© Пазюк А.В.

Захист права на приватність користувачів Інтернет.

Вступ.

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 зазначив 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 рядків 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 зустріла публічний протест через застосування системи пошуку людей. Можливості системи дозволяли опрацювати дані про 175 мільйонів людей, вибравши їх із списків прямої розсилки реклами. Після отримання претензій, Yahoo вирішила знищити дані з адресами 85-ти мільйонів користувачів, що їх не було включено до цих списків. У 1997 році, компанія American Online (AOL) оприлюднила плани стосовно розкриття даних, які містили телефонні номери передплатників своїм партнерам по бізнесу. Передплатники виступили проти цього і зазначили, що це суттєво порушувало б умови угоди про надання послуги. У відповідь, компанія відмовилася від своїх планів.[2]

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 права на приватність користувачів глобальної мережі Інтернет.

Право на приватність.

Приватна сторона життя людини отримала свій правових захист у вигляді права на приватність (right to privacy) не так давно. Своє світове визнання право на приватність отримало саме у двадцятому столітті, що пов'язано із появою нових технологій, завдяки яким втручання у приватну сферу життя людини значно спростилося.

У своїй статті, в 1890 році, американські юристи Луїз Д. Брендіс та Самуель Д. Воррен писали: "сучасні винаходи і бізнес-методи вимагають уваги до наступних кроків, що мають бути зроблені для захисту індивідів". [3]. Автори вперше спробували визначити, що таке "право на приватність". На їхню думку, це право "бути залишеним на самоті"(let to be alone), яке містить у собі ідею захисту результатів інтелектуальної і емоційної активності особи у суспільстві.

З розвитком телекомунікаційних технологій, появою комп'ютерів і поширенням автоматизованої обробки персональної інформації, право на приватність набуває додаткового змісту. У відомому рішенні Федерального Конституційного Суду Німеччини, датованому 1983-тім роком 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 основу покладено систему прав особи, що є суб'єктом даних, і якій 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 набувачів, і права під час збору даних;

- отримати копію даних, що були зібрані, включаючи інформацію про їх використання; вносити корективи, знищувати або блокувати (забороняти використання) даних, що обробляються з порушенням закону; а також вимагати повідомлення про це сторонам, яким ці дані було розкрито;

- заперечувати проти обробки на безумовних 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 адекватною, суттєвою і не надмірною у відношенні до таких цілей;

(г) була точною і не застарілою;

(д) 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 набувачів, 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 укладення 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 у суспільних інтересах або здійснюється під час виконання владних повноважень, якими наділено контролера або третю особу, якій ці дані розкриваються;

(е) коли це потрібно для правомірних цілей, яких бажають досягти контролер або третя особа. Або у разі, коли 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. За принципом "обмеження ціллю", використання і обробка персональної інформації обмежені попередньо визначеною ціллю збору даних Вищезазначені принципи правомірності обробки є законним виключенням з цього принципу.

За іншим принципом, обробка персональних даних, що розкривають расове або етнічне походження, політичні переконання або філософські погляди, членство у профспілках, сексуальне життя, стан здоров'я, - заборонена (з великою кількістю винятків). 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 примусових заходів у разі їх порушення. Такі функції на національному рівні виконують уповноважені державні органи. Однак глобальна і децентралізована інфраструктура Інтернет ускладнює цю роботу.

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 століття, Інтернет поступово перетворюється на "мережу мереж".[6] ЇЇ починають використовувати на повсякденних засадах і стрімко поширювати у всьому

світі, завдяки концепції відкритої архітектури побудови мережі (open architecture networking).[7]

У порівняні із уже звичайними засобами передачі інформації, такими як теле- , радіомовлення, Інтернет є новим видом медіуму з унікальними характеристиками. Унікальність цієї мережі полягає у тому, що вона функціонує не тільки як звичайний транслятор, тобто поширювач інформації, але до того ж є комунікаційним засобом.[8]

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

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

Кожний з операторів слугує проміжною ланкою і має можливість втручання у цей процес. Оператори можуть дізнатися не тільки про зміст повідомлення, а і отримати додаткову інформацію. Стандартне повідомлення електронною поштою містить заголовок з інформацією про відправника та набувача, яка включає в себе ім’я, інтернет-адресу, назву вузла, час листування. Це вимагає від користувачів вжиття технічних засобів для забезпечення приватності процесу обміну електронними повідомленнями. [10]

Інтернет загрожує не тільки комунікаційній 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 “он-лайн”, користувач має вступити у контакт з постачальниками цих публікацій чи послуг.

Рухаючись рівень за рівнем в інформаційному “павутинні” 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]

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 користування 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 такою можливістю Інтернет як послуги “он-лайн”. За визначенням, послуги “он-лайн” – це електронні комунікаційні системи, які пропонують за попередньою оплатою своїм передплатникам перелік послуг (електронна пошта, інформаційні послуги, ігри, участь у дискусійних групах за інтересами або спілкування в режимі реального часу), які є доступними через телефонну мережу з використанням модему і комп’ютера. [13]

Як для функціонування будь-якої з традиційних електронних систем, для послуг “он-лайн” потрібна інформація про користувача. Ця інформація використовується в процесах, що відбуваються під час роботи в електронних системах, таких як: авторизації, ідентифікації і посвідчення, контроль права доступу, ревізія і розрахунок .[14] Постачальники послуг “он-лайн” збирають і опрацьовують персональні дані про особу користувача, оскільки це потрібно для роботи електронних 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, висловлювання. Більше того, в США існують організації, які пропонують так звані “пошукові послуги” (“look-up services”) на комерційних засадах.

Шляхи вирішення проблеми.

Вирішити питання захисту приватності користувачів Інтернет можливо за умов вжиття комплексу заходів на організаційному, технічному і нормативному рівнях.

Перш за все, на організаційному рівні пропонується створити міжнародний наглядовий механізм за дотриманням приватності користувачів Інтернет в рамках існуючої системи регулювання Інтернет.[15] 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 отримувати зиск від цього.”[16] Через цю причину, 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 мали належне нормативно-технічне втілення.

На сучасному етапі ситуація починає змінюватися. Так з’являються концепції і технічні розробки, які дають можливість користування телекомунікаційними послугами без ідентифікації особи користувача. [17]

Анонімність користування Інтернет визнається як один із суттєвих принципів, що дозволяє гарантувати певний рівень приватності під час користування Інтернет. [18] З іншого боку, 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 полягає у балансуванні, яке має відбуватися за принципом пропорційності задіяних інтересів, публічних та індивідуальних. Цей принцип знайшов своє відображення в практиці Європейського Суду з прав людини у застосуванні статті 8 Європейської Конвенції про захист прав і основних свобод людини, яка проголошує право на повагу до приватного життя людини.[19]

Слід звернути увагу і на такий механізм як саморегуляція телекомунікаційного сектора через прийняття кодексів “чесної інформаційної практики” (fair information practice) і систему посвідчення

відповідності такої практики проголошеним стандартам. Хоча такий підхід справедливо критикується поборниками ідеї державного регулювання за його слабкість у вирішенні питання притягнення порушників до відповідальності. [20]

На думку автора, для забезпечення приватності в Інтернет, суттєву роль мають відігравати і міжнародні інструменти. Оскільки це глобальне, як сам Інтернет, питання на національному рівні вирішити проблематично.

Закріплені в існуючих міжнародно-правових актах основні засади захисту права на приватність потребують адаптації для застосування в Інтернет. З цією метою вчені пропонують розширити коло прав людини. Серед "нових" прав є такі:

- право не бути внесеним до списків ("a right not to be indexed"); [21]
- право на ефективне шифрування персональної інформації ("a right to encrypt personal information effectively"); [22]
- право на справедливе поводження з людиною у сфері використання системи шифрування "відкритим ключем" ("a right to fair treatment in key public infrastructures"); [23]
- право на розкриття людині даних, що можуть бути використані для створення його споживчого профілю ("a right of disclosure of the collections to which others will have access and which might affect the projection of the profile of the individual concerned"). [24]

Проголошеним правам користувачів Інтернет мають відповідати обов'язки інших суб'єктів інформаційних відносин, задіяних у приватному і публічному секторі.

Феномен Інтернет, якому ми зобов'язані появою такого поняття як приватність "он-лайн", вимагає вжиття комплексних заходів, аби "кінець приватності" не настав.

---

1. The End of Privacy // The Economist. – 1999. - 1 May. – No 11.
2. Jerry Berman, Deirdre Mulligan. Privacy in the Digital Age: Work in Progress// Nova Law Review. – 1999. – Vol. 23. – No 2.
3. Louis D. Brandeis, Samuel D. Warren The Right To Privacy // Harv. L. Rev. – 1890. - P. 193-220

4. Це право проголошується в Ст. 12 Загальної Декларації з прав людини, Ст. 8 Європейської Конвенції про захист прав людини та основних свобод та інших міжнародних документах.
5. Далі наводяться принципи і правила, що встановлені в Директиві Європейського Союзу 1995 року. Стандарти цієї Директиви є жорсткішими у порівняні із відповідними вимогами Конвенції Ради Європи 1981 року та Керівними Принципами Організації Економічної Співпраці і Розвитку 1980 року.
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 і мережі на федеративних засадах.
8. За визначенням Федеральної Ради з питань Побудови Мережі США (Federal Nerworking Council), термін "Інтернет" має застосовуватися до глобальної інформаційної системи, яка - (i) логічно зв'язана глобально унікальним адресним простором, який базується на Протоколі Інтернету (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. Див. посилання 6.
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 Велика Британія, вжили комплекс технічних і організаційних заходів для того, щоб електронні повідомлення, які мають відправника і отримувача на їхніх територіях, не виходили за національні кордони під час свого руху.
10. Серед таких засобів найбільш ефективним є криптографічний захист інформації.
11. Така інформація автоматично записується на комп'ютері користувача завдяки використанню технології "cookies".
12. Recommendation On Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware. Working Party. – 1999. - 23 February. – No. 1/99
13. Таке визначення послугам "он-лайн" дано Комісією ЄС. Див.: Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services. – 1996. – COM (96) 487.
14. Ronald Hes, John Borking. Privacy Enhancing Technologies: the Path to Anonymity. - The Hague. - 1998.

15.Data Protection and Privacy on the Internet: Report and Guidance. The 20th Meeting of the International Working Group on Data Protection in Telecommunications. – Berlin. - 1996. - 19 November.
16.Standardisation and the Global Information Society: The European Approach. Communication from the Commission to the Council and the Parliament. – Brussels. – 1996. – 24 July. – Com (96) 359
17.Серед них, концепція "Захисник Ідентичності" ("Identity Protector"). Див.: посилання 14.
18.Anonymity on the Internet. Recommendation 3/97 EU. Working Party. – 1997. - 3 December.
19. Пазюк А. Захист приватного життя людини в діяльності Ради Європи // Вісник Українського Центру Прав Людини. - 1999. – № 1-2. - С. 9-12.
20.Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country? Working Party. – 1998. - 14 January.
21.Kirby M. D. Privacy Protection – A New Beginning. Доповідь на 21-ій Міжнародній конференції з питань приватності і захисту персональних даних. - Гон-Конг. - 1999.
22.Guidelines for Cryptography Policy. Organisation for Economic Cooperation and Development. – 1997. - 27 March.
23.Див. посилання 20.
24.Clark R. Profiling and Its Privacy Implications. // PLPR. – 1994. – No 7. – P. 128-129; R Wacks. Privacy in Cyberspace: Personal Information, Free Speech and the Internet. Privacy and Loyalty. – Oxford. – 1997. – P. 93.