/sites/kashmirhill/2012/02/07/the-austrian-thorn-in-facebooks-side

3. Cloud computing. – Режим доступу : http://www.searchcloudcomputing.techtargetcom/ definiti on/cloud-computing

4. Protection of personal data. – Режим доступу : http://www.ec.europa.eu/justice/data-protection/ index_en.htm

5. 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. – Режим доступу : http://www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri= CELEX: 31995L0046:EN:NOT

6. 2001/497/EC: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC. – Режим доступу : http://www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001D0497:EN:NOT

7. Commission Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries. – Режим доступу : http://www.eur-lex.europa.eu/LexUriServ/Lex UriServ. do?uri=CELEX:32004D0915:EN:NOT

8. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. – Режим доступу : http:// www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0045:EN:NOT

9. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). – Режим доступу : http://www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:NOT

10. Protection of personal data. – Режим доступу : http://www.europa.eu/legislation_ summaries/information_society/data_protection/l14012_en.htm

11. Data Protection Directive. – Режим доступу : http:// www.en.wikipedia.org/wiki/Data_ Protection_Directive

12. International Safe Harbor Privacy Principles. – Режим доступу : http://www.en.wiki pedia.org/wiki/Safe_Harbor_Principles

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~