Вищий навчальний заклад «Український католицький університет»

Факультет суспільних наук

Кафедра теорії права та прав людини

Пояснювальна записка

до дипломного проекту (магістерської роботи)
магістр
на тему «Згода на обробку персональних даних: правова характеристика»

Виконала:
студент ІІ курсу, групи СПЛ17/М
спеціальності
081 «Право»
Мальчик Г. В.
Керівник Галецька Н. Б.
Рецензент Бем М. В.

Львів – 2018 року

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Розвиток технологій сприяє ефективнішому застосуванню автоматизованих методів аналізу даних, у тому числі й персональних. Підприємства все частіше використовують персональні дані у своїх бізнес-процесах. Унаслідок цього, перед належним захистом персональних даних постають нові виклики.

Обробляти персональні дані закон дозволяє лише за наявності легітимних підстав для цього. Згода на обробку персональних даних є однією з таких підстав. Для того, щоби застосувати згоду як підставу для обробки персональних даних, необхідно дотриматися низки вимог. Згода є важливою підставою, оскільки вона надає особі можливість приймати рішення щодо обробки її персональних даних. Правовий аналіз згоди надає можливість правильно розуміти і використовувати цю підставу для обробки персональних даних.

Згода як підстава для обробки персональних даних, є на високому рівні досліджена європейськими науковцями. Проаналізовані окремі вимоги щодо згоди та багато праць щодо аналізу цієї підстави для обробки персональних даних. В Україні ця тема згадана в працях щодо захисту персональних даних, проте детально не проаналізовано особливості згоди, вимоги до неї.

Мета. З огляду на останні зміни в правовому регулюванні згоди в Європейському Союзі та напрям України на євроінтеграцію, вважаю доцільним провести правовий аналіз згоди на обробку персональних даних. Це дозволить провести аналіз українського правового регулювання згоди та одночасно порівняти його з європейським регулюванням.

Метою аналізу є встановлення відповідності українського правового регулювання згоди на обробку персональних даних міжнародним стандартам та визначення способів удосконалення правового регулювання в Україні.

Завдання. Для проведення правового аналізу згоди на обробку персональних даних необхідно передусім розглянути історію розвитку правового регулювання з цього питання. Також, варто проаналізувати наявні

підстави для обробки даних та встановити, чи згода посідає особливе місце серед них. Варто визначити переваги згоди як підстави для обробки персональних даних. Окремо слід проаналізувати, що розуміється під поняттям згоди на обробку персональних даних.

Потрібно дослідити українське законодавство, щоби встановити які вимоги висуваються до згоди, аби вона вважалася дійсно наданою. Аналогічне питання постає до вимог, що передбачені в інших юрисдикціях. На підставі цього можна порівняти вимоги національного регулювання з міжнародними стандартами захисту персональних даних щодо умов дійсності згоди на обробку персональних даних.

Крім того, треба проаналізувати концепцію згоди в сучасному інформаційному суспільстві та визначити її слабкі сторони й можливі напрями удосконалення. На підставі цього слід запропонувати зміни до законодавства щодо згоди на обробку персональних даних, що вдосконалять інститут захисту персональних даних в Україні.

Об’єкт і предмет дослідження. Об’єктом дослідження магістерської роботи є суспільні відносини між суб’єктом персональних даних та володільцем персональних даних у процесі надання першим згоди на обробку своїх персональних даних. Предметом дослідження є нормативна база, а також правозастосовна практика України щодо згоди як підстави для обробки персональних даних та нормативна база зарубіжних країн і окремих міжнародних організацій із вказаного питання.

Теоретичні підходи й методологія дослідження. У ході підготовки магістерської роботи було використано історичний метод для визначення історії становлення згоди як підстави для обробки персональних даних. Широко використовувався порівняльно-правовий метод під час аналізу національних та міжнародних нормативно-правових актів. Системний метод був вжитий для розкриття правових ознак згоди на обробку персональних даних. Крім того, були використані й інші логічні та теоретичні методи.

Джерела. Серед фундаментальних наукових праць щодо захисту персональних даних, використаних під час написання магістерської роботи, можна зазначити роботи таких українських науковців: Бем М.В., Городиський І.М., Бєлова Ю., Кохановська О.В., Пазюк А.В., Брижко В.М., Пилипчук В.Г., Дмитренко О.А.. Окремо згоду на обробку персональних даних досліджують у своїх працях наступні закордонні науковці: Браунсворд Р., Голланд Б., Коста Є., Мізек Я., Мозер Дж., Шермер Б., Солове Д., Карен Й. та багато інших.

Структура магістерської роботи складається зі вступу, трьох розділів та семи підрозділів у них. Перший розділ описує історію розвитку правового регулювання згоди на обробку персональних даних у контексті інституту захисту персональних даних. Також, у цьому розділі міститься порівняння згоди з іншими підставами для обробки персональних даних та досліджується особливість згоди як підстави для обробки персональних даних. У другому розділі досліджуються вимоги до згоди на обробку персональних даних в Україні та інших юрисдикціях, зокрема в Європейському Союзі. Крім того, цей розділ містить порівняння українського правового регулювання та нового європейського регулювання щодо умов дійсності згоди. Третій розділ починається з дослідження слабких сторін згоди на обробку персональних даних та переходить у відповідні пропозиції вдосконалення механізму згоди на обробку персональних даних в Україні.

РОЗДІЛ І
ЗГОДА ЯК ПРОВІДНА ПІДСТАВА ДЛЯ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

1.1. Історія формування та розвитку підстав для обробки персональних даних.

Для того, щоби здійснити правову характеристику згоди на обробку персональних даних, важливо проаналізувати історію формування та розвитку підстав для обробки персональних даних загалом та згоди, як однієї з підстав, зокрема. Досліджуючи історію розвитку згоди на обробку персональних даних (далі – «згоди») варто почати з історії закріплення правового поняття приватності. Зародження права на приватність відбувається в США.

Питання приватності персональних даних цікавило людей здавна, проте актуальності набуло з поширенням перших друкованих газет, коли в рази зросла швидкість поширення інформації. Унаслідок цього назрівають дискусії про те, наскільки преса може втручатися в приватне та сімейне життя.

У 1890 році в американському журналі Harvard Law Review виходить стаття про приватність. Її автори, Уоррен та Брандейс, уперше формують концепцію приватності, як “права бути залишеним у спокої”[1]. В основі права на приватність є загальне право особи бути вільним від переслідування та розголошення, порушенням цього права є моральна шкода особі. Тим не менш, це право не є абсолютним та має свої обмеження. Одним із таких обмежень є “публікація фактів самою особою або з її згоди”[2].

У той час ще не існувало правового закріплення захисту приватності чи персональних даних. В Америці на початку двадцятого сторіччя з’являються судові справи щодо згоди на публікацію фотографій особи в газеті. Першою справою стає Roberson v. The Rochester Folding Box Company у 1902 році[3]. Уже в

[1] Warren S. D., Brandeis L. D. The Right to Privacy // Harvard Law Review. — 1890. — Vol. 4. — P. 193–220..
[2] Там само с. 205, 218.
[3] Spears V. P. The case that started it all: Roberson v. the Rochester folding box company / V. P. Spears // Privacy & Data Security Law Journal. — 2008. — Vol. 11. — P. 1043–1050.

цій справі згадується про згоду особи на оприлюднення її фотографій, і саме згода стає наріжним каменем справи. Хоча справа вирішилася не на користь позивачки, це призвело до подальшого публічного незадоволення і прийняття законодавчих змін. В Нью-Йорку використання імені, фото чи зображення особи з комерційною метою без згоди особи стає злочином[4]. У такий спосіб виникає перше законодавче закріплення згоди на обробку персональних даних.

У 1948 році Генеральна Асамблея ООН приймає визначний документ – Загальну декларацію прав людини. Там знаходиться місце для закріплення права особи на приватність, а саме у статті 12: "Ніхто не може зазнавати безпідставного втручання у його особисте і сімейне життя, безпідставного посягання на недоторканність його житла, таємницю його кореспонденції або на його честь і репутацію. Кожна людина має право на захист закону від такого втручання або таких посягань"[5].

Європейська конвенція про захист прав людини і основоположних свобод 1950 року закріплює в статті 8 право кожного на повагу до свого приватного й сімейного життя, до свого житла і кореспонденції. А втручання в це право дозволяється, лише коли воно "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"[6].

Практика вирішення спорів у Європейському суді з прав людини підтвердила віднесення різних аспектів захисту персональних даних до розуміння приватності в контексті статті 8 Конвенції. Так свого часу до права на приватне життя було віднесено телефонні дзвінки[7], телефонні номери[8], голосові

[4] Spears V. P. The case that started it all: Roberson v. the Rochester folding box company.
[5] Загальна декларація прав людини від 10.12.1948. База даних «Законодавство України»/ВР України. URL: http://zakon2.rada.gov.ua/laws/show/ 995_015 .
[6] Європейська конвенція про захист прав людини і основоположних свобод від 4 листопада 1950 року. База даних «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/995_004.
[7] Рішення ЄСПЛ у справі Klass v Germany, заява 5029/71, 06/09/1978, п.41 URL: http://hudoc.echr.coe.int/eng?i=001-57510.
[8] Рішення ЄСПЛ у справі Malone v UK, заява 8691/79, 02/08/1984, п.64 URL: http://hudoc.echr.coe.int/eng?i=001-57533.

записи[9], використання електронної пошти та інтернету[10], відеоспостереження[11], комп'ютери[12], право на доступ до своїх даних[13] та інші.

У справі ЄСПЛ Ротару проти Румунії Суд визнав, що систематичне збирання та зберігання персональних даних державними службами підпадає під розуміння приватності відповідно до статті 8 Європейської конвенції про захист прав людини і основоположних свобод[14]. Суд у цій справі встановив, що якість законодавства не забезпечувала належні гарантії щодо захисту персональних даних заявника у разі їх обробки, отже, мало місце порушення права на приватність[15]. Отже, ЄСПЛ відносить захист персональних даних до одного з аспектів захисту приватності.

Міжнародний пакт про громадянські і політичні права ООН 1966 року також зазначає в статті 17, що "ніхто не повинен зазнавати свавільного чи незаконного втручання в його особисте і сімейне життя, свавільних чи незаконних посягань на недоторканність його житла або таємницю його кореспонденції чи незаконних посягань на його честь і репутацію"[16].

Жоден із цих документів не згадує згоду на обробку персональних даних, що є логічним, зважаючи на їх загальний та декларативний характер. У них йдеться про безпідставне та незаконне втручання в приватне життя особи, а сама законність втручання встановлюється кожною державою.

У цей час починають з'являтися перші комплексні національні закони щодо захисту персональних даних. Це було пов'язано, насамперед, з комп'ютерною революцією 1960-70-их років та створенням баз даних осіб, адже

---

[9] Рішення ЄСПЛ у справі P.G. and J.H. v UK, заява 44787/98, 25/09/2001, п.59, URL: http://hudoc.echr.coe.int/eng?i=001-59665.

[10] Рішення ЄСПЛ у справі Copland v UK, заява 62617/00, 03/04/2007 , п.44, URL: http://hudoc.echr.coe.int/eng?i=001-79996.

[11] Рішення ЄСПЛ у справі Perry v UK, заява 63737/00, 17/07/2003, п.39, URL: http://hudoc.echr.coe.int/eng?i=001-61228.

[12] Рішення ЄСПЛ у справі Leander v. Sweden, заява 9248/81, 26/03/1987, п.48, URL: http://hudoc.echr.coe.int/eng?i=001-57519.

[13] Рішення ЄСПЛ у справі Gaskin v UK, заява 10454/83, 07/07/1989, п.49, URL: http://hudoc.echr.coe.int/eng?i=001-57491.

[14] Рішення ЄСПЛ у справі Potaru v Romania, заява 28341/95, 04/05/2000, п.44, URL: http://hudoc.echr.coe.int/eng?i=001-58586.

[15] Так само.

[16] Міжнародний пакт про громадянські і політичні права від 16.12.1966. База даних «Законодавство України»/ВР України. URL: http://zakon2.rada.gov.ua/laws/show/ 995_043.

перед захистом приватності постають нові виклики. У Європі укладають національні закони, що регулюють захист даних. Першим стає шведський Закон про дані в 1973 році. Слідом за Швецією, національні закони приймають Німеччина та Франція в 1977 та 1978 роках відповідно. Французький захист даних базується на свободі, у той час коли німецький – на праві визнання людської гідності[17].

Тим часом, американська концепція приватності розвивалась у іншому напрямі. У 1973 році Міністерство охорони здоров'я, освіти і соціального забезпечення США видає звіт «Записи, комп'ютери та права громадян» («Records, Computers and the Rights of Citizens»), у якому вводиться ідея кодексу чесного використання інформації (fair informational practices). Ця ідея не дає підстав для визначення апріорі того, які дані повинні або можуть бути зібрані та використані, або з яких підстав і коли. Однак, вона забезпечує основу для встановлення процедур, що гарантують особі право брати участь у значущій формі в прийнятті рішень про те, яка інформація збирається про нього та про те, як ця інформація буде використовуватися[18].

Уже через рік, в 1974 році, у США приймають Акт про Приватність. Сферою його дії була діяльність федеральних органів влади, та не поширювалася на органи влади штатів, місцеві органи та приватний сектор[19]. Протягом подальших десятиріч у США прийнято низку законодавчих актів, що врегульовують галузеві питання захисту персональних даних. До таких можна віднести Акт про банківську таємницю 1970 року, Акт про право на фінансову приватність 1978 року, Акт про політику кабельного зв'язку 1984 року, Акт про приватність електронних комунікацій 1986 року, Акт про відповідальність і перенесення даних про страхування здоров'я громадян (HIPAA) 1996 року, Акт про захист приватності дітей онлайн (COPPA) 1998 року.

[17] Ajana, Btihaj. (2009). Reinventing data protection? Springer Netherlands. P. 10.
[18] United States. Department of Health, Education, and Welfare. Secretary's Advisory Committee on Automated Personal Data Systems & Ware, Willis H 1973, Records, computers, and the rights of citizens : report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Dept. of Health, Education & Welfare.
[19] Solove, Daniel J., A Brief History of Information Privacy Law. Proskauer On Privacy, PLI, 2016; GWU Law School Public Law Research Paper No. 215. URL: https://ssrn.com/abstract=914271.

Проте ні загальний, ні спеціальні закони не передбачали підстав для обробки персональних даних. Про згоду згадується лише в контексті розголошення даних, а не їх збирання, в Акті про Приватність 1974 року.

Основні відмінності європейського та американського підходів до захисту персональних даних охарактеризував у своїй дисертаційній роботі Андрій Пазюк:

> За європейським підходом будь-яке обмеження права на приватність як фундаментального права людини, у тому числі з метою захисту свободи слова, розглядається з точки зору дотримання певних вимог, вироблених у практиці європейських конвенційних органів - Європейської Комісії й Суду з прав людини. Такі обмеження права на приватність повинні запроваджуватися на підставі закону, мати легітимну ціль, бути необхідними в демократичному суспільстві і пропорційними до мети їх застосування.
>
> Судова доктрина США, навпаки, розглядає прийняття будь-якого нормативно-правового акта з інформаційних питань, у тому числі щодо захисту права на приватність персоніфікованої інформації, як обмеження свободи слова, отже, як таке, що повинно бути виправданим суттєвими інтересами і не обмежувати надмірно, як за засобами так і обсягом, свободу вільного одержання й поширення інформації[20].

Трохи з іншого боку описав ці відмінності іноземний спеціаліст приватності Даніель Солове. Він вказує, що в ЄС більш патерналістський підхід до обробки даних. Право ЄС має більш суворі й докладні вимоги до згоди, ніж право США. До того ж, право ЄС більш суворе до збирання, використання чи розкриття даних, вимагаючи легітимну підставу перед обробкою даних. У той час у США дані за загальним правилом можуть оброблятися, якщо закон окремо не забороняє певну обробку[21].

Це є дуже вдалі описи різниці між захистом персональних даних у двох юрисдикціях (якщо брати правове регулювання ЄС, як окрему юрисдикцію). Фактично, підходи до захисту персональних даних у ЄС та США ґрунтуються на різних аспектах. У той час, коли в ЄС вимагається виправдання втручання в

[20] Пазюк А. В. Міжнародно-правовий захист права людини на приватність персоніфікованої інформації : автореф. дис. на здобуття наук. ступеня канд. юр. наук : спец. 12.00.11 "міжнародне право" / Пазюк Андрій Валерійович – Київ, 2004. – 13 с.

[21] Solove D. J. Privacy self-management and the consent dilemma / D. J. Solove // Harvard Law Review. — 2013. — Vol. 126, No. 7. — P. 1880–1903. P. 1897.

приватність, у США лише встановлюють окремі обмеження щодо певних даних. Водночас, у ЄС використовують згоду, а в США вимагають повідомлення суб'єкта про обробку його даних. Ці підходи відрізняються концептуально. В Україні було прийнято європейський підхід, отже, подальший аналіз буде зосереджений на ньому.

Міжнародна спільнота просувається далі в регулюванні захисту персональних даних. Взявши за основу принципи чесного використання інформації розроблені в 1973 році в США, в 1980 році Організація економічного співробітництва і розвитку приймає Керівні принципи, що регулюють захист приватності і транскордонні потоки персональних даних. Одним із принципів є обмеження збирання персональних даних, такі дані повинні бути отримані законно й чесно та, де доречно, з обізнаністю або згодою суб'єкта персональних даних[22].

В той час , 1981 року, Рада Європи приймає Конвенцію про захист осіб у зв'язку з автоматизованою обробкою персональних даних, або так звану Конвенцію № 108. Вона містить рекомендації щодо захисту персональних даних у разі їх автоматичної обробки, гарантії такого захисту. Проте, цей документ ще не містить ні інституту підстав обробки даних, ні згоди, як однієї з підстав. І немає очевидних причин, чому згода не відіграє більшої ролі в цій Конвенції[23].

Тим не менш, Конвенція № 108 є важливою в контексті українського законодавства. За словами одного з авторів законопроекту «Про захист персональних даних», Брижко Валерія Михайловича, саме завдяки курсу України на інтеграцію до Європейського Союзу[24], Конвенція № 108 була приводом для написання даного законопроекту і творенні інституту захисту персональних даних в Україні[25]. Згадана Конвенція № 108 підписана у 2005 році

[22] Guidelines governing the protection of privacy and transborder flows of personal data (23 September 1980) Organisation for Economic Cooperation and Development.
[23] Opinion 15/2011 on the definition of consent. Adopted on 13 July 2011. URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187en.pdf, p. 4.
[24] Брижко В. М Про приведення інформаційного законодавства України у відповідність до положень європейського права / В Брижко // Правова інформатика. - № 1(25)/2010. – С. 14-22.
[25] Брижко В. М. Про упорядкування законодавства України із захисту персональних даних / В. М. Брижко // Правова інформатика. – 2008. – № 1(17). – С. 20-34.

та ратифікована Україною у 2010 році, безпосередньо після прийняття Закону України «Про захист персональних даних». Ключову роль у Конвенції № 108 відіграло те, що вона фактично зобов'язала держави приймати національне законодавство у сфері захисту персональних даних, як це і відбулося в Україні.

Розвиток технологій та поява інтернету в 90-их призвели до нових викликів безпеці персональних даних. І саме тоді згода вперше отримує юридичне закріплення на рівні ЄС у Директиві 95/46/ЄС Європейського Парламенту й Ради "Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних" від 24 жовтня 1995 року.

Метою прийняття Директиви 95/46/ЄС було полегшення транскордонних потоків даних із дотриманням однакового рівня захисту даних на території країн ЄС. Ця Директива вводить підстави для обробки персональних даних, які одержують назву категорій законності обробки даних, й однією з категорій якраз є недвозначна згода суб'єкта даних[26].

Директива також вводить у загальноєвропейський правовий обіг визначення згоди: "згода суб'єкта даних означає будь-яке вільно виражене спеціальне й поінформоване зазначення його бажань, за допомогою якого суб'єкт даних дає свою згоду на обробку персональних даних, які його стосуються"[27]. Це призводить до певної уніфікації правового розуміння згоди серед європейських держав.

Проте, юридична сила директив для держав-членів ЄС визначається відповідно до статті 249 Договору про заснування Європейської Спільноти, а саме наступним чином: "директива є обов'язковою для кожної держави-члена, якій її адресовано, щодо результатів, що їх треба досягти, однак залишає національній владі цілковиту свободу вибирати форму та засоби досягнення цих результатів"[28]. Тобто, для реалізації цілей директиви держави повинні прийняти

[26] 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. Official Journal L. 1995. URL: http://eur-lex.europa.eu/legal- content/en/TXT/?uri=CELEX%3A31995L0046. - art. 7.

[27] 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.

[28] European Union - Consolidated version of the Treaty on the Functioning of the European Union - Protocols - Annexes - Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed

відповідні рішення на національному рівні. Крім того, вони вільні обирати, як вони досягатимуть поставлених цілей. Отже, такий підхід не призводив до уніфікованого законодавства щодо захисту персональних даних у ЄС, а лише встановив вимогу результату – належного захисту даних.

Уже невдовзі ЄС приймає перший документ, що закріплює права людини на рівні Союзу. Це Хартія основоположних прав ЄС 2000 року. Поміж інших прав знаходиться й захист персональних даних. Згідно з текстом Хартії "такі дані мають оброблятися справедливо та можуть збиратися виключно для спеціально визначених цілей і на підставі попередньої згоди зацікавленої особи або на іншій законній підставі, передбаченій законодавством"[29]. Відповідно до даного положення, згода суб'єкта даних відіграє першочергову роль при обробці порівнюючи з іншими підставами. Проте в подальшій регулятивній правотворчості ця позиція виділення згоди перед іншими підставами не збережеться.

За кілька років, у 2002 році, в ЄС була прийнята Директива № 2002/58/ЄС Європейського Парламенту і Ради ЄС стосовно обробки персональних даних та захисту права на недоторканість особистого життя в сфері електронних комунікацій, або Директива ePrivacy. Вона також робить акцент на згоді при обробці персональних даних в сфері електронних мереж та комунікацій. Зокрема, Директива № 2002/58/ЄС поширюється й на захист легітимних інтересів юридичних осіб, у тому числі вимоги щодо дійсності згоди, визначені Директивою 95/46/ЄС[30]. Цей документ є спеціальним актом що застосовується до обмеженого кола правовідносин, та підтримує вже закріплені положення про згоду на обробку персональних даних.

---

on 13 December 2007, art.87((2)a) and art 88(2(a)) URL : http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT. Art. 249.

[29] Charter of Fundamental Rights Of The European Union, 18.12.2000, Official Journal of the European Communities, C 364/1 : http://www.europarl.europa.eu/charter/pdf/text_en.pdf. Art. 8.

[30] 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) URL: http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32002L0058&model=guichett.

Натомість, в Україні довгий час не було правового регулювання захисту персональних даних. У 2003 зареєстрований перший законопроект, який після вето Президента так і не був прийнятий[31]. У ньому була спроба запровадити право власності на персональні дані. На підтримку цієї концепції було написано кілька наукових робіт, які описані нижче.

Наприклад, у дисертації Дмитренко Олени «Право фізичної особи на власні персональні дані в цивільному праві України» детально розписується вказана концепція. Змістом права власності на персональні дані є правомочності благообладання, благовикористання та права на захист. Під благовикористанням мається на увазі "юридично забезпечену можливість фізичної особи приймати рішення щодо використання власних персональних даних у суспільних відносинах"[32]. Також "підкреслено, що в сучасному праві та правовій доктрині право на погодження використання персональних даних представлено як обов'язок зобов'язаного суб'єкта отримати від суб'єкта права на персональні дані згоду на таке використання перед його початком"[33]. Проте саме ця концепція призвела до відмови прийняти законопроект 2003 року[34].

Необхідність прийняття відповідного законодавства в Україні була зумовлена потребою захисту прав осіб на приватність на відповідному рівні та курсом євроінтеграції України[35]. Зокрема, у Програмі інтеграції України до Європейського Союзу від 04.09.2000 року, визнано потребу розроблення проекту базового комплексного Закону України з питань захисту інформації про особу. Згідно з цим документом, основним орієнтиром для відповідного законодавства може слугувати, окрім Конвенції № 108, ще й Директива 95/46/ЄС.

---

[31] Брижко В. М. Про упорядкування законодавства України із захисту персональних даних. С. 25.

[32] Право фізичної особи на власні персональні дані в цивільному праві України : автореф. дис. ... канд. юрид. наук : 12.00.03 / О. А. Дмитренко; Акад. прав. наук України, НДІ приват. права і підприємництва. - К., 2010. - 19 с. с. 12

[33] Там само.

[34] Пилипчук, В. Г.. Реформування і розвиток системи захисту персональних даних в Україні [Текст] / Пилипчук В. Г., Брижко В. М. // Інформація і право : наук. журн.. - 2017. - N 3. - С. 5-21. - С. 8.

[35] Пояснювальна записка до Проекту Закону України «Про захист персональних даних» № 2297-VI від 01.06.2010. База даних «Законодавство України»/ВР України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=32124&pf35401=119742.

Саме таким шляхом пішов законодавець і прийнятий 01.06.2010 року Закон України «Про захист персональних даних»[36] фактично базується на положеннях Директиви 95/46/ЄС, у тому числі положеннях щодо згоди. Це підтверджується порівнянням обох актів. Крім того, М. Бем, І. Городиський та інші стверджують, "що якби не Директива, положення Закону було би вкрай важко правильно розуміти"[37]. Отже, сам законотворчий процес вказує на тісний зв'язок українського інституту захисту персональних даних із європейськими актами.

Для реалізації положень Закону України «Про захист персональних даних» було створено Державну службу з питань захисту персональних даних. У 2014 році згадану службу ліквідовано, а повноваження із захисту персональних даних покладено на Уповноваженого Верховної Ради з прав людини[38].

Уповноваженим затверджено низку підзаконних актів, що регулюють втілення положень Закону України «Про захист персональних даних». Серед них Типовий порядок обробки персональних даних, Роз'яснення Уповноваженого Верховної Ради України з прав людини до Типового порядку обробки персональних даних. У такий спосіб був створений та розбудовувався інститут захисту персональних даних в Україні.

Згодом у ЄС виникає потреба в оновленні правового регулювання захисту персональних даних, причини для чого викладені в тексті Загального Регламенту Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних (GDPR)), зокрема:

---

[36] Про захист персональних даних : Закон України від 01.06.10 р. № 2297-VI // Відомості Верховної Ради України (ВВР). – 2010. – № 34. – Ст. 481.

[37] Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. – К.: К.І.С., 2015. – С. 17.

[38] Законом України «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних», який набув чинності 1 січня 2014 року, Уповноваженому ВР з прав людини надано повноваження у сфері захисту персональних даних.
Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних: Закон від 03.07.2013 № 383-VII. База даних «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/383-18.

> Стрімкий технологічний розвиток і глобалізація призводять до виникнення нових труднощів для захисту персональних даних. Масштаби збирання та спільного використання персональних даних суттєво зросли. Технології дозволяють як приватним компаніям, так і публічним органам користуватися персональними даними в безпрецедентних масштабах з метою реалізації своєї діяльності. Фізичні особи дедалі частіше надають доступ до персональної інформації для громадськості та в глобальному масштабі. Технології змінили як економіку, так і суспільне життя і повинні надалі стимулювати вільний рух персональних даних у межах Союзу та передавання їх до третіх країн і міжнародних організацій, забезпечуючи при цьому високий рівень захисту персональних даних[39].

Загальний регламент про захист даних ЄС (GDPR) запроваджує нові правила щодо обробки даних, зокрема й щодо згоди на таку обробку. Докладніше про вимоги до згоди згідно з цим актом буде описано в наступних розділах. Проте варто зауважити, чому Регламент (ЄС) 2016/679 (GDPR) є важливий саме в українському контексті.

Уже згаданий курс на євроінтеграцію України, що зараз набирає обертів, є одним із чинників. В Угоді про асоціацію між Україною та Європейським Союзом від 27 червня 2014 року вказано, що "сторони домовилися співробітничати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських та міжнародних стандартів"[40]. На виконання Угоди Кабінетом Міністрів України 25 жовтня 2017 року затверджено план заходів. У ньому завданням 11 визначено "Удосконалення законодавства про захист персональних даних з метою приведення його у відповідність з Регламентом (ЄС) 2016/679 (GDPR)"[41]. Тобто, рано чи пізно, Україна буде змушена прийняти законодавство, що відповідатиме європейським вимогам щодо захисту даних.

---

[39] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). Офіційний вісник Європейського Союзу L 119/1 04.05.2016 (офіційний переклад).

[40] Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 27.06.2014 року. База даних «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/984_011 ст. 13

[41] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних).

Крім того, Регламент (ЄС) 2016/679 (GDPR) уже зараз може бути застосований в Україні, оскільки він має екстериторіальну дію. Це стосується, наприклад, компаній, які обробляють дані резидентів ЄС чи яким компанії з ЄС передають персональні дані[42]. У таких випадках Регламент матиме пряму дію для окремих осіб.

Крім того, Регламентом встановлено вимоги до передачі даних у треті країни. Така передача даних можлива лише за гарантії належного рівня захисту персональних даних, що відповідатиме стандартам Регламенту[43]. Можна стверджувати, що для України важливо розглядати положення про захист персональних даних у порівнянні з відповідними положеннями Європейського Союзу.

Для втілення положень Директиви 95/46/ЄС було створено Робочу групу, що діє відповідно до статті 29 (Article 29 Working Party). Вона видала Думку про визначення згоди та Напрямні щодо згоди відповідно до Регламенту (ЄС) 2016/679 (GDPR). Вони є основними офіційними документами, що тлумачать положення про згоду на обробку персональних даних та детально роз'яснюють умови дійсності згоди. Відповідно, до них варто звертатися для належного уточнення норм щодо захисту даних у ЄС.

У підсумку, згода на обробку персональних даних згадується ще в перших публікаціях, які вводили концепцію права на приватність, отже, вона є тісно пов'язана з цим правом. З часом законодавство про приватність персональних даних розвивається різними шляхами в США та країнах Європи. Зі стрімким технологічним розвитком наприкінці 20 століття утворюється система захисту персональних даних на рівні Європейського Союзу.

Українське законодавство в значній мірі бере за основу положення правових актів ЄС при прийнятті власного законодавства щодо захисту даних. У сучасних умовах євроінтеграції і з огляду на екстериторіальність Регламенту про

[42] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних).
[43] Там само.

захист даних ЄС, необхідно розглядати та аналізувати українське законодавство в порівнянні з Регламентом (ЄС) 2016/679 та його тлумаченням.

1.2. Види підстав для обробки персональних даних

Чинна система захисту персональних даних не дозволяє незаконного втручання в приватність життя осіб. Один із принципів опрацювання персональних даних є законність обробки. Це означає, що дані можна обробляти лише за наявності відповідної підстави, передбаченої законом.

Оскільки на законодавчому рівні визнається бажання людини не поширювати особисту інформацію про неї, то лише закон може встановити випадки, коли ця інформація може використовуватись. Це є передусім згода самої особи, а також інші підстави. Крім того, виділяються особливі категорії, так звані чутливі дані, які можуть оброблятися лише у виняткових випадках, перелічених у законі.

“Кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції”[44], зазначає стаття 8 Європейської конвенції про захист прав людини і основоположних свобод. Це зумовлює те, що втручання в приватність особи не може бути свавільним. Випадки такого втручання мають бути встановлені законами, про що пише в другій частині цієї статті Конвенції. Ці випадки втілюються в підставах для обробки персональних даних.

У Конституції України також закріплено право на приватність, яке сформульоване наступним чином:

> Стаття 32. 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[45].

[44] Європейська конвенція про захист прав людини і основоположних свобод від 4 листопада 1950 року.
[45] Конституція України: Закон від 28.06.1996 № 254к/96-ВР. База даних «Законодавство України»/ВР України. URL: http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

З цього положення можна зробити висновок, що підставами для обробки персональних даних є згода особи та інші законні підстави. Це положення Конституції отримало також своє тлумачення Конституційним Судом України. “Положення частини другої статті 32 Основного Закону України передбачають вичерпні підстави можливого правомірного втручання в особисте та сімейне життя особи”[46]. І судді Конституційного Суду також виділяють обробку на підставі згоди, а у випадку її відсутності – на підставі законів.

Згода та інші законні підстави для обробки персональних даних перелічені в ч. 1 ст. 11 Закону України «Про захист персональних даних»[47], яка визначає загальні вимоги до такої обробки:

> Підставами для обробки персональних даних є:
> 1) згода суб’єкта персональних даних на обробку його персональних даних;
> 2) дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень;
> 3) 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;
> 4) захист життєво важливих інтересів суб’єкта персональних даних;
> 5) необхідність виконання обов’язку володільця персональних даних, який передбачений законом;
> 6) необхідність захисту законних інтересів володільця персональних даних або третьої особи, якій передаються персональні дані, крім випадків, коли потреби захисту основоположних прав і свобод суб’єкта персональних даних у зв’язку з обробкою його даних переважають такі інтереси.[48]

Порівнюючи згоду з іншими підставами можна вважати розумним поділ усіх підстав на згоду та інші законні підстави. Адже до згоди закон встановлює підвищені вимоги, зокрема щодо поінформованості суб’єкта персональних даних. Інші підстави таких вимог не містять. Також, незалежно від того, яка

---

[46] Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20.01.2012 № 2-рп/2012. База даних «Законодавство України» /ВР України. URL: http://zakon1.rada.gov.ua/laws/show/v002p710-12.

[47] «Обробка персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством.»
Про захист персональних даних: Закон від 01.06.2010 № 2297-VI.

[48] Про захист персональних даних: Закон від 01.06.2010 № 2297-VI.

підстава була використана для збирання даних, для їх поширення необхідно отримати згоду суб'єкта персональних даних, за винятками визначеними законом, і лише якщо це необхідно в інтересах національної безпеки, економічного добробуту та прав людини[49]. Тобто, згода виділяється з-поміж інших підстав.

Актуально в даному контексті відмітити, що згода є особливою підставою для обробки даних. При прийнятті першої Директиви ЄС про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних у 1995 році в початковій редакції цього документу в основі законності обробки лежала саме згода, а всі інші підстави були другорядними, винятками до згоди[50]. У прийнятому варіанті це змінили, і згода стала лише однією серед підстав, серед яких немає пріоритетності. Крім того, Хартія основоположних прав ЄС вказує згоду як підставу для обробки даних, водночас, лише зазначаючи на противагу згоді всі інші законні підстави для обробки[51].

Тим не менш, деякі науковці прирівнюють підставу щодо укладення та виконання правочину до згоди. Так, М. Бем, І. Городиський та інші відносять правочин до згоди, аргументуючи це тим, що добровільність правочину, встановлена цивільним законодавством, відповідає схожим вимогам до згоди[52].

Цю думку частково підтримує німецький юрист Яна Мозер: "Вільне волевиявлення правочину відповідає праву на інформаційне самовизначення"[53]. Це право визначене практикою Німецького Конституційного Суду, і фактично означає "право вирішувати для себе коли і в яких межах особиста інформація та факти можуть бути розкриті іншим"[54]. Фактично, у цій справі німецький суд

[49] Про захист персональних даних: Закон від 01.06.2010 № 2297-VI. ст. 14.
[50] Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data COM(90) 314 final — SYN 287 (Submitted by the Commission on 27 July 1990) (90/C 277/03) URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51990PC0314(01)&from=EN.
[51] Charter of Fundamental Rights Of The European Union, 18.12.2000, Official Journal of the European Communities, C 364/1 : http://www.europarl.europa.eu/charter/pdf/text_en.pdf. Art. 8.
[52] Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. С. 53, 61.
[53] Mozer J. Consent and contract under GDPR – Prohibition of consent bundling. URL: https://datareality.eu/consent-contract-gdpr-bundling/.
[54] A Comparative Analysis in Relation to Informational Self-Determination and Privacy: The Icelandic Health Sector Database Decision and The German Census Act Decision. 2007. URL: https://www.duo.uio.no/bitstream/handle/10852/21511/8003.pdf?sequence=1 С. 7.

визначив, що втручання має супроводжуватись однозначними положеннями законодавства, чіткою метою та відповідними гарантіями, що відповідає трактуванню Європейського суду з прав людини[55].

Проте, на мою думку, ризиковано стверджувати, що при підставі правочину виконуються всі вимоги, що ставляться до згоди, адже це не завжди знаходить підтвердження. Спільним для обох підстав є воля особи. Правочин згідно з цивільним законодавством повинен відповідати низці вимог, які викладені в статті 203 Цивільного Кодексу України, відповідно до частини 3 якої "волевиявлення учасника правочину має бути вільним і відповідати його внутрішній волі"[56]. Тому, у разі виявлення бажання вчинити правочин, особа має розуміти, що деякі персональні дані можуть бути опрацьовані для досягнення результату правочину.

Відмінним, як видається, є обсяг обробки даних. Для виконання правочину обробка даних має бути необхідною умовою, без якої унеможливлюється укладення та виконання правочину. У згоді особа може дозволити використання даних для будь-якої наперед визначеної проінформованої мети.

Щодо цього питання в ЄС зазначають, що "здійснюючи оцінку того, чи є згода вільно наданою, необхідно максимально враховувати те, чи залежить, між іншим, виконання договору, у тому числі надання послуги, від згоди на опрацювання персональних даних, що не є необхідною для виконання такого договору"[57]. Тут підстава правочину більше нагадує виконання офіційних повноважень володільцем, оскільки передбачає певний обов'язок володільця персональних даних, для виконання якого й необхідна обробка даних.

[55] Decision of the First Senate of 15 December 1983 - 1 BvR 209/83 et al. Federal Constitutional Court, Karlsruhe. URL: http://www.datenschutzberlin.de/gesetze/sonstige/volksz.htm.

[56] Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. С. 61.

[57] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). Ст. 7(4).

Крім того, за підставою правочину в особи немає права відкликати згоду. Це встановлює надмірну необмеженість цієї підстави, тому вона значно відрізняється від згоди особи на обробку даних.

Щодо права ЄС, аналогічно до нашого законодавства, Регламент (ЄС) 2016/679 (GDPR) виділяє шість підстав для обробки персональних даних:

- згода;
- взаємовідносини за контрактом;
- правові зобов'язання володільця;
- життєво важливі інтереси суб'єкта персональних даних;
- суспільний інтерес та виконання офіційних повноважень;
- законні інтереси, які переслідує володілець або третя особа[58].

Ці підстави практично відповідають тим, що передбачені в нашому законодавстві, але є окремі відмінності, що будуть проаналізовані згодом.

Окремо регулюється обробка чутливих даних. Чутливими вважаються дані, що вимагають посиленого контролю. "Персональні дані, що, за своєю специфікою, є особливо чутливими щодо фундаментальних прав і свобод, потребують особливого захисту, оскільки контекст їхнього опрацювання може створити істотні ризики для фундаментальних прав і свобод"[59]. До таких даних Закон України «Про захист персональних даних» відносить "расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також дані, що стосуються здоров'я, статевого життя, біометричних або генетичних дані"[60].

Стаття 7 цього Закону України встановлює загальну заборону обробки таких даних, проте в другій частині встановлено випадки, коли такі дані можуть все таки оброблятися. Ці випадки підпадають під перелічені раніше загальні

[58] Посібник з європейського права у сфері захисту персональних даних. — К.: К.І.С., 2015. — С. 89-93.
[59] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних), преамбула п. 51.
[60] Про захист персональних даних: Закон від 01.06.2010 № 2297-VI. ст. 7.

підстави, проте вони є вужчими й конкретнішими, оскільки їх неналежний захист несе значні ризики. Цими підставами за законом (ч. 2 ст. 7 ЗУ «Про захист персональних даних») є:

> (…) якщо обробка персональних даних:
> 1) здійснюється за умови надання суб'єктом персональних даних однозначної згоди на обробку таких даних;
> 2) необхідна для здійснення прав та виконання обов'язків володільця у сфері трудових правовідносин відповідно до закону із забезпеченням відповідного захисту;
> 3) необхідна для захисту життєво важливих інтересів суб'єкта персональних даних або іншої особи у разі недієздатності або обмеження цивільної дієздатності суб'єкта персональних даних;
> 4) здійснюється із забезпеченням відповідного захисту релігійною організацією, громадською організацією світоглядної спрямованості, політичною партією або професійною спілкою, що створені відповідно до закону, за умови, що обробка стосується виключно персональних даних членів цих об'єднань або осіб, які підтримують постійні контакти з ними у зв'язку з характером їх діяльності, та персональні дані не передаються третій особі без згоди суб'єктів персональних даних;
> 5) необхідна для обґрунтування, задоволення або захисту правової вимоги;
> 6) необхідна в цілях охорони здоров'я, встановлення медичного діагнозу, для забезпечення піклування чи лікування або надання медичних послуг, функціонування електронної системи охорони здоров'я за умови, що такі дані обробляються медичним працівником або іншою особою закладу охорони здоров'я чи фізичною особою - підприємцем, яка одержала ліцензію на провадження господарської діяльності з медичної практики, та її працівниками, на яких покладено обов'язки щодо забезпечення захисту персональних даних та на яких поширюється дія законодавства про лікарську таємницю, працівниками центрального органу виконавчої влади, що реалізує державну політику у сфері державних фінансових гарантій медичного обслуговування населення, на яких покладено обов'язки щодо забезпечення захисту персональних даних;
> 7) стосується вироків суду, виконання завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом та здійснюється державним органом в межах його повноважень, визначених законом;
> 8) стосується даних, які були явно оприлюднені суб'єктом персональних даних[61].

Так, щодо згоди, для обробки чутливих даних потрібно отримати однозначну згоду особи на обробку її даних. Така згода "повинна бути явно вираженою, зрозумілою та безсумнівною"[62]. Обробка даних у сфері трудових правовідносин відповідає правовим зобов'язанням володільця. Питання обмеженої дієздатності чи недієздатності чітко вписуються в загальну підставу

[61] Про захист персональних даних: Закон від 01.06.2010 № 2297-VI, ст.7.
[62] Бєлова Ю. Умови дійсності згоди на обробку персональних даних / Ю. Бєлова // Підприємництво, господарство і право. — 2017. —№ 11. — Р. 14–18.

життєвих інтересів суб'єкта даних. Виняток щодо участі в об'єднаннях громадян також відповідає підставі виконання обов'язку володільцем даних. Обґрунтування правової вимоги розглядається через необхідність захисту законних інтересів володільця даних або третіх осіб. Обробка чутливих даних у цілях охорони здоров'я може бути виконанням офіційних повноважень чи виконанням правочину. Сьомий пункт прямо вказує на виконання офіційних повноважень володільцем даних. Пряме ж оприлюднення даних означає, що особа сама дозволяє використовувати ці дані невизначеному колу осіб, тобто передбачає згоду. Очевидно, що підстави для обробки чутливих даних вужчі за загальні підстави, проте вони всі охоплюються загальними.

Уповноважений Верховної Ради з прав людини також відмежовує згоду від інших підстав, проте дає рекомендацію використовувати згоду, якщо інші підстави не підходять. У своєму Листі від 03.03.2014 № 2/9-227067.14-1/НД-129 Уповноважений вказує, що володільцям та розпорядникам персональних даних отримувати згоду на обробку таких даних доведеться, зокрема, у тих випадках, коли є потреба для обробки цих даних, а інші передбачені статтею 11 Закону підстави для обробки таких даних не поширюються на цей випадок обробки даних[63].

Проте наявна судова практика вказує, що часто згоду змішують із підставою договору. Зокрема таке відслідковується при укладенні договорів банківського кредиту чи позики. Наприклад, рішення Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ від 26 жовтня 2016 року в справі 473/2644/15-ц демонструє неточності у виділенні конкретної підстави для обробки персональних даних.

Позивач звернулася до суду з позовом та просила, поміж іншого, визнати неправомірними дії банку щодо поширення її персональних даних без відповідної згоди. Основна мотивація суду полягала в наступному:

[63] Лист Уповноваженого Верховної Ради з прав людини від 03.03.2014 № 2/9-227067.14-1/НД-129. База даних «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/v7067715-14.

Згідно із п. 3 ч. 1 ст. 11 Закону України «Про захист персональних даних» підставами для обробки персональних даних є 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.

Відмовляючи в задоволенні позову, суд першої інстанції, з висновками якого погодився й апеляційний суд, виходив із того, що уклавши кредитний договір № 11395008000 від 23 вересня 2008 року, ОСОБА_1 надала банку свою згоду збирати, зберігати, використовувати, поширювати і отримувати інформацію - дані про неї, відомі банку або третім особам у зв'язку з укладенням та виконанням договору, у тому числі банківську та комерційну таємницю, необхідну при укладанні договорів, у тому числі щодо відступлення права вимоги та переведення боргу за кредитним договором до відповідних фізичних чи юридичних осіб. Крім того, судами встановлено, що пунктом 6.11 укладеного між сторонами Договору іпотеки від 23 вересня 2008 року визначено, що іпотекодавець у випадку неналежного виконання ним своїх зобов'язань надає іпотекодержателю право використовувати банківську таємницю, що стосується виконання зобов'язань за цим договором.

Такі висновки судів відповідають нормам матеріального і процесуального закону, а також встановленим обставинам справи[64].

Суд погодився з висновками судів першої та апеляційної інстанцій та відмовив у задоволенні скарги. У наведеному уривку суд спершу згадує про підставу укладення та виконання договору. Згодом він погоджується з висновками судів, що особа надала згоду на обробку даних, уклавши договір.

Проте для укладення і виконання правочину закон не вимагає згоди. Сама воля до правочину і його наслідків породжує погодження суб’єктом обробки персональних даних. Тому додатковий пункт у договорі про згоду на обробку даних не є необхідним. Проте його вживають, щоби застрахувати себе від потенційних скарг і звернень.

Я вважаю таку практику такою, що вводить в оману щодо підстави обробки даних. В осіб виникає відчуття, що вони надали згоду, а відповідно й мають право її відкликати й обробка даних припиниться. Проте на практиці їх заяви про відкликання згоди, навіть у випадку їх погодження, не призведуть до припинення обробки, адже почне діяти інша підстава для обробки персональних даних.

[64] Рішення Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ від 26 жовтня 2016 року у справі 473/2644/15-ц. URL: http://www.reyestr.court.gov.ua/Review/62754765.

Згода вважається універсальною підставою, проте варто її використовувати, як останній захід. І дійсно, усі інші підстави мають чіткіше обмеження мети використання даних, тому такий підхід певним чином захищає дані особи. Якщо використати підставу виконання обов'язку володільцем даних, то він оброблятиме дані лише в межах мети виконання цього обов'язку. Проте, якщо застосувати підставу згоди, то може бути розширена потенційна обробка даних. Отже, дані будуть підлягати вужчій обробці при використанні інших підстав, ніж згода.

Проаналізувавши усі підстави для обробки даних, можна зробити висновок, що є загальні підстави та підстави для обробки чутливих даних. До того ж, ці підстави можна умовно поділити на згоду та інші законні підстави для обробки даних. Цей поділ знаходить вираження в законодавстві України та ЄС.

До того ж, згода є особливою підставою для обробки персональних даних. Згоду потрібно відрізняти від інших підстав, для того, щоб особа усвідомлювала свої права, якщо обробка здійснюється не на підставі згоди. Особливо проблемним є розмежування згоди та договору, проте важливо пам'ятати, що згоду суб'єкт даних може відкликати, на відміну від інших підстав.

1.3. Поняття згоди на обробку персональних даних як однієї із підстав для обробки персональних даних.

У попередньому підрозділі встановлено, що згода вирізняється серед усіх підстав для обробки персональних даних. У чому ж полягають її особливості та чому так багато є обговорень саме про підставу згоди? Розпочнемо з формального аналізу поняття згоди.

Для того, щоби провести аналіз, потрібно визначити поняття і встановити, що ми під ним розуміємо. Хоча згода і є загальновживаним словом, тим не менш у сфері обробки персональних даних вона має свою характеристику й необхідні елементи.

Доцільно розглядати наявне законодавче положення, що визначає поняття згоди, закріплене в статті 2 Закону України «Про захист персональних

даних», зокрема: “Згода суб’єкта персональних даних – добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене в письмовій формі або у формі, що дає змогу зробити висновок про надання згоди”[65].

Отже, можна виокремити наступні ознаки згоди: а) волевиявлення щодо надання дозволу на обробку персональних даних; б) добровільність; в) поінформованість; г) відповідна форма; ґ) мета обробки. Для обробки чутливих даних згода має виконувати також вимогу однозначності, тобто, однозначність є додатковою ознакою згоди.

Для того, щоби проаналізувати згоду на обробку персональних даних, важливо з’ясувати поняття персональних даних та їх обробки. Персональними даними, відповідно за Закону України Про захист персональних даних, є “відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована”[66]. Закон або сама особа можуть віднести персональні дані до конфіденційної інформації. Конституційний Суд України вважає, що перелік даних про особу, які визнаються як конфіденційна інформація, не є вичерпним[67].

Законодавче визначення обробки персональних даних – “будь-яка дія або сукупність дій, таких, як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання й поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем”[68].

Тобто, згода дається на вчинення необмеженого кола дій щодо персональних даних особи. Отже, волевиявлення щодо надання дозволу на

[65] Про захист персональних даних: Закон від 01.06.2010 № 2297-VI, ст. 2.
[66] Про захист персональних даних: Закон від 01.06.2010 № 2297-VI, ст. 2.
[67] Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20.01.2012 № 2-рп/2012.
[68] Про захист персональних даних: Закон від 01.06.2010 № 2297-VI, ст. 2.

обробку персональних даних полягає в дозволі на вчинення необмеженого кола дій щодо персональних даних особи.

Інші ознаки (вимоги) до згоди, а саме добровільність, поінформованість, відповідна форма, мета обробки, а також однозначність будуть проаналізовані докладніше в наступному розділі. Згадані ознаки можна розділити на змістовні та формальні. Так, добровільність, мета обробки та поінформованість будуть змістовними ознаками, тоді, як форма та однозначність – формальними.

Європейське законодавство вводить дещо інше розуміння поняття згоди. Відповідно до нового Загального регламенту про захист даних (ЄС) 2016/679 (GDPR) "згода суб'єкта даних означає будь-яке вільно надане, конкретне, поінформоване та однозначне зазначення бажань суб'єкта даних, яким він або вона, шляхом оформлення заяви чи проявом чітких ствердних дій, підтверджує згоду на опрацювання своїх персональних даних"[69]. У порівнянні з українським визначенням додаються вимоги щодо конкретності та однозначності для всіх видів персональних даних, а не лише для чутливих даних.

Чому ж серед підстав виділяють згоду? Фактично, втручання в приватність особи не допускається, за певними визначеними законом випадками. Проте надання згоди підтверджує той факт, що право на приватність не є порушеним, адже особа сама визначає спосіб і межі реалізації свого права. І якщо вона погоджується на його обмеження, то не можна говорити, що її право порушили. До того ж, підстава згоди дозволяє в будь-який момент відкликати її, що зупинить подальшу обробку даних. Саме тому до згоди стоять підвищені вимоги, щоб особи чітко усвідомлювали на що вони погоджуються.

У закордонній літературі згода також виділяється у порівнянні з іншими законними підставами. Зокрема, як зазначає Й. Карен про значення згоди на обробку персональних даних: "Наголос на згоді природньо випливає з особливого значення індивідуального вибору. Мої самостійні вибори просочені

[69] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних).

моральним та політичним значенням просто тому, що вони є моїми, а в ліберальних суспільствах існує презумпція, що вибори особи гідні поваги просто завдяки тому, що вони є її власними, якими б безглуздими чи нерозумними вони б не були"[70].

Отже, згода виділяється тим, що вона є виявленням власних поглядів особи на втручання у її приватність. Враховується думка особи щодо втручання у її право.

Утворюється ціла система захисту приватності, яка бере за основу згоду. Науковець у сфері приватності, Даніель Солове, вводить поняття privacy self-management. Відповідно до цього підходу, людям надається набір прав із контролю над їх особистими даними, завдяки чому люди самі вирішують, як оцінювати втрати та переваги збирання, використання чи розкриття інформації про них[71]. Цей підхід "знаходить прихисток у згоді та робить фокус на тому, на які дії щодо даних особа надала згоду"[72].

Робоча група 29 (Article 29 Working Party) також трактує згоду, як пов'язану з концепцією інформаційного самовизначення. Автономія суб'єкта даних є одночасно умовою й наслідком згоди: вона дає суб'єкту даних вплив на обробку даних[73]. Тому, за допомогою згоди суб'єкт даних може визначати, які саме дії він дозволяє вчиняти стосовно своїх персональних даних.

З цього випливає визначальна роль згоди. У своїх працях дослідник приватності Р. Браунсворд відокремлює основну (але не виняткову) функцію згоди – легітимізувати дію, яка в іншому випадку є порушенням прав. Відповідно до цього, одержувач згоди не завдає нічого поганого надавачу згоди[74].

З огляду на вимогу добровільності та інформованості згоди, дійсно можна стверджувати, що факт надання згоди слугує підставою виправдання

[70] Yeung, Karen, '"Hypernudge": Big Data as a Mode of Regulation by Design'', Information, Communication & Society, 1 (2016), 31. P.17.
[71] Solove D. J. Privacy self-management and the consent dilemma. P. 1880.
[72] Так само.
[73] Opinion 15/2011 on the definition of consent. Adopted on 13 July 2011. URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187en.pdf, p. 8-9.
[74] Brownsword R. (2009) Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality. In: Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S. (eds) Reinventing Data Protection?. Springer, Dordrecht. P. 89.

потенційних претензій суб’єкта даних. Це і відрізняє згоду від усіх інших підстав для обробки персональних даних.

Отже, згода є важливою правовою підставою обробки персональних даних особи. Вона містить певні обов’язкові елементи, без наявності яких згода не буде вважатися наданою. Також, згода є особливою підставою обробки персональних даних.

Унікальність згоди полягає в її пов’язаністю з волею особи. Згода виступає виправданням втручання в право на приватність та захист персональних даних. Оскільки згода іде саме від особи, у права якої відбудеться втручання, то вона повністю легітимізує втручання.

РОЗДІЛ ІІ
УМОВИ ДІЙСНОСТІ ЗГОДИ НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ

2.1. Вимоги щодо дійсності згоди на обробку персональних даних в Україні.

Для того, щоби здійснити правову характеристику згоди на обробку персональних даних, важливо проаналізувати вимоги щодо дійсності згоди на обробку персональних даних відповідно до українського законодавства.

Змістом згоди на обробку персональних даних є попередньо визначені елементи згоди або, як їх інакше називають, умови дійсності згоди чи складові елементи дійсної згоди[75]. Такі умови дійсності згоди можна ще найменувати вимогами до згоди або ознаками згоди – тобто, це ті характерні риси згоди, які власне й роблять її відповідною чинному законодавству. Умови дійсності згоди є тими мінімальними вимогами, що ставляться перед володільцями та розпорядниками персональних даних та покликані гарантувати права суб'єкта персональних даних у процесі обробки його даних.

Національне законодавство не містить детальних вимог щодо згоди. Зокрема, положення щодо умов дійсності згоди наявні в рамковому Законі України «Про захист персональних даних», Типовому порядку обробки персональних даних та Роз'ясненні Уповноваженого Верховної Ради України з прав людини до Типового порядку обробки персональних даних. Проаналізувавши ці положення можна встановити наступне.

У попередньому розділі, аналізуючи поняття згоди на обробку персональних даних, було визначено наступні вимоги до згоди:

- добровільність;
- поінформованість;

[75] Термін «складові елементи дійсної згоди» використовується у праці Посібник з Європейського права у сфері захисту персональних даних, виданій 2014 року Агенцією Європейського Союзу з питань основоположних прав та Рада Європи.
Посібник з європейського права у сфері захисту персональних даних. — К.: К.І.С., 2015. — 216 с. с. 64
Термін «умови дійсності згоди на обробку персональних даних» в українському науковому полі зустрічаються у статті «Умови дійсності згоди на обробку персональних даних» Юлії Бєлової.
Бєлова Ю. Умови дійсності згоди на обробку персональних даних / Ю. Бєлова // Підприємництво, господарство і право. — 2017. —№ 11. — Р. 14–18.

· відповідна форма.

Окремі науковці виділяють ще такі умови, як конкретність та однозначність. Так, Ю. Бєлова зазначає, що під конкретністю мається на увазі мета та конкретні цілі обробки персональних даних[76]. Про те, чи є доцільність виділяти окремо таку складову й називати її саме таким чином, розглянуто далі в цьому розділі. Однозначність обробки згадується в Законі України «Про захист персональних даних» стосовно обробки так званих чутливих персональних даних, тому її розглянуто окремо. Ці елементи були виділені відповідно до Регламенту про захист даних ЄС, проте вони наразі не мають підтвердження в законодавчому полі України.

Першою умовою дійсності, що зазначена в Законі України «Про захист персональних даних», є **добровільність** згоди. Відповідно до п. 5 Роз'яснення до Типового порядку обробки персональних даних, виданого Уповноваженим Верховної Ради України з прав людини, "згода на обробку персональних даних має бути свідомим рішенням особи, яке вона приймає добровільно, без примусу і погроз"[77]. Питання примусу досліджене в праці М. Бема, І. Городиського та інших.

> Щодо прямого примусу, то тут все більш-менш зрозуміло – згода не може бути добровільною, якщо надавалася під тиском із боку представників володільця чи інших осіб. Якщо мова йде про опосередкований примус, мається на увазі ситуація, коли отримання особою тієї чи іншої життєво важливої послуги, чи реалізація тих чи інших прав ставиться в залежність від надання нею згоди на обробку персональних даних. Зазвичай таке трапляється у випадках нерівності між суб'єктом та володільцем, зокрема залежності суб'єкта від володільця (зазвичай так і буває, оскільки суб'єкт звертається до володільця за тими чи іншими послугами).[78]

Також питання добровільності згоди можна розглянути через положення недійсності правочину в цивільному праві. Зокрема, згідно з ст. 231 Цивільного

[76] Бєлова Ю. Умови дійсності згоди на обробку персональних даних / Ю. Бєлова // Підприємництво, господарство і право. С. 15.
[77] Роз'яснення до Типового порядку обробки персональних даних: Уповноважений Верховної Ради з прав людини, 08.01.2014. База даних «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/n0001715-14.
[78] Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. С. 58-59.

кодексу України, “правочин, вчинений особою проти її справжньої волі внаслідок застосування до неї фізичного чи психічного тиску з боку другої сторони або з боку іншої особи, визнається судом недійсним”[79].

За аналогією, у разі застосування примусу чи погроз, що проявляються шляхом вчинення до особи фізичного чи психічного тиску, такі дії (у даному випадку згода) не відповідають закону. Це одразу викликає сумнів у дійсності згоди.

Тож можна стверджувати, що добровільність згоди передбачає прийняття особою рішення, що відповідає її внутрішній волі та не сформоване під тиском інших осіб, який може виражатися, зокрема, у формі примусу чи погроз.

Так звані “договори про приєднання”[80] в цій сфері, на думку Кохановської О., можуть спричинити багато зловживань. Вона визначає небезпеки умови добровільності згоди, якщо така згода не передбачає для суб’єкта персональних даних можливості вносити пропозиції чи зміни в сам текст згоди.

Проте переважно згода на обробку персональних даних виступає односторонньою пропозицією з боку володільця персональних даних. Зокрема це проглядається у сфері електронних комунікацій. І переважно особа не має впливу на зміст згоди, і законодавство не встановлює конкретних вимог, що вирішили б таку проблему.

Дуже часто добровільність згоди порушується, коли вимагають згоду на обробку персональних даних, а насправді обробка має здійснюватися на іншій підставі. Уповноважений Верховної Ради з прав людини у своїй щорічній доповіді за 2017 рік вказала, що стосовно згоди продовжується проблема з отримання згоди на обробку персональних даних у випадках, коли згідно із законом така згода не вимагається[81].

---

[79] Цивільний кодекс України: Закон від 16.01.2003 № 435-IV. База даних «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/435-15.

[80] Кохановська О.В. До питання про захист персональних даних в Україні // Вісник Верховного Суду України. - 2011. - № 6. - С. 28-33. URL: http://nbuv.gov.ua/UJRN/vvsu_2011_6_8.

[81] Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання прав і свобод людини і громадянина в Україні за 2017 рік. URL: www.ombudsman.gov.ua/files/Dopovidi/Report-2018-1.pdf, с. 486.

Наявна значна кількість судової практики з цієї проблеми. Наприклад, у рішенні Луцького міськрайонного суду Волинської області від 07 лютого 2018 року в справі № 161/18512/17 особа звернулась із вимогою зобов’язати Управління соціального захисту населення надати їй субсидії. Управління відмовило, мотивуючи це тим, що особа не надала згоду на обробку своїх персональних даних.

Суд встановив, що в даному випадку обробка має здійснюватися на підставі дозволу на обробку персональних даних, наданого володільцю персональних даних відповідно до закону виключно для здійснення його повноважень. Тобто окремої згоди суб’єкта даних не потрібно. Суд наступним чином мотивував своє рішення:

> …Отримання від суб'єктів персональних даних письмової згоди на обробку їх персональних даних у сфері призначення субсидії не є обов'язковим, оскільки дозвіл на обробку їх персональних даних наданий законом виключно для здійснення його повноважень у сфері їх призначення.(…)
>
> Будь-які дії володільця бази персональних даних, що виходять за межі дозволу, наданого йому відповідно до закону виключно для здійснення його повноважень, повинні здійснюватись за згодою суб'єкта персональних даних. (…)
>
> Володілець бази персональних даних, який здійснює їх обробку, на підставі проведеного аналізу законодавства, відповідно до якого здійснюються його повноваження щодо обробки персональних даних в сфері призначення субсидій, самостійно визначає підстави виникнення права на використання персональних даних фізичних осіб, які звертаються за їх призначенням[82].

Суд правильно витлумачив закон і встановив належну підставу для обробки даних. Водночас, особа звільнилася від непотрібного розголошення персональних даних.

Інший поширений випадок неправильного трактування підстави для обробки персональних даних є у сфері відносин із надання освітніх послуг. Одним із прикладів є рішення Вінницького міського суду Вінницької області від 03 червня 2014 року в справі № 127/7229/14-ц.

[82] Рішення Луцького міськрайонного суду Волинської області від 07 лютого 2018 року у справі № 161/18512/17. URL: http://www.reyestr.court.gov.ua/Review/72248664.

Згідно зі встановленими судом обставинами, особі відмовили у видачі диплому посилаючись на відсутність згоди на обробку персональних даних. Проте, відповідно до ст. 22 Закону України «Про вищу освіту», навчальний заклад може обробляти дані студентів, тобто існує підстава, встановлена законом. Суд мотивував своє рішення наступним чином:

> Вищий навчальний заклад згідно чинного законодавства України має повноваження на збір та обробку персональних даних про студентів без обов'язкового отримання згоди на обробку персональних даних.
>
> Отже, відповідач має право збирати та обробляти персональні дані про позивача і без його згоди, отримання такої згоди не є обов'язковою[83].

Ще один приклад у сфері надання послуг комунальним підприємством є у рішенні Жовтневого районного суду м. Харкова від 26 липня 2013 року у справі № 639/4355/13-ц. Позивач просив знищити свої персональні дані, що оброблялися комунальним підприємством, оскільки він не надавав згоду на їх обробку. Суд встановив наступне.

> Враховуючи той факт, що відповідно до ст. 11 Закону України «Про захист персональних даних»: «підставами виникнення права на використання персональних даних є…дозвіл на обробку персональних даних, наданих володільцю бази персональних даних відповідно до закону виключно для здійснення його повноважень», а ведення обліку власників, співвласників, наймачів чи орендарів, які проживають (розташовані) в житлових (нежитлових) приміщеннях житлового будинку є обов'язком, а не правом відповідача, згода на обробку персональних даних власників або наймачів житлових приміщень не є обов'язковою[84].

У такий спосіб суд розмежував згоду як підставу для обробки персональних даних та підставу, передбачену п. 2 ч. 1 ст. 11 Закону України «Про захист персональних даних».

Таких прикладів є багато, що свідчить про низьку поінформованість володільців персональних даних про принципи захисту даних, а зокрема,

---

[83] Рішення Вінницького міського суду Вінницької області від 03 червня 2014 року у справі № 127/7229/14-ц. URL: http://www.reyestr.court.gov.ua/Review/39125979.

[84] Рішення Жовтневого районного суду м. Харкова від 26 липня 2013 року у справі № 639/4355/13-ц. URL: http://www.reyestr.court.gov.ua/Review/34565599.

законність обробки. Плутанина між підставами для обробки даних призводить до порушення добровільності згоди в таких ситуаціях. Окрім справ, що дійшли до суду, ці ж володільці даних раніше вимагали надати згоду на обробку персональних даних у інших осіб, а, можливо, і продовжують таку практику. Це нівелює вимогу добровільності згоди та руйнує суспільне переконання, що згода надається без примусу.

Умова інформованості згоди встановлена в законодавчому визначенні згоди. Під **інформованою** згодою на обробку персональних даних, відповідно до п. 2 Роз'яснення до Типового порядку обробки персональних даних, варто розуміти "добровільне, компетентне прийняття особою рішення про обробку її персональних даних, яке ґрунтується на одержанні нею повної, об'єктивної і всебічної інформації щодо майбутньої обробки персональних даних"[85].

Як видається, перша частину даного роз'яснення, а саме слова "добровільне прийняття особою рішення"[86] не зовсім доцільна, адже вона стосується аспекту добровільності згоди, а не інформованості. Уже сама вказівка на добровільність і факт прийняття особою рішення стосуються розуміння волевиявлення особи, а не її обізнаності щодо обробки даних. Друга частина визначення інформованої згоди вірно вказує, що таке рішення має ґрунтуватися на отриманні суб'єктом персональних даних належної інформації про майбутню обробку його чи її даних. Така інформація характеризується повнотою, об'єктивністю і всебічністю. Ці ознаки не є детально описані в законотворчості чи судовій практиці, тому про їх зміст можна робити лише суб'єктивні висновки.

Щодо повноти, зокрема, п. 2 Роз'яснення до Типового порядку обробки персональних даних передбачає перелік інформації, з якою особо повинна ознайомитись перед тим, як приймати рішення про надання згоди на обробку її даних:

[85] Роз'яснення до Типового порядку обробки персональних даних: Уповноважений Верховної Ради з прав людини, 08.01.2014. База даних «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/n0001715-14.
[86] Там само.

Для того, щоб зробити свідомий вибір - давати чи не давати згоду на обробку персональних даних - особа до надання згоди повинна мати відповіді на такі питання:

- Хто оброблятиме її персональні дані? (назва володільця персональних даних, його адреса, контактні телефони тощо)
- З якою метою оброблятимуться персональні дані? (Мета має бути сформульована чітко та зрозуміло)
- Які персональні дані будуть оброблятися? (Конкретний вичерпний перелік персональних даних особи, який планується обробляти)
- Які дії з персональними даними передбачатиме їх обробка? (збір, зберігання, передача, оприлюднення, знеособлення тощо)
- Хто є розпорядником персональних даних? Які права і повноваження розпорядника щодо обробки персональних даних?
- Кому можуть бути передані персональні дані? З якою метою? На яких підставах?
- Скільки часу персональні дані будуть зберігатися у володільця?
- На яких умовах особа може відкликати згоду на обробку персональних даних та які наслідки такої дії?
- Інші права, визначені статтею 8 Закону «Про захист персональних даних»[87].

Зазначена інформація повинна надаватися володільцем у повному обсязі, в простій та зрозумілій формі до надання суб'єктом персональних даних згоди на обробку своїх персональних даних.

Також питання інформації є витлумачене в Роз’ясненні Міністерства юстиції України про Деякі питання практичного застосування Закону України «Про захист персональних даних»:

Згідно з вимогами Закону згода суб'єкта персональних даних на обробку персональних даних повинна містити інформацію щодо:

- мети, яка визначається володільцем бази персональних даних в залежності від виду його діяльності, при здійсненні якої виникає необхідність у обробці персональних даних у базах персональних даних, конкретних цілей обробки персональних даних, для досягнення яких володілець бази персональних даних обробляє персональні дані у цій базі (стаття 2 Закону);
- обсягу персональних даних, а саме чіткого переліку персональних даних фізичної особи, які можуть обробляються володільцем бази персональних даних у цій базі (стаття 6 Закону);
- порядку використання персональних даних, який передбачає дії володільця бази щодо обробки цих даних, в тому числі використання персональних даних працівниками володільця бази персональних даних, відповідно до їхніх професійних чи службових або трудових обов'язків, дії щодо їх захисту, а також дії щодо надання часткового або повного права обробки персональних даних іншим суб'єктам відносин, пов'язаних із персональними даними (стаття 10 Закону);

[87] Роз'яснення до Типового порядку обробки персональних даних: Уповноважений Верховної Ради з прав людини, 08.01.2014.

- порядку поширення персональних даних, який передбачає дії володільця бази персональних даних щодо передачі відомостей про фізичну особу з бази персональних даних (стаття 14 Закону);

- порядку доступу до персональних даних третіх осіб, який визначає дії володільця бази персональних даних у разі отримання запиту від третьої особи щодо доступу до персональних даних, у тому числі порядок доступу суб'єкта персональних даних до відомостей про себе (стаття 16 Закону)[88].

Загалом перелік, визначений Уповноваженим Верховної Ради з прав людини є більш деталізованим і ширшим, хоча перелік Міністерства юстиції й підкріплений посиланнями на конкретні статті закону, що передбачають, чому така інформація має бути подана особі перед прийняттям нею рішення про згоду на обробку персональних даних.

Цікаво відмітити, що серед зазначеної інформації вказується **мета обробки даних.** Враховуючи те, що мета безпосередньо зазначена у визначенні згоди на обробку персональних даних, варто на неї звернути окрему увагу.

Зокрема, у ч. 1 ст. 6 Закону України «Про захист персональних даних» вказано, що “у разі зміни визначеної мети обробки персональних даних на нову мету, яка є несумісною з попередньою, для подальшої обробки даних володілець персональних даних повинен отримати згоду суб’єкта персональних даних на обробку його даних відповідно до зміненої мети, якщо інше не передбачено законом”[89].

Також, принцип мінімізації даних пов’язаний із метою. Відповідно до ч. 3 ст. 6 Закону України «Про захист персональних даних», “склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними щодо визначеної мети їх обробки”[90].

Конкретизація мети є одним з принципів обробки даних. Вона знаходить свій вираз, зокрема, у вимозі інформованості згоди. А необхідність окремої згоди, якщо змінилася мета обробки, є дуже важливою. Отже, для мети обробки

[88] Деякі питання практичного застосування Закону України "Про захист персональних даних": Роз’яснення Міністерства юстиції України від 21.12.2011. База даних «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/n0076323-11.
[89] Про захист персональних даних: Закон від 01.06.2010 № 2297-VI.
[90] Про захист персональних даних: Закон від 01.06.2010 № 2297-VI.

характерні такі риси, як конкретизованість, незмінність, співмірність з обсягом персональних даних, що обробляються.

Наступною вимогою до дійсної згоди є належна **форма**. З аналізу законодавчого визначення згоди на обробку персональних даних згодою є волевиявлення особи, висловлене в письмовій формі або у формі, що дає змогу зробити висновок про надання згоди. Ключовою тут є частина, що вказує на можливість підтвердження надання особою згоди на обробку її даних, тобто, наявності належних доказів, що згода була надана.

> Зазвичай володілець повинен отримати від суб'єкта персональних даних згоду на обробку його персональних даних у письмовому вигляді. Допускається будь-яка інша форма надання згоди, однак володілець повинен мати змогу підтвердити наявність згоди впродовж всього часу здійснення обробки персональних даних.(…) Інше розуміння є недопустимим, оскільки передбачатиме існування ситуацій, коли персональні дані оброблятимуться начебто на підставі згоди, яка нічим не підтверджується[91].

Частково ця вимога збігається з умовою однозначності згоди, наведеною в праці Ю. Бєлової. Умови дійсності згоди суб'єкта персональних даних диктують вимоги до її об'єктивованої форми. У першій редакції відповідного положення Закону України «Про захист персональних даних» вимагалось, щоби волевиявлення фізичної особи щодо надання дозволу на обробку її персональних даних було документоване, зокрема письмове.

У подальшому, внаслідок неодноразових змін, ця вимога була значно спрощена. Тепер закон встановлює фактично єдину вимогу щодо форми згоди суб'єкта персональних даних, а саме: така форма повинна давати змогу зробити висновок про надання згоди[92] (абзац четвертий ч. 1 ст. 2 Закону України «Про захист персональних даних»).

Законом України "Про захист персональних даних" конкретно не визначено форму надання згоди на обробку персональних даних. Так, згода

[91] Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. С. 60.
[92] Про захист персональних даних: Закон від 01.06.2010 № 2297-VI.

суб’єкта персональних даних може бути вчинена в письмовій формі, як правило, у вигляді окремого документа (згода на обробку персональних даних).

“Також згода суб’єкта персональних даних може бути надана шляхом конклюдентних дій, тобто якщо його поведінка засвідчує волю на обробку персональних даних, зокрема, шляхом проставлення відмітки про надання дозволу на обробку своїх персональних даних під час реєстрації в інформаційно-телекомунікаційній системі суб’єкта електронної комерції. ”[93]

“Щодо усної форми згоди, то фактично вона не заборонена, однак навряд чи усна форма зможе надати володільцю змогу підтвердити наявність згоди впродовж усього часу здійснення обробки персональних даних”[94]. Зокрема, у володільця даних виникнуть проблеми з підтвердженням самого факту надання згоди, відповідності згоди вимогам дійсності, належної інформованості суб’єкта даних. “В будь-якому випадку володілець, отримуючи таку згоду, повинен мати можливість в подальшому надати (на вимогу особи/суду/Уповноваженого) переконливі докази того, що особа дійсно добровільно її надала, а також що перед цим їй було надано вказану вище інформацію”[95].

Отже, належна форма також може вказувати на дотримання вимоги інформативності згоди. Оскільки перед наданням згоди володілець даних зобов’язаний проінформувати особу про деталі майбутньої обробки персональних даних, то в самому тексті згоди може міститися вказівка на ознайомлення особи з вказаною інформацією. Очевидно, що у випадку надання згоди в усній формі або у формі конклюдентних дій важче або й узагалі неможливо буде довести дотримання вимоги інформативності згоди.

Крім того, текст згоди може безпосередньо містити дану інформацію, як елемент тексту, або ж посилання на те, де цю інформацію можна отримати. Тим не менш, перерахування інформації в тексті згоди не гарантує належного ознайомлення з нею особою, яка вирішує питання про надання згоди на обробку

[93] Бєлова Ю. Умови дійсності згоди на обробку персональних даних. С. 16.
[94] Там само.
[95] Роз'яснення до Типового порядку обробки персональних даних: Уповноважений Верховної Ради з прав людини, 08.01.2014. База даних «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/n0001715-14, п. 11.

персональних даних, як і не гарантує, що ця інформація буде доступною і зрозумілою. Хоча юридично й будуть дотримані вимоги, проте фактично особа може надати згоду, не читаючи умов. Ця проблема породжує безліч жартів на тему беззмістовності проставлення відмітки про надання дозволу на обробку своїх персональних даних та буде проаналізована в наступному розділі.

Однозначність згоди є додатковою умовою дійсності згоди в певних випадках. Зокрема, однозначність згоди вимагається для обробки особливих категорій даних, так званих чутливих даних. Мається на увазі, що "надання згоди має бути таким, що не викликає жодних сумнівів у її наданні"[96].

Ю. Бєлова зазначає, що однозначна згода повинна бути "явно вираженою, зрозумілою та безсумнівною. З цієї ж причини згода повинна, очевидно, походити від конкретного суб'єкта персональних даних, при цьому не залишаючи сумнівів щодо його дозволу на обробку персональних даних"[97].

Органи державної влади не надають тлумачення цієї вимоги. Фактично, можна її трактувати, як таку, що створює обов'язок володільця даних мати недвозначне підтвердження факту надання згоди. А відсутність правового роз'яснення цієї вимоги ставить під ризик найбільш захищені категорії персональних даних.

Важливо зазначити, що й до інших, нечутливих категорій персональних даних, важливо застосовувати вимогу однозначності, адже в разі наявності сумнівів щодо факту надання згоди, обробка персональних даних є неправомірною.

Як видається, однозначність згоди можна трактувати в контексті безсумнівності згоди щодо обробки саме чутливих даних. Іншими словами, особа має чітке усвідомлення того, що надається згода на обробку саме чутливих персональних даних, а не просто персональних даних. Хоча й на законодавчому рівні не встановлено способів досягнення однозначності, можна навести кілька

[96] Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. С. 70.
[97] Бєлова Ю. Умови дійсності згоди на обробку персональних даних / Ю. Бєлова // Підприємництво, господарство і право. С. 15.

прикладів, як от маркування спеціальним шрифтом, кольором чутливих даних у тексті згоди, виділення цієї інформації в окремому місці тощо.

Отже, українське законодавство встановлює наступні вимоги до згоди: добровільність, інформованість, відповідна форма та однозначність. Окремим важливим аспектом згоди є мета обробки даних. Ці вимоги частково витлумачені в підзаконних актах. Судової практики, що визначала б конкретні вимоги до згоди, наразі немає, проте є практика, що опосередковано дає змогу зробити висновок про непряме примушування до надання згоди, що порушує вимогу добровільності згоди.

Детальний перелік інформації, що повинна надаватися суб'єкту персональних даних при наданні згоди, встановлений підзаконними актами. Основна вимога до форми згоди полягає в тому, щоби володілець персональних даних зумів підтвердити факт її надання суб'єктом даних. Однозначна згода має не викликати сумнівів у її наданні. Наступним постає питання відповідності цих положень міжнародним стандартам захисту персональних даних.

2.2. Вимоги щодо дійсності згоди на обробку персональних даних в інших юрисдикціях.

З огляду на напрям євроінтеграції України та високий рівень розвитку системи захисту персональних даних у юрисдикції Європейського Союзу, найбільший акцент у цьому підрозділі зроблено саме на європейському правовому регулюванні питання вимог щодо дійсності згоди на обробку персональних даних.

Згодом проаналізовано й інші юрисдикції, що мають високий рівень захисту персональних даних. Такий аналіз видається корисним із погляду порівняння із національно-правовим регулюванням та визначенням напрямків удосконалення законодавства України у цій сфері.

Як уже було зазначено вище, Загальний регламент про захист даних (ЄС) 2016/679 (GDPR) є основним правовим актом в ЄС, що регламентує захист персональних даних. Відповідно до визначення згоди в п. 14 ст. 4 Загального

регламенту про захист даних (ЄС) 2016/679 (GDPR), елементами згоди є добровільність, конкретність, поінформованість та однозначність. Важливим є розгляд цих елементів з точки зору тлумачення її компетентними органами ЄС. Ключовим інструментом є Напрямні щодо згоди згідно з Регламентом (ЄС) 2016/679, прийняті Робочою групою захисту даних, що діє згідно зі статтею 29 (Article 29 Working Party).

Першою ознакою є **добровільність** надання згоди. "Згоду не можна вважати такою, що було добровільно надано, якщо суб'єкт даних не здійснює справжнього чи добровільного вибору, або неспроможний відмовити в наданні згоди або її відкликанні, не заподіюючи водночас шкоди"[98].

Відповідно до напрацювань Робочої групи захисту даних, що діє згідно зі статтею 29, при визначенні добровільності надання згоди необхідно враховувати наступне.

Щоби забезпечити, що згоду було надано добровільно, вона не повинна передбачати необхідність застосування дійсних законних підстав опрацювання персональних даних у спеціальному випадку, коли існує помітний дисбаланс між суб'єктом даних і контролером, зокрема коли контролер є органом публічної влади і, тому, малоймовірно, що згоду було надано добровільно за всіх обставин такої спеціальної ситуації.

"Презумпція ненадання добровільної згоди виникає у разі відсутності окремого дозволу на здійснення різних операцій опрацювання персональних даних, незважаючи на її відповідність окремому випадку, або, якщо виконання договору, в тому числі, надання послуги, залежить від надання згоди, незважаючи на те, що така згода не є обов'язковою для такого виконання"[99].

На думку Робочої групи захисту даних, для таких випадків можуть бути застосовані інші підстави для обробки даних, замість згоди. Зокрема, відповідно до пп. c, e ч. 1 ст. 6 Регламенту (ЄС) 2016/679 (GDPR): "опрацювання є

[98] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних), п. 42 преамбули.
[99] Там само, п. 43 преамбули.

необхідним для дотримання встановленого законом зобов'язання, яке поширюється на контролера; опрацювання є необхідним для виконання завдання в суспільних інтересах або здійснення офіційних повноважень, покладених на контролера"[100]. Також, дисбаланс сил присутній у відносинах між роботодавцем та працівником.

Згода може бути дійсною тільки в разі, якщо суб'єкт даних у змозі здійснювати реальний вибір і немає ніякого ризику обману, залякування, примусу або істотних негативних наслідків (наприклад, істотні додаткові витрати), якщо він / вона не згодні. Згода не буде вільною у випадках, коли є якийсь елемент примусу, тиску або нездатності здійснювати вільну волю[101].

"Здійснюючи оцінку того, чи є згода вільно наданою, необхідно максимально враховувати те, чи залежить, між іншим, виконання договору, у тому числі надання послуги, від згоди на опрацювання персональних даних, що не є необхідною для виконання такого договору"[102]. Це положення прагне забезпечити, щоби мета обробки персональних даних не була замаскована та не була пов'язана з наданням договору послуги, для якої ці персональні дані не є необхідними.

Водночас, GDPR гарантує, що обробка персональних даних, для яких вимагається згода, не може прямо або побічно стати зустрічним виконанням договору. Дві законні підстави для законної обробки персональних даних, тобто згоди та контракту, не можуть бути об'єднані та розмиті[103]. Якщо контролер намагається обробляти особисті дані, які насправді є необхідними для виконання договору, то згода не є належною законною підставою.

Послуга може передбачати кілька операцій обробки даних для декількох цілей. У таких випадках суб'єктам даних слід дати змогу вільно вибирати, яку

[100] Там само, пп. c, e ч. 1 ст. 6.
[101] Article 29 Working Party Guidelines on consent under Regulation 2016/679 (WP259 rev.01) Adopted on 28 November 2017, p. 7.
[102] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних), ч. 4 ст. 7
[103] Article 29 Working Party Guidelines on consent under Regulation 2016/679 (WP259 rev.01) Adopted on 28 November 2017, p. 8.

ціль вони приймуть, а не давати згоду на сукупність різних цілей обробки. Якщо контролер об'єднав декілька цілей для обробки та не намагався шукати окремої згоди для кожної мети, має місце брак волі. Цей ступінь деталізації тісно пов'язаний із необхідністю згоди бути конкретною. “Коли обробка даних виконується для досягнення кількох цілей, рішення щодо дотримання умов для дійсної згоди полягає в деталізації, тобто поділі цих цілей та отриманні згоди для кожної цілі”[104].

Контролер повинен продемонструвати, що можна відмовитися або відкликати свою згоду без збитків для суб’єкта. Зокрема, “контролер повинен довести, що відкликання згоди не призводить до будь-яких витрат для суб'єкта даних, і, таким чином, немає явного недоліку для тих, хто відкликає згоду”[105].

Цікавим є проаналізувати практику застосування вищеописаних правових положень. У перший ж день введення в дію Регламенту (ЄС) 2016/679 (GDPR), організація noyb подала чотири скарги до компетентних органів різних країн ЄС, що стосуються невідповідності згоди сервісів Google, Facebook, Instagram та WhatsApp вимогам Регламенту[106]. Вони всі містять схожі вимоги. Зокрема, основною проблемою визнають не добровільність згоди на обробку даних у вказаних сервісах.

В обґрунтуванні скарги на вимогу дати згоду при користуванні телефоном на системі Android (що належить Google) вказано:

“Суб'єкт даних, здається, не має ніякого іншого реального вибору, крім як погодитися з політикою конфіденційності та умовами встановленими контролером, з огляду на дисбаланс сил між ними. Не погодження може призвести до суттєвого негативного наслідку для суб'єкта даних. Отже, будь-яка згода отримано від суб'єкта даних є недійсною тільки на цій підставі”[107].

---

[104] Article 29 Working Party Guidelines on consent under Regulation 2016/679 (WP259 rev.01) Adopted on 28 November 2017, p. 10.
[105] Там само, с. 10.
[106] GDPR: noyb.eu filed four complaints over “forced consent” against Google, Instagram, WhatsApp and Facebook URL: https://noyb.eu/4complaints/.
[107] Complaint under article 77(1) GDPR on Google to CNIL (France) URL: https://noyb.eu/wp-content/uploads/2018/05/complaint-android.pdf.

Також вказується на аспект згоди, що особа або погоджується з умовами, або не може користуватися сервісом («take it or leave it»). Тобто, особа зазнає негативних наслідків. Дуже чітко встановлено порушення вимоги добровільності згоди[108].

Тобто, на підставі цих прикладів можна зробити висновок, про те, що добровільність тлумачиться у світлі свободи вибору щодо надання чи ненадання згоди.

Конкретність є ще однією вимогою. Для виконання умови конкретності, контролер повинен використовувати: уточнення цілей, як захист від злиття цілей, деталізація в запитах на згоду та чітке розмежування інформації, пов'язаної з отриманням згоди на обробку даних від інформації про інші питання. Щодо кожної іншої цілі контролер повинен отримати згоду особи, тому доцільно збирати згоду окремо щодо різних цілей обробки даних.

“Контролер, який шукає згоду для різних цілей, повинен надавати окремий вибір для кожної цілі, щоби дозволити користувачам надавати конкретну згоду для конкретних цілей. Також, контролери повинні надавати конкретну інформацію з кожною окремою згодою щодо даних, які обробляються для кожної цілі, щоби суб'єкти даних знали про вплив різних варіантів, які вони мають”[109]. “Це узгоджується з якістю наданої інформації про мету згоди. У цьому контексті відповідними будуть розумні очікування звичайного суб’єкта персональних даних”[110].

У скаргах організації noyb робиться послання на загальність згоди. Немає можливості визначати окремі цілі й давати згоду лише на них[111]. Це чудово видно на скарзі Google, оскільки компанія пропонує багато сервісів (YouTube, Chrome Browser, Google Services, Google Maps, Google Search, Google News, Gmail та інші), проте згода є загальною для всіх. Варто почекати на результати розгляду

[108] Так само.
[109] Article 29 Working Party Guidelines on consent under Regulation 2016/679 (WP259 rev.01) Adopted on 28 November 2017, p. 11-12.
[110] Посібник з європейського права у сфері захисту персональних даних, с. 64.
[111] GDPR: noyb.eu filed four complaints over “forced consent” against Google, Instagram, WhatsApp and Facebook URL: https://noyb.eu/4complaints/.

цих скарг, однак тлумачення конкретності згоди, як такої, що має надаватися на кожен вид послуги, товару окремо, а не узагальнено, видається слушною і доцільною.

Питання буде полягати в ступені конкретизації, тобто, наскільки дрібними мають бути послуги для того, щоби для них отримувалась окрема згода, що буде конкретною. Наприклад, чи потрібно мати окремі конкретизовані згоди для огляду товарів в інтернет-магазині, їх купівлі, підписки на новини та розіграші від інтернет-магазину.

Наступною розглянемо вимогу **інформованості** згоди. "Зазвичай, поінформована згода включає точний і легко зрозумілий опис суті справи, у зв'язку з якою необхідне надання згоди, а також виклад наслідків надання або ненадання згоди. Викладена інформація має бути зрозумілою тим, кому вона адресується. Те, чи є надана інформація достатньою, чи ні, має вирішуватися окремо в кожному випадку"[112].

Для того, щоб отримати інформовану згоду, необхідно повідомити суб'єкта даних про деякі елементи, які мають вирішальне значення для вибору. Тому Робоча група захисту даних 29 (Article 29 Working Party) вважає, що для отримання дійсної згоди необхідна, принаймні, така інформація: "особа контролера; мета кожної з операцій обробки, для яких згода потрібна; які типи даних збиратимуться та використовуватимуться; існування права відкликати свою згоду; інформація про використання даних для автоматичного прийняття рішень відповідно до статті 22 (2) (c), де це необхідно; про можливі ризики передачі даних через відсутність компетентного рішення та відповідних гарантій передачі даних"[113].

[112] Посібник з європейського права у сфері захисту персональних даних, с. 64.
[113] Article 29 Working Party Guidelines on consent under Regulation 2016/679 (WP259 rev.01) Adopted on 28 November 2017, p. 13.

Для того, щоби згода вважалася поінформованою, “суб’єкт даних повинен бути обізнаним принаймні про особу контролера та цілі опрацювання, для яких призначено використання персональних даних”[114].

Важливо, проаналізувати цю вимогу на практиці, зокрема досліджено рішення німецького суду з цього питання. Об’єднання німецьких організацій користувачів подало скаргу на Facebook, посилаючись на невідповідність вимогам дійсної згоди[115]. Суд у Берліні (das Landgericht Berlin) постановив, що Facebook залишає безліч налаштувань включеними за замовчуванням, не пропонуючи користувачам реальний вибір щодо того, як використовуватимуться їхні дані. Повідомляється, що “судді визначили п'ять різних налаштувань конфіденційності за замовчуванням незаконними, у тому числі обмін даними про місцезнаходження між співрозмовниками у чаті, а також доступність профілів для зовнішніх пошукових систем, що дозволяє будь-якому користувачеві інтернету натрапити на них”[116].

Налаштування конфіденційності не відповідали вимогам інформованої згоди. Параметри за замовчуванням не можуть розглядатися, як інформована згода, якщо користувач не має явного та активного сповіщення про параметри за замовчуванням в процедурі реєстрації. Facebook недостатньо забезпечив, щоб користувач знав про параметри за замовчуванням[117].

Також у ЄС встановлюється вимога **недвозначності** (unambiguity). З Регламенту (ЄС) 2016/679 (GDPR) ясно, що згода “вимагає заяви суб'єкта даних або чіткої ствердної дії, що означає, що вона завжди повинна бути надана за допомогою активного ходу або оголошення. Має бути очевидним, що суб'єкт

[114] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв’язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних), п. 42 преамбули.
[115] The Regional Court of Berlin judgment of 16 January 2018 (docket no. 16 O 341/15).
[116] Facebook не має вимагати справжні імена при реєстрації — суд Берліна. «Центр інформації про права людини». URL: https://humanrights.org.ua/material/facebook_ne_maje_vimagati_spravzhni_imena_pri_rejestraciji__sud_berlina_postanoviv_shho_.
[117]German court issues important judgment on consent and transparency in Facebook case. Technology Law Dispatch. URL: https://www.technologylawdispatch.com/2018/03/privacy-data-protection/german-court-issues-important-judgment-on-consent-and-transparency-in-facebook-case/.

даних погодився на окрему обробку даних"[118]. Це описує так званий метод opt-in згоди, на противагу opt-out. В opt-in згода не вважається наданою, якщо відмітка про надання згоди була попередньо проставленою. Особа має ствердною дією заявити про своє згоду. Метод opt-out передбачає, що персональні дані збиратимуть та використовуватимуть за замовчуванням, якщо особа не висловить заперечення проти обробки даних.

Проте є думка, що немає необхідності виділяти недвозначність, як окрему вимогу, оскільки вона вже закладена у вимозі добровільності. А ця додаткова вимога не дає справжньої цінності щодо тлумачення згоди[119]. Проте її можна зіставляти із вимогою щодо форми згоди в українському законодавстві. Тобто, недвозначність можна було би розуміти як можливість доказування факту отримання згоди.

Обробка чутливих даних згідно з Регламентом (ЄС) 2016/679 (GDPR) вимагає **явної** (explicit) згоди. Явна стосується способу, яким вона виражена суб'єктом даних. Особа має надати однозначне вираження згоди.

Очевидним способом це зробити є письмове підтвердження. Проте цим методом не обмежується. "Контролер повинен усунути будь-який сумнів та відсутність доказів про факт згоди у майбутньому"[120]. Тобто, в ЄС встановлено високий рівень вимог щодо явності згоди. До цієї вимоги встановлені підвищені стандарти, проте, враховуючи високі стандарти до загальної згоди на обробку персональних даних, немає чіткого її розмежування і тлумачення. Можливо, це питання має вирішуватися в кожному окремому випадку відповідно до обставин конкретної справи.

Такими є вимоги до дійсної згоди як підстави на обробку персональних даних. Одразу потрібно провести порівняльний аналіз відповідності українського правового регулювання стандартам Регламенту (ЄС) 2016/679

[118] Article 29 Working Party Guidelines on consent under Regulation 2016/679 (WP259 rev.01) Adopted on 28 November 2017.
[119] Kosta, E. (2011). Unravelling consent in European data protection legislation - a prospective study on consent in electronic communications. P. 199.
[120] Article 29 Working Party Guidelines on consent under Regulation 2016/679 (WP259 rev.01) Adopted on 28 November 2017, p. 18.

(GDPR). Для зручності порівняння вимог дійсності згоди в українському законодавстві та у ЄС варто розглянути детально кожну вимогу в табличному форматі.

Таблиця №1. Порівняльна характеристика умов дійсності згоди в Україні та ЄС

Україна	**ЄС**
Добровільність	
Свідоме рішення особи, яке вона приймає добровільно, без примусу й погроз.	Реальний вибір і відсутність ризику обману, залякування, примусу або істотних негативних наслідків. Врахування дисбалансу сил між сторонами.
Аналогічними є положення про відсутність примусу та обману, для забезпечення вільної згоди. В праві ЄС додатково вказується на потенційні негативні наслідки, що додатково убезпечує особу від непрямого примусу до згоди. Крім того, право ЄС наголошує на рівності сторін для забезпечення добровільності.	
Конкретність	
Мета обробки персональних даних повинна бути чіткою й законною.	Уточнення цілей, деталізація в запитах на згоду та чітке розмежування інформації, пов'язаної з отриманням згоди на обробку даних від інформації про інші питання.

Тут українське законодавство не містить відповідних положень щодо розмежування різних цілей обробки та відмежування згоди від інших положень договору. Відмежування згоди від інших договірних положень допомагає особі чітко побачити всю інформацію про згоду. Тому варто внести таке положення в національне регулювання.	
Інформованість	
Добровільне, компетентне прийняття особою рішення про обробку її персональних даних, яке ґрунтується на одержанні нею повної, об'єктивної і всебічної інформації щодо майбутньої обробки персональних даних.	Точний і легко зрозумілий опис суті справи, у зв’язку з якою необхідне надання згоди, а також виклад наслідків надання або ненадання згоди. Інформація має бути зрозумілою.
Українське законодавство містить вимоги щодо повноти і всебічності, тобто отримання суб’єктом даних усієї інформації. Право ЄС в інформативності зосереджується на точності та легкості сприйняття. Також у праві ЄС постає аспект зрозумілості інформації для особи, що вимагає простого пояснення.	
Форма/Недвозначність	
Волевиявлення особи, висловлене в письмовій формі або у формі, що дає змогу зробити висновок про надання згоди.	Згода вимагає заяви суб'єкта даних або чіткої ствердної дії, що означає, що вона завжди повинна бути надана за допомогою активного ходу або оголошення. Opt-in підхід до згоди.

Українське право встановлює основну вимогу – щоби можна було зробити висновок про надання згоди. Право ЄС детальніше і змістовніше підходить. Воно вимагає не лише підтвердження факту надання згоди, а й щоб згода була активною дією особи, а не пасивною чи мовчанням.	
Однозначність/Явність	
Явно виражена, зрозуміла та безсумнівна.	Особа має надати однозначне вираження згоди.
Обидві юрисдикції не містять конкретності щодо вимоги до обробки чутливих даних. Встановлено, що така згода має бути чітко й точно наданою, і щоб це можна було підтвердити.	

Можна зробити висновок, що для узгодження українського законодавства з європейським у сфері захисту персональних даних, в українське законодавство необхідно внести певні зміни. Проте існують змістовні паралелі між переліком і тлумаченням вимог до дійсної згоди в обох юрисдикціях. Це зумовлено фактом ґрунтування українського режиму захисту даних на Директиві 95/46 ЄС. Проте, це підґрунтя допоможе швидше імплементувати вимоги до згоди в ЄС до національного регулювання.

Персональні дані захищаються на належному рівні не лише в межах ЄС. Зокрема, для забезпечення належного захисту даних при передачі їх у треті країни, в ЄС є механізм визнання адекватного рівня захисту у певній державі, що гарантує безпеку при передачі даних у цю державу. Такими державами станом на час написання цієї роботи є Андорра, Аргентина, Канада (приватні особи), Фарерські острови, Гернсі, Ізраїль, Острів Мен, Джерсі, Нова Зеландія,

Швейцарія, Уругвай, США (в межах Privacy Shield framework)[121]. Розглянемо положення і вимоги до згоди в деяких із вище перелічених держав.

В Швейцарії діє Федеральний акт про захист даних від 1992 року. Відповідно до його положень, "порушення приватності є незаконним, за винятком якщо було отримано згоду особи, чиї права порушено, або є переважаючий публічний чи приватний інтерес чи відповідно до закону"[122].

Якщо для обробки персональних даних вимагається згода, то вона буде дійсною лише якщо буде надана добровільно на підставі достатньої інформації. До того ж, згода має бути однозначно наданою у випадку обробки чутливих даних або особистих профілів[123]. Тобто повторюються вимоги щодо добровільності та інформативності згоди, а також явності/однозначності при обробці чутливих даних. Водночас, згода є лише однією з законних підстав для обробки. Тобто, можна зробити висновок про відсутність якихось суттєво відмінних підходів у правовому регулюванні, у порівнянні з ЄС.

Ізраїльський Закон про приватність був прийнятий ще в 1981 році, проте щоб посилити гарантії та відповідати новим міжнародним вимогам у 2017 було прийняте Регулювання із Захисту Приватності (Privacy Protection (Data Security) Regulations). Відповідно до закону, "ніхто не може втручатися у приватність без згоди суб'єкта"[124].

У визначенні згоди наводяться вимоги інформованості та вираженості (expressed) або неявності (implied)[125]. Інформована згода передбачає отримання повної та належної інформації про обробку даних та вимагається завжди[126]. В різних ситуаціях вимагається надання вираженої (expressed) згоди. Прикладом

---

[121] Adequacy of the protection of personal data in non-EU countries. European Commission. URL: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

[122] Swiss Federal Act on Data Protection of 19 June 1992. URL: https://www.admin.ch/opc/en/classified-compilation/19920153/index.html, article 13.

[123] Swiss Federal Act on Data Protection of 19 June 1992 URL: https://www.admin.ch/opc/en/classified-compilation/19920153/index.html, article 4.

[124] Israel Protection of Privacy Law, 5741 – 1981, article 1, URL: https://www.gov.il/BlobFolder/legalinfo/legislation/en/ProtectionofPrivacyLaw57411981unofficialtranslatio.pdf.

[125] Israel Protection of Privacy Law, 5741 – 1981, article 3 URL: https://www.gov.il/BlobFolder/legalinfo/legislation/en/ProtectionofPrivacyLaw57411981unofficialtranslatio.pdf.

[126] Privacy Glossary URL: https://www.gov.il/he/Departments/Guides/glossary?chapterIndex=1.

неявної згоди може бути обробка даних відповідно до виконання обов'язку згідно з договором[127].

Хоча в цьому аспекті ізраїльський закон відрізняється від регулювання ЄС, він встановлює достатньо гарантій щодо захисту даних, щоб визнаватися таким, який гарантує адекватний рівень захисту.

У Канаді система захисту персональних ґрунтується на Акті про захист персональної інформації та електронні документи (The Personal Information Protection and Electronic Documents Act (PIPEDA)). Він поширює свою дію лише на приватні організації. За загальним правилом, "організація може збирати, використовувати чи розкривати персональну інформацію лише для цілей, які розумна людина вважатиме належними в обставинах"[128]. Одним із принципів вказано згоду.

"Знання та згода особи необхідні для збирання, використання чи розкриття особистої інформації, за винятком коли це недоречно"[129]. Були прийняти Напрямні для згоди, проте вони містять більше описової інформації, ніж уточнених вимог до згоди[130]. Там встановлено принципи, якими мають керуватись організації для отримання змістовної згоди.

Відповідно до самого Акту, "згода особи є дійсною, лише якщо можна розумно очікувати, що особа, на яку спрямована діяльність організації, зрозуміє природу, ціль та наслідки збирання, використання чи розкриття персональної інформації, на які вони дають згоду"[131]. Можна сказати, що ці норми є більш загального характеру й менш вимогливі до організацій, на які вони поширюють свою дію.

Крім державного рівня та ЄС, можна розглянути також один міжнародний документ із питань захисту даних. Конвенція Африканського Союзу про Кібер

---

[127] Там само.

[128] The Personal Information Protection and Electronic Documents Act (PIPEDA) 2000. URL: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html article 5(3).

[129] Там само, schedule 1, 4.3.

[130] Guidelines for obtaining meaningful consent, Canada, 2018. URL: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/.

[131] The Personal Information Protection and Electronic Documents Act (PIPEDA) 2000. URL: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html article 6.1.

Безпеку та Захист Персональних Даних (African Union Convention on Cyber Security and Personal Data Protection), прийнята у 2014 році та підписана одинадцятьма країнами й ратифікована трьома.

Відповідно до цієї Конвенції, "згода суб'єкта даних означає будь-який прояв вираженого, однозначного, добровільного, конкретного та інформованого бажання, яким особа чи її законний, судовий чи договірний представник приймає, що її особисті дані будуть піддані ручній чи електронній обробці"[132]. І за загальним правилом для обробки персональних даних вимагається згода, проте є винятки, як виконання юридичного обов'язку чи договору, захист важливих прав суб'єкта даних тощо. Цей акт встановлює ще більше вимог до згоди, ніж Загальний регламент про захист даних (ЄС) 2016/679 (GDPR).

Регулювання згоди відповідно до Регламенту (ЄС) 2016/679 (GDPR) є набагато конкретнішим та вимогливішим порівнюючи з українським регулюванням. Окрім добровільності, інформованості й однозначності висуваються додаткові вимоги конкретності, явності. Зазначення більшої кількості вимог, з одного боку, спричиняє до роздроблення первинних вимог. З іншого боку, чим більше вимог закріплено, тим більше володільці персональних даних звертатимуться до них і перевірятимуть їх дотримання.

Українське регулювання потребує вдосконалення, щоб відповідати адекватному рівню захисту відповідно до вимог ЄС. Водночас, країни, які визнані такими, що мають належний рівень захисту, не завжди відтворюють правове регулювання ЄС. Часто вони мають свої режими захисту даних, які, тим не менш, як видається, гарантують достатній захист персональних даних.

[132] African Union Convention on Cyber Security and Personal Data Protection 2014. URL: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

РОЗДІЛ ІІІ
НАПРЯМИ УДОСКОНАЛЕННЯ ЗГОДИ ЯК ПІДСТАВИ ДЛЯ ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ

3.1. Слабкі аспекти згоди як підстави для обробки персональних даних.

Для підприємств обирати згоду як підставу для обробки персональних даних, створює додаткові складнощі, якщо брати до уваги необхідність дотримання всіх вимог до згоди. Відтак, згода не є популярним вибором з-поміж усіх підстав для обробки персональних даних. Згідно з роз'ясненням щодо Регламенту (ЄС) 2016/679 (GDPR), виданим британським органом із безпеки даних Information Commissioner's Office "GDPR встановлює високий стандарт для згоди. Але вам часто не потрібна згода. Якщо згода надто складна, погляньте на інші законні підстави"[133]. Проте, окрім складності вимог, сама ідея згоди має слабкі сторони.

У першому розділі згода позиціонується, як панацея до всіх закидів на недосконаліть правового механізму захисту персональних даних. Якщо особа самостійно погоджує втручання у свої права, то, мовляв, які ще можуть бути аргументи проти згоди. Проте варто зауважити недосконаліть самої концепції згоди і її втілення на практиці. Згоду можна критикувати з різних аспектів. Зокрема з боку окремих вимог інформованості згоди, добровільності згоди чи власне в концепції згоди, як такої.

Інформованість, як умова дійсності згоди, видається абсолютно логічною та необхідною. Щоб згода вважалася чесно отриманою, особа має мати розуміння, де, ким і як її дані будуть використані. Проте на практиці цю вимогу важко, а то й подекуди неможливо задовільнити.

Проблема з інформуванням суб'єктів даних полягає в тому, що люди не читають політику конфіденційності. Якщо вони читають їх, вони не розуміють їх, і, навіть якщо вони їх читають та розуміють, у них часто не вистачає знань для

[133] Information Commisioner's Office, 'Lawful Basis for Processing Consent', 2018, p. 44.

розуміння того, що означає політика та які наслідки надання згоди. У випадку, коли люди читають політику, розуміють її та усвідомлюють її наслідки, рішення може бути деформоване різними психологічними чинниками.[134]

Науковці провели дослідження і встановили, що якби особа дослівно читала всі політики конфіденційності, на які вона в середньому дає згоду, це б зайняло 201 годину в рік[135]. Крім того, переважно особи не розуміють або неправильно трактують прочитані політики конфіденційності[136].

В одному експерименті люди підписували згоду на обробку даних, що містила пункт про "безповоротний дозвіл вимагати безсмертну душу"[137] суб'єкта даних. Незважаючи на те, що власник сайту дав змогу відмовитися від цього пункту, лише дванадцять відсотків користувачів скористалися такою відмовою[138]. Це демонструє, що дуже малий відсоток усе таки заглядає в політики конфіденційності.

Вказана проблема певним чином взята до уваги при розробці Регламенту (ЄС) 2016/679 (GDPR). Зокрема в тому, що "інформація повинна бути в зрозумілій та доступній формі, з використанням чітких і простих формулювань"[139]. Проте, чи призведе таке положення до того, що люди звертатимуть увагу на умови політик конфіденційності, наразі рано стверджувати. В українському регулюванні також наявна вимога повної, об'єктивної та всебічної інформації. Та чи повнота та всебічність допомагають надавати дійсно інформовану згоду?

У дослідженні користувачів інтернету щодо оцінки приватності, менше третини опитуваних ствердили, що вони знають, що для покращення своєї

---

[134] Jakub Misek, 'Consent to Personal Data Processing - The Panacea or the Dead End', Masaryk University Journal of Law and Technology, 8.1 (2014), 69–83. P. 76.
[135] McDonald, A. M., & Cranor, L.F. (2008). The Cost of Reading Privacy Policies. A Journal of Law and Policy for the Information Society. 4, 541.
[136] Reidenberg, Joel & D. Breaux, Travis & Cranor, Lorrie & French, Brian & Grannis, Amanda & T. Graves, James & Liu, Fei & M. McDonald, Aleecia & B. Norton, Thomas & Ramanath, Rohan & Cameron Russell, N & Sadeh, Norman & Schaub, Florian. (2014). Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding.
[137] 7,500 Online Shoppers Unknowingly Sold Their Souls. FoxNews. URL: https://www.foxnews.com/tech/7500-online-shoppers-unknowingly-sold-their-souls
[138]. Там само.
[139] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних), ст. 7(2).

безпеки можуть прочитати політику конфіденційності. Тим не менш, лише дванадцять відсотків дійсно прочитали її[140]. Тому стурбованість людей не завжди призводить до активних дій щодо забезпечення захисту своїх даних.

З цього випливає парадокс приватності (так званий privacy paradox). У той час, коли багато людей заявляють, що дуже турбуються про свою приватність, вони добровільно розкривають значну кількість інформації про себе. "Є великий розрив між заявленою стурбованістю й діями осіб"[141]. Це пов'язано з різноманітними чинниками, що впливають на особу в момент надання згоди.

Одним з аспектів інформованості, є зазначення мети обробки даних. Така вимога, як чітко вказати ціль використання даних ставиться вже під час надання згоди. Проте це суперечить концепції Big Data, яка спрямована на накопичення даних і їх потенційне використання, яке може бути визначене згодом[142]. Отримати згоду для обробки даних із метою використання її в технології Big Data може бути складно, з огляду на вимоги, які ставляться до згоди[143]. Отже, підвищені вимоги до згоди впливають на технологічний розвиток, зокрема, ускладнюючи його.

Інша небезпека, що йде від Big Data аналізу, полягає у загрозі колективної приватності. Це добре демонструється на прикладі соціальних мереж. Чим більше інформації особа добровільно розкриває про себе для алгоритмів, тим легше спрогнозувати роботу відповідних алгоритмів. Крім того, чим більше особа розкриває про себе, тим збільшується ймовірність розкриття інформації про інших користувачів незалежно від їх згоди[144]. На допоможу приходить соціологічна схильність ділитися інформацією, якщо нею діляться всі навколо[145]. Наприклад, якщо в особи є певний відсоток друзів, що належать до окремої

[140] TRUSTe, GB Consumer Privacy Index, 2016.
[141] Hermstruwer, Yoan, 'Contracting around Privacy: The (Behavioral) Law and Economics of Consent and Big Datamics of Consent and Big Data', *JlPlTEC*, 8 (2017), 9–26, p. 16.
[142] Yeung, Karen, '"Hypernudge": Big Data as a Mode of Regulation by Design'', Information, Communication & Society, 1 (2016), 31. P.13.
[143] Zarsky, Tal Z., 'Incompatible: TheThe GDPR in the Age of Big Data', Seton Hall Law Review, 47 (2017), 995–1020, p.1017.
[144] Hermstruwer, Yoan, 'Contracting around Privacy: The (Behavioral) Law and Economics of Consent and Big Datamics of Consent and Big Data', P. 12.
[145] Holland, H. Brian, Privacy Paradox 2.0 (April 4, 2010). Widener Law Journal, Forthcoming. URL: https://ssrn.com/abstract=1584443, p. 17.

соціальної групи (прихильники певної політичної ідеології, абощо), то алгоритми можуть вирахувати, яка ймовірність належності цієї особи до соціальної групи.

Складність полягає в тому, що отримавши згоду на обробку даних від частини осіб, алгоритми продукують зовсім нову інформацію, яка не походить від особи. Проте цю нову інформацію прив'язують до особи та можуть на основі цих даних приймати пені рішення, зокрема щодо цільової реклами. І така інформація не вважається персональними даними, тому в особи не виникає права її виправити чи видалити.

Італійський науковець Т. Сканіккіо у своїй докторській роботі порівнює згоду на обробку даних з угодою з дияволом[146]. Він аналізує Правила користування й Політику конфіденційності Google, та, окрім недотримання прав осіб щодо захисту своїх даних, також встановлює недоліки згоди. Зокрема, він відзначає фактичну безумовність згоди, коли особа хоче користуватися послугами Google[147]. Він також згадує нечітко описану мету збирання даних, яка фактично дозволяє компанії збирати дані про більшість активності особи в мережі.[148] І хоча умови обробки описати в простій і зрозумілій формі, це не допомагає захистити свої дані від небажаної обробки, з огляду на дещо монополістичне становище Google на ринку.

Переконливим є аргумент, що "згода перестала працювати, оскільки ми не маємо стійкого чи відчутного розуміння, скільки нам потрібно отримати інформації, щоб згода була достатньо інформованою"[149]. Відповідь частково прописана в правових нормах, що встановлюють перелік інформації, необхідної для згоди. Проте, у різних ситуаціях особа потребує різної інформації.

Окрім інформованості, питання постають і до **добровільності** згоди. Виникають ситуації, коли цю умову неможливо забезпечити, оскільки від

[146] Tommaso Scannicchio PhD Thesis Google's Faustian Bargain: Contested Issues On TheInterface Between Privacy And Contract. URL: https://uniba-it.academia.edu/TommasoScannicchio/Thesis-Chapters.
[147] Там само.
[148] Політика конфіденційності Google. URL: https://policies.google.com/privacy?hl=uk#infocollect.
[149] Brownsword R. (2009) Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality. In: Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S. (eds) Reinventing Data Protection?. Springer, Dordrecht. P. 99.

надання згоди залежить отримання певного блага суб'єктом даних. Відповідно до вже згаданого дослідження користувачів інтернету, тринадцять відсотків опитуваних відчувають себе змушеними використовувати сайт, якому вони не довіряють, серед яких більше третини вказали, що це був єдиний сайт, що продавав конкретний товар чи надавав послугу[150]. Отже, особи змушені погоджуватися навіть на несприятливі умови, для того, щоб отримати бажане благо.

Проте цей недолік може відслідковуватися не лише з погляду захисту приватності, адже аналогічні ситуації можуть виникати і в повсякденних справах, що не вимагатимуть розкриття персональних даних, та вони є зумовлені ринковою економікою. Якщо якась компанія продає ексклюзивний товар чи надає ексклюзивну послугу, то особа не має можливості обрати іншого контрагента і змушена погоджуватися на наявні умови, наприклад, вищу ціну.

У такий спосіб, деякі компанії, що є володільцями персональних даних, будують свої підприємства, щоб підлаштуватися під ці чинники. "Переважна бізнес-модель для сучасних цифрових сервісів, є видом «бартеру», за яким користувачі погоджуються розкривати свої особисті дані фірмі в обмін на послуги"[151]. Відповідно до цього, "модель бізнесу є швидше платною, ніж безоплатною ('fee' rather than 'free'), приваблюючи клієнтів, які спершу невпевнені, наскільки вони готові платити за цей сервіс"[152]. У результаті вони «платять» надаючи дозвіл на обробку своїх персональних даних.

Це нагадує модель захисту приватності, за якої персональні дані розглядаються, як власність. Правомочність благовикористання[153] дає можливість особі розпоряджатися своїми даними на власний розсуд, у тому числі передавати їх в обмін на користування сервісом, наприклад, соціальною мережею. Тут можна сказати, що цей підхід унеможливлює встановлення

[150] TRUSTe, GB Consumer Privacy Index, 2016.
[151] van Dijck, J. (2014). Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology. Surveillance & Society. 12(2), 199-208.
[152] Lambrecht, A. (2013) The Economics of Pricing Services Online. In S.N. Surlauf & L.E. Blume (Eds.), The New Palgrave Dictionary of Economics.
[153] Право фізичної особи на власні персональні дані в цивільному праві України : автореф. дис. ... канд. юрид. наук : 12.00.03 / О. А. Дмитренко, с. 12.

захисту персональних даних, оскільки вся відповідальність покладається на суб'єкта даних. Хоча цей підхід не відображається в законодавстві, насправді часто у такий спосіб трактується надання згоди в сучасному цифровому просторі.

Крім того, проблема з добровільністю виникає і з іншого аспекту. "Зазвичай право утримується від визнання певного акту, який зовні виглядає узгодженим, та толерує значну кількість маніпуляцій або і примусу, перед тим, як визнавати акт таким, що був вчинений без згоди особи"[154]. Водночас, "обман є однозначним порушенням автономії особи, оскільки передбачає контроль іншого без згоди цієї особи"[155]. Особа має як мінімум моральне право не бути підданою обману. К. Єунг стверджує, що коли люди погоджуються на обробку даних, вони "супутньо не нівелюють своє право не бути обманутими"[156].

Єунг наводить приклад політичного маніпулювання виборцями в соціальних мережах. Хоча особи не давали конкретної згоди для цілей отримання політичної реклами, проте дані були використані з такою метою.[157] Найяскравішими прикладами є вибори Президента США 2016 року та Референдум про вихід Сполученого Королівства з Європейського Союзу 2016 року[158]. Тут не було волі осіб на цю конкретну обробку персональних даних.

Це переносить нас до проблематики **самої концепції згоди**. Згода є нейтральною до суті. Якщо особа погодилася на конкретну дію щодо своїх даних, згоді немає різниці чи це збирання, використання чи розкриття даних хороше чи погане. Згода легітимізує будь-яку обробку. Даніель Солове підтверджує необхідність включення в правове регулювання захисту даних концепції privacy self-management. Тим не менш, він стверджує, що "згоді

[154] Solove D. J. Privacy self-management and the consent dilemma, P. 1897.
[155] Wendler, D. (1996). Deception in Medical and Behavioral Research: Is It Ever Acceptable?. The Milbank Quarterly. 74 (1), 87-114. P. 91.
[156] Yeung, Karen, '"Hypernudge": Big Data as a Mode of Regulation by Design'', P.15.
[157] Там само.
[158] Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, The Guardian, 27.03.2018. URL: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

доручили роботу, що понад її сили. Вона не дає людям змістовного контролю над їх даними”[159].

Особа може надати згоду на передачу даних третім особам, але право не оцінює з етичної позиції чи ці дані не будуть використані на добро. Так, можна згадати про використання даних для маніпуляцій переконаннями виборців чи для надсилання цільової реклами. І в різних осіб може бути різне ставлення до такого використання їх даних. Дехто може бути задоволений, що отримує релевантну рекламу щодо його зацікавлень, а інші ж навпаки вважатимуть це грубим порушенням їх приватності. Аналогічно, деякі особи хочуть мати вплив і контроль над діями щодо їх персональних даних, інші ж готові віддати це питання на розсуд регулятора. “Немає універсального підходу до згоди, який задовільнив би всіх користувачів”[160].

Ще один чинник, це велика кількість контрагентів, з якими щоденно стикається особа. “Навіть якщо особі надають простий та зрозумілий спосіб керувати своїми даними, є просто занадто багато суб’єктів, що збирають, використовують та розкривають дані, щоб їх усіх проконтролювати, навіть раціональній особі”[161]. Це викликає необхідність у створенні певного глобального способу контролювати свої дані.

Фактично, саме на презумпції раціональних суб’єктів даних і збудована чинна система захисту даних. Такі особи уважно читають політики конфіденційності і зважують ризики розкриття своїх персональних даних[162]. Проте ця презумпція помилкова. Уже досліджено, що особи не читають політик конфіденційності, що ж до оцінки ризиків?

При наданні згоди особа оцінює переваги, які вона отримує від надання згоди. Це може бути безоплатний доступ до певного сервісу чи веб-ресурсу, наприклад, соціальної мережі. З іншого боку, оцінюються недоліки від розкриття

[159] Solove D. J. Privacy self-management and the consent dilemma, P. 1880.
[160] Hutton L, Henderson T. "I didn't sign up for this!": Informed consent in social network research. In Proceedings of the 9th International AAAI Conference on Web and Social Media (ICWSM). 2015. p. 178-187. P. 186.
[161] Solove D. J. Privacy self-management and the consent dilemma, P. 1888.
[162] Schermer, Bart Willem and Custers, Bart and van der Hof, Simone, The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection (February 25, 2014). Ethics and Information Technology, DOI: 10.1007/s10676-014-9343-8, Forthcoming. URL: https://ssrn.com/abstract=2412418 p. 14.

персональних даних. Проте, “дуже часто є неможливо оцінити переваги й недоліки розкриття певних даних, оскільки замало інформації надано або вона є подана в складній формі, що унеможливлює адекватне прийняття рішення про згоду”[163].

Тут знову спрацьовує ефект надання переваги короткочасній і безпосередній перевазі над потенційними втратами в майбутньому[164]. Ф. Боржесьюс називає це упередження міопією, або короткозорістю. “Багато людей обирають негайний доступ до сервісу, навіть якщо це означає, що вони мають погодитися на цільову рекламу, незалежно від їх попередніх планів не погоджуватись на такі цілі обробки”[165].

Крім того, діє помилка, яку ще називають «мені нічого ховати». Коли порівнюють індивідуальне право на приватність і колективне право на безпеку, то часто особи розкривають дані керуючись аргументом – “якщо тобі нічого ховати, то тобі немає причин боятися”[166]. Однак ця думка є в корені помилкова, якщо звернутися до перших ідей приватності. Кожен має право не розкривати якусь інформацію про себе.

Навіть якщо хтось не думає надавати згоду, на нього може вплинути ефект розплутування (unraveling), описаний Й. Хермструвер. Наприклад, страхова компанія пропонує знижку, якщо особа розкриє певну вартісну інформацію, таку, як дані про стан здоров’я. Люди з хорошим станом здоров’я однозначно погодяться, оскільки їм це принесе вигоду. Серед тих, що залишаться опиняться особи, що мають також досить хороше здоров’я і для них також вигідним буде розкрити ці дані, оскільки вони ще попереду багатьох інших, а

[163] Solove D. J. Privacy self-management and the consent dilemma, P. 1880.
[164] Hermstruwer, Yoan, ‘Contracting around Privacy: The (Behavioral) Law and Economics of Consent and Big Datamics of Consent and Big Data’, P. 23.
[165] Zuiderveen Borgesius, Frederik, Consent to Behavioural Targeting in European Law - What are the Policy Implications of Insights from Behavioural Economics? (July 27, 2013). Amsterdam Law School Research Paper No. 2013-43. URL: https://ssrn.com/abstract=2300969, p. 40.
[166] Murumaa-Mengel, Maria & Laas-Mikko, Katrin & Pruulmann-Vengerfeldt, Pille. (2015). “I Have Nothing to Hide”: A Coping Strategy in a Risk Society. https://www.researchgate.net/publication/283713758_I_Have_Nothing_to_Hide_A_Coping_Strategy_in_a_Risk_Society, p. 198.

нерозкриття даних свідчить, що їм що приховувати. І так триватиме поки всі користувачі не дадуть згоду[167].

Це спричиняє психологічний тиск на осіб, що не дають згоди. Навіть якщо особа має переконання, що вона не збирається розкривати свої дані, у цьому ланцюжку вона опиняється в невигідному становищі. Це призводить і до дискримінації, залежно від надання згоди чи залежно від стану здоров'я.

Уже зараз трапляються випадки, коли страхові компанії пропонують за знижки надати доступ до даних із фітнес браслетів[168]. Проте чи враховують особи, які дають згоду на таку оброку всі ризики, зокрема щодо майбутньої дискримінації щодо них чи інших осіб? Ефект розплутування в дії має негативні наслідки не лише на приватність даних. Усі ці проблеми концепції згоди є глобальними, а тому актуальними і для України також.

Згода на обробку персональних даних далека від досконалості. Інформованість губиться, коли люди не читають політик конфіденційності. А нові технології, як Big Data, та сервіси не прагнуть надати чітку інформацію про майбутню обробку, зважаючи на проблематику ведення бізнесу. Монопольність певних сервісів примушує погоджуватися на невигідні умови захисту даних. Унаслідок, люди починають «торгувати» своїми даними в обмін на безоплатні сервіси. Згода легітимізує будь-яку обробку, у тому числі погану.

Об'єктивні чинники, як велика кількість контрагентів, та помилки, як обрання негайної переваги у порівнянні з ризиками в майбутньому, впливають на наше рішення щодо згоди. Дії інших суб'єктів також впливають на наш вибір. Врешті, згода зачіпає й дискримінацію.

Відтак, якщо існує стільки проблемних питань, то чи варто продовжувати розвивати інститут, який усе менше працює. Чи є якісь способи вдосконалити згоду, чи потрібно відмовлятися від неефективного інструменту?

---

[167] Hermstruwer, Yoan, 'Contracting around Privacy: The (Behavioral) Law and Economics of Consent and Big Datamics of Consent and Big Data', p. 13.

[168] What happens when life insurance companies track fitness data? The Verge. URL: https://www.theverge.com/2018/9/26/17905390/john-hancock-life-insurance-fitness-tracker-wearables-science-health and Insurance policies tracking fitness, diet, sleep have alarming discrimination and privacy risks, experts say. URL: https://www.sbs.com.au/news/the-feed/insurance-policies-tracking-fitness-diet-sleep-have-alarming-discrimination-and-privacy-risks-experts-say.

3.2. Пропозиції змін до правового регулювання згоди для обробки персональних даних.

Хоча згода й сильно критикується, забравши її ми позбавимо особу можливості визначатися щодо власної приватності. Тож варто розглянути можливості покращення регулювання згоди, щоби вона стала більш ефективною. Спершу іде огляд пропозицій до зміни концепції згоди, а потім пропозиції зміни в національне законодавство.

Перший спосіб змінити концепцію згоди, це дати особам можливість впливати на конкретні умови згоди, змінювати їх, відмовлятися від них тощо. Фактично надати "можливість обирати, які частини сервісу особа хоче використовувати та які персональні дані розкривати"[169]. Чинна модель згоди є лише двозначною (або особа дає згоду, або ні). "Згода є більш багатогранною, та право приватності потребує нового підходу до граней, при цьому не стаючи надто складним, щоб працювати"[170].

Реєстрація на веб ресурси, як Google чи Facebook не подібна переговорам і "користувач не може відмовити окремим умовам, що загрожують його баченню приватності"[171]. Коли особа надає згоду на обробку персональних даних, то вона зазвичай погоджується на умови обробки, запропоновані потенційним володільцем даних і не має змоги запропонувати зміни до цих умов.

Якщо особа хоче детально регулювати свою приватність, то вимога добровільності згоди буде більшою мірою задоволена. Адже тоді особа дійсно свідомо надаватиме згоду на таку обробку даних, проти якої вона не має заперечень. Також буде задоволена вимога конкретності згоди, оскільки особа зможе контролювати цілі обробки своїх даних.

Якщо взяти до уваги вимогу Регламенту (ЄС) 2016/679 (GDPR) щодо виділення згоди від інших умов надання послуг, то за аналогією можна встановити норму, що вимагатиме розділяти різні аспекти обробки і відповідно

[169] Misek Jakub, 'Consent to Personal Data Processing - The Panacea or the Dead End', P.80.
[170] Solove D. J. Privacy self-management and the consent dilemma, P. 1902.
[171] Jammet Adrien, The Evolution of EU Law on the Protection of Personal Data, Centre for European Law and Legal Studies (CELLS) Online Papers (2014) URL: http://ssrn.com/abstract=2501417, p. 14.

давати згоду на кожен із них. Проте, такий підхід підходить далеко не всім. Уже були згадані проблеми витрати часу на розбирання правил приватності, які призводять до погано зважених рішень заради швидкого блага. “Багато осіб не хочуть займатися детальним керуванням своїх даних”[172].

Щоб розв’язати проблему надмірної кількості контрагентів, яким особа надає згоду на обробку своїх даних, можна встановити загальний спосіб управління даними. Цю ідею підтримує Д. Солове. Він вказує, однак, що “знайти шлях керувати приватністю щодо всіх контрагентів може бути викликом. Оскільки складно визначити загальний набір налаштувань приватності, що будуть підходити всіх організаціям. А також наслідки збирання, використання чи розкриття даних можуть бути різними, залежно від обставин”[173].

Тим не менш, я вважаю, що можна знайти, зокрема, технологічне рішення вказаної проблеми. Створити сервіс, у якому особа висловлює свої погляди щодо обробки різних даних та різних видів обробки. Згодом, коли особа зіткнеться з необхідністю приймати рішення про надання згоди на обробку даних, сервіс може проаналізувати умови обробки даних потенційним володільцем даних та прийняти рішення про повну чи часткову згоду на обробку даних, залежно від заявлених переконань особи.

Втілення такого сервісу вимагатиме першочергового втілення можливості погоджуватися лише на окрему обробку даних. Проте поєднання цих рішень усуне безліч проблем, що виникають при прийнятті рішення про надання згоди на обробку самою особою. “Люди хочуть мати змогу керувати своєю приватністю, проте не забагато. Закони про приватність мають знайти шлях надавати часткове керування приватністю”[174].

Крім того, закон може встановити обов’язок компетентних органів видавати напрямні (роз’яснення, рекомендації) щодо видів використання даних, супутніх ризиків та загроз. “Певні види обробки можуть бути заборонені, певні

[172] Solove D. J. Privacy self-management and the consent dilemma, P. 1901.
[173] Там само, с. 1900.
[174] Там само, с. 1902.

обмежені, певні можуть вимагати додаткової згоди або не вимагати такої. Компетентні органи повинні переглядати нові способи використання даних, як тільки вони виникають"[175]. З одного боку, такі авторитарні приписи будуть обмежували автономію суб'єкта даних. Проте, якщо вони нестимуть рекомендаційний та інформативний характер, то можуть допомагати особі зрозуміти, як діяти у разі потенційної оброки певного виду.

У час Big Data принцип приватності за згодою несе все менше значущості та має бути замінений на приватність за відповідальністю, включаючи суворіші заходи щодо притягнення до відповідальності використання даних компаніями, вважає Маєр-Шьонбергер[176].

В цю епоху Big Data значною частиною цінності даних є їх вторинне використання, яке не було передбачено під час збирання даних. Отже, захист даних повинен надавати менший наголос на збір даних та більше на подальше використання даних. Дані більше не збираються з огляду на конкретну мету та інформовану згоду користувача, навпаки, "мета збору даних часто формулюється в широких загальних термінах і приймається користувачем з обмеженим сприйняттям того, що передбачає згода"[177].

Це, здається, ігнорує або зменшує фундаментальний розрив між комерційною цінністю, яку особисті дані мають для компанії, і правом особи на конфіденційність. "Повірити, що принцип відповідальності компаній разом із більш сильними механізмами застосування буде достатнім для захисту права особи на приватне життя, здається надто оптимістичним у час, коли особисті дані мають безпрецедентну комерційну цінність, а також, коли збір персональних даних є основою онлайн бізнес-моделі"[178].

Що ж до українського законодавства. Передусім, потрібно привести його у відповідність з Регламентом у зв'язку з зобов'язаннями України відповідно до

[175] Solove D. J. Privacy self-management and the consent dilemma, P. 1902.
[176] Mayer-Schönberger, V. C. K. (2013). Big data: a revolution that will transform how we live, work, and think. Boston: Houghton Mifflin Harcourt: 173-175.
[177] Там само.
[178] Rikke Frank Joergensen, The unbearable lightness of user consent, The Danish Institute for Human Rights, Copenhagen, Denmark, Published on: 21 Oct 2014.

Угоди про Асоціацію. У другому розділі наведена таблиця порівняння умов дійсності згоди на обробку персональних даних в Україні та ЄС. Відповідно до неї можна визначити важливі аспекти згоди, які потребують вдосконалення та узгодження.

Першочергово, це розширення вимог до добровільності згоди. Вимога відокремлення положень щодо згоди від інших умов допоможе чітко розрізняти згоду, як окрему підставу для обробки даних. Також, варто додати положення про врахування негативних наслідків для особи у випадку відмови від надання згоди. Крім того, пропоную додати положення про можливість суб'єкта даних давати згоду на окремі аспекти обробки даних, а від певним мати право відмовитися. Також, варто додати повноваження Уповноваженого Верховної Ради з прав людини видавати рекомендації щодо способів використання персональних даних.

Пропоную розглянути запропоновані законодавчі зміни в порівняльній таблиці, поданій далі.

Таблиця №2. Порівняння запропонованих змін до законодавства

Чинна редакція	Запропонована редакція
Закон України „Про захист персональних даних"	
Стаття 2. Визначення термінів "… згода суб'єкта персональних даних - добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди. У сфері	Стаття 2. Визначення термінів … згода суб'єкта персональних даних – добровільне, **конкретне та поінформоване** волевиявлення фізичної особи щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або **шляхом ствердних дій**, що

електронної комерції згода суб'єкта персональних даних може бути надана під час реєстрації в інформаційно-телекомунікаційній системі суб'єкта електронної комерції шляхом проставлення відмітки про надання дозволу на обробку своїх персональних даних відповідно до сформульованої мети їх обробки, за умови, що така система не створює можливостей для обробки персональних даних до моменту проставлення відмітки; …"[179]	дають змогу зробити висновок про надання згоди[180]. ***(далі виключити)***
Стаття 10. Підстави для обробки персональних даних "1. Підставами для обробки персональних даних є: 1) згода суб'єкта персональних даних на обробку його персональних даних; …"[181]	Стаття 10. Підстави для обробки персональних даних 1. Підставами для обробки персональних даних є: 1) згода суб'єкта персональних даних на обробку його персональних даних **для однієї чи декількох конкретних цілей[182];** … ***(далі включити)*** 2. У сфері інформаційних електронних послуг згода суб'єкта персональних

[179] Про захист персональних даних: Закон від 01.06.2010 № 2297-VI, ст. 2.
[180] Змінено визначення шляхом додавання до нього вимог конкретності, виділення вимоги інформованості та зміни до форми згоди. За основу взято визначення відповідно до ст. 2 Закону України «Про захист персональних даних».
[181] Про захист персональних даних: Закон від 01.06.2010 № 2297-VI, ст. 10.
[182] До переліку підстав для обробки персональних даних у підставі згоди додано вказівку на цілі обробки таких даних. За основу взято положення відповідно до ст. 10 Закону України «Про захист персональних даних».

	даних може бути надана під час реєстрації в інформаційно-телекомунікаційній системі шляхом проставлення відмітки про надання дозволу на обробку своїх персональних даних відповідно до сформульованої мети їх обробки, за умови, що така система не створює можливостей для обробки персональних даних до моменту проставлення відмітки[183]. Мовчання, автоматичне заповнення клітинок відмітками про надання згоди або бездіяльність не становлять надання згоди на обробку персональних даних[184]. 3. Якщо суб'єкт даних надає згоду в контексті письмового волевиявлення, що також стосується інших питань, запит на надання згоди необхідно подавати у формі, що чітко відрізняється від інших питань[185]. Якщо володілець даних здійснює обробку персональних даних з метою укладення та виконання правочину,

[183] Перенесено з визначення згоди у ст. 2 Закону України «Про захист персональних даних». Змінено сферу електронної комерції на сферу електронних послуг, що розширює застосування даного положення.
[184] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних), п. 32 преамбули.
[185] Частково взято з ст. 7(2) Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних).

	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, то згода не є належною підставою для такої обробки. 4. Згоду не можна вважати такою, що була добровільно наданою, якщо суб'єкт даних не здійснює справжнього чи добровільного вибору, або неспроможний відмовити в наданні згоди не заподіюючи водночас собі негативних наслідків[186]. У разі надання згоди на обробку персональних даних, суб'єкт даних має право відмовитися від окремих дій щодо використання персональних даних проставивши відповідну відмітку[187].
	Стаття 23. Повноваження Уповноваженого Верховної Ради з прав людини у сфері захисту персональних даних

[186] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних), п. 42 преамбули.
[187] Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних), ст. 7(2).

	1. Уповноважений має такі повноваження у сфері захисту персональних даних: … ***(далі включити)*** 6-1) надавати рекомендації щодо способів використання персональних даних, які можуть містити потенційні ризики та загрози правам людини, передбаченим Конституцією України та міжнародно-правовими актами, згоду на обов'язковість яких надана Верховною Радою України; …

Запропоновані зміни адресовані вищенаведеним способам вдосконалення згоди як підстави для обробки персональних даних. Вони не змінюють докорінно інститут захисту персональних даних, проте дають змогу суб'єкту даних мати вибір та контроль щодо обробки своїх персональних даних.

Підсумовуючи, слабкі аспекти згоди можна виправити шляхом змін до механізму надання згоди. Зокрема, можна надати можливість суб'єкту даних погоджуватись або відмовлятися від окремих видів використання персональних даних. Для кращого контролю складного процесу згоди, можна створити сервіс, що проводитиме аналіз пропонованих умов згоди і прийматиме рішення щодо надання згоди на підставі переконань конкретної особи. Для покращення розуміння ризиків та загроз окремих видів використання даних компетентний орган може видавати рекомендації. Українське законодавство необхідно привести у відповідність з окремими вимогами європейського регулювання та відповідними пропозиціями удосконалення згоди. Для цього вище наведена таблиця пропонованих змін до законодавства.

ВИСНОВКИ

Унаслідок дослідження правового регулювання згоди на обробку персональних даних було зроблено наступні висновки:

1. Ще перші публікації про право на приватність містять згадку про згоду особи на використання її персональних даних. Законодавство про захист персональних даних розвивається різними шляхами в різних юрисдикціях, окремо розрізняються європейська та американська моделі захисту персональних даних. У Європейському Союзі утворюється міжнародна система захисту персональних даних. Її взято за основу при формуванні положень національного законодавства з захисту персональних даних в Україні, а саме Закону України «Про захист персональних даних».

Нещодавно в ЄС прийнято новий Регламент (ЄС) 2016/679 (GDPR), який має пряму дію для держав-членів ЄС, а також екстериторіальну дію. Це означає, що він може в певних випадках застосовуватися в Україні. З огляду на це, а також на курс євроінтеграції України, варто розглядати положення українського законодавства в порівнянні з положеннями даного Регламенту.

2. Проаналізувавши всі підстави для обробки даних, можна зробити висновок, що є загальні підстави та підстави для обробки особливих категорій даних – чутливих даних. Крім того, ці підстави можна розділити на згоду та інші законні підстави для обробки даних. Такий поділ знаходить вираження в різноманітних правових актах.

Згода відрізняється від інших підстав для обробки даних тим, що вона надає особі змогу самостійно контролювати втручання у її право на приватність. Особливо складно розмежувати підставу згоди на обробку персональних даних та обробку даних для укладення чи виконання правочину, стороною якого є суб’єкт персональних даних. У випадку включення згоди, як однієї з умов договору, суб’єкт даних може вводитися в оману щодо потенційного відкликання такої згоди, яке не припинить обробку, оскільки вступить в дію

друга підстава. Тому важливо розглядати згоду, як окрему й особливу підставу для обробки персональних даних.

3. Особливість згоди полягає в її міцному зв'язку з волею особи. Згода постає особистим дозволом на втручання в право на приватність та захист персональних даних. Згода означає волевиявлення особи, що легітимізує використання її персональних даних іншими особами. Щоб таке волевиявлення було дійсним, воно має відповідати певним встановленим вимогам.

4. Українське законодавство встановлює наступні вимоги до згоди: добровільність, інформованість, форма та факультативно однозначність (при обробці чутливих даних). Окремо виділяється й мета обробки, як невіддільний елемент згоди. Добровільність згоди ставиться під сумнів у судових справах, де суб'єкти даних надавали згоду, у той час, як насправді мали бути застосовані інші підстави для обробки даних.

Вимоги до згоди деталізовано окремими підзаконними актами, наприклад, уточнено, яку саме інформацію повинен отримати суб'єкт персональних даних, щоб згода вважалась інформованою. Для належної форми важливо, щоб володілець згодом міг підтвердити факт надання згоди суб'єктом даних. Однозначність згоди має підтверджувати її безсумнівне надання.

5. Відповідно до Регламенту (ЄС) 2016/679 (GDPR) вимоги дійсності згоди є набагато конкретнішими та вимогливішими в порівнянні з українським регулюванням. Окрім добровільності, інформованості й однозначності висуваються також вимоги конкретності, явності. Зазначення більшої кількості вимог, з одного боку, спричиняє до роздроблення первинних вимог, з іншого – чим більше вимог закріплено, тим більше володільці персональних даних зважатимуть на їх дотримання.

Порівняння українських та європейських умов дійсності згоди дає можливість проводити паралелі та знаходити напрями інтеграції українського права. Українське регулювання потребує змін, щоб мати адекватний рівень захисту відповідно до вимог ЄС. Тим часом, країни, які визнані такими, що мають належний рівень захисту (наприклад, Канада, Ізраїль, Швейцарія), не

завжди дослівно повторюють регулювання ЄС. Часто вони застосовують інші режими захисту даних, які все ж гарантують належний захист персональних даних.

6. Згода не є досконалою підставою для обробки даних. Інформованість згоди не досягається, оскільки люди не читають політик конфіденційності, зважаючи на їх складність та обсяг. А нові бізнес-моделі не прагнуть надати чітку інформацію про майбутню обробку, оскільки це не сприятиме методам ведення підприємницької діяльності. Монополія певних сервісів фактично змушує осіб погоджуватися на невигідні для них умови захисту персональних даних. Унаслідок, люди починають «торгувати» своїми даними в обмін, зокрема, на безоплатні сервіси.

Згода може легітимізувати будь-яку обробку, не виключаючи і спрямовану на погані цілі. Об’єктивні чинники, як велика кількість контрагентів, та помилки, як обрання негайної переваги в порівнянні з ризиками у майбутньому, впливають на наше рішення щодо згоди. Проблеми згоди ставлять під сумнів повсюдне застосування саме цієї підстави для обробки даних.

7. Слабкі аспекти згоди можна змінити шляхом покращення процесу її надання. Зокрема, можна надати змогу суб’єкту даних погоджуватись або відмовлятися від окремих форм використання персональних даних. Щоб краще контролювати складний процес згоди, можна сформувати сервіс, що аналізуватиме пропоновані умови згоди і прийматиме рішення про надання згоди, враховуючи думку окремої особи.

Щоб особи більше розуміли ризики та загрози окремих форм використання даних, компетентний орган може видавати рекомендації щодо таких форм. Для вдосконалення українського законодавства і виведення його на належний рівень захисту персональних даних, запропоновано зміни до Закону України «Про захист персональних даних».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Міжнародно-правові акти:

1. Європейська конвенція про захист прав людини і основоположних свобод від 4 листопада 1950 року. База даних «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/995_004.

2. Загальна декларація прав людини від 10.12.1948. База даних «Законодавство України»/ВР України. URL: http://zakon2.rada.gov.ua/laws/show/ 995_015 .

3. Міжнародний пакт про громадянські і політичні права від 16.12.1966. База даних «Законодавство України»/ВР України. URL: http://zakon2.rada.gov.ua/laws/show/ 995_043.

4. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). Офіційний вісник Європейського Союзу L 119/1 04.05.2016 (офіційний переклад).

5. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 27.06.2014 року. База даних «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/984_011.

6. African Union Convention on Cyber Security and Personal Data Protection 2014. URL: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

7. Article 29 Working Party Guidelines on consent under Regulation 2016/679 (WP259 rev.01) Adopted on 28 November 2017.

8. Charter of Fundamental Rights of The European Union, 18.12.2000, Official Journal of the European Communities, C 364/1: http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

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) URL: http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi! celexapi!prod!CELEXnumdoc&lg=en&numdoc=32002L0058&model=guichett.

10. 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. Official Journal L. 1995. URL: http://eur-lex.europa.eu/legal- content/en/TXT/?uri=CELEX%3A31995L0046.

11. European Union - Consolidated version of the Treaty on the Functioning of the European Union - Protocols - Annexes - Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007, URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT.

12. Guidelines governing the protection of privacy and transborder flows of personal data (23 September 1980) Organisation for Economic Cooperation and Development.

13. Opinion 15/2011 on the definition of consent. Adopted on 13 July 2011. URL: http://ec.europa.eu/justice/policies/ privacy/docs/wpdocs/2011/wp187en.pdf.

Національне законодавство:

14. Деякі питання практичного застосування Закону України "Про захист персональних даних": Роз'яснення Міністерства юстиції України від 21.12.2011. База даних «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/n0076323-11.

15. Конституція України: Закон від 28.06.1996 № 254к/96-ВР. База даних «Законодавство України»/ВР України. URL: http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

16. Лист Уповноваженого Верховної Ради з прав людини від 03.03.2014 № 2/9-227067.14-1/НД-129. База даних «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/v7067715-14.

17. Пояснювальна записка до Проекту Закону України «Про захист персональних даних» № 2297-VI від 01.06.2010. База даних «Законодавство України»/ВР України. URL: http:// w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=32124&pf35401=119742.

18. Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних: Закон від 03.07.2013 № 383-VII. База даних «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/383-18.

19. Про захист персональних даних: Закон від 01.06.2010 № 2297-VI. База даних «Законодавство України»/ВР України. URL: http://zakon0.rada.gov.ua/laws/show/2297-17.

20. Роз'яснення до Типового порядку обробки персональних даних: Уповноважений Верховної Ради з прав людини, 08.01.2014. База даних «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/n0001715-14.

21. Цивільний кодекс України: Закон від 16.01.2003 № 435-IV. База даних «Законодавство України»/ВР України. URL: http://zakon.rada.gov.ua/laws/show/435-15.

22. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання прав і свобод людини і громадянина в Україні за 2017 рік. URL: www.ombudsman.gov.ua/files/Dopovidi/Report-2018-1.pdf.

23. Israel Protection of Privacy Law, 5741 – 1981, article 1, URL: https://www.gov.il/BlobFolder/legalinfo/legislation/en/ProtectionofPrivacyLaw57411981unofficialtranslatio.pdf.

24. Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data COM (90) 314 final — SYN 287 (Submitted by the Commission on 27 July 1990) (90/C 277/03) URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51990PC0314(01) &from=EN.

25. Swiss Federal Act on Data Protection of 19 June 1992. URL: https://www.admin.ch/opc/en/classified-compilation/19920153/index.html.

26. The Personal Information Protection and Electronic Documents Act (PIPEDA) 2000. URL: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html.

27. United States. Department of Health, Education, and Welfare. Secretary's Advisory Committee on Automated Personal Data Systems & Ware, Willis H 1973, Records, computers, and the rights of citizens: report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Dept. of Health, Education & Welfare.

Судова практика:

28. Рішення Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ від 26 жовтня 2016 року у справі 473/2644/15-ц. URL: http://www.reyestr.court.gov.ua/Review/62754765.

29. Рішення Вінницького міського суду Вінницької області від 03 червня 2014 року у справі № 127/7229/14-ц. URL: http://www.reyestr.court.gov.ua/Review/39125979.

30. Рішення ЄСПЛ у справі Copland v UK, заява 62617/00, 03/04/2007, URL: http://hudoc.echr.coe.int/eng?i=001-79996.

31. Рішення ЄСПЛ у справі Gaskin v UK, заява 10454/83, 07/07/1989, URL: http://hudoc.echr.coe.int/eng?i=001-57491.

32. Рішення ЄСПЛ у справі Klass v Germany, заява 5029/71, 06/09/1978, URL: http://hudoc.echr.coe.int/eng?i=001-57510.

33. Рішення ЄСПЛ у справі Leander v. Sweden, заява 9248/81, 26/03/1987, URL: http://hudoc.echr.coe.int/eng?i= 001-57519.

34. Рішення ЄСПЛ у справі Malone v UK, заява 8691/79, 02/08/1984, URL: http://hudoc.echr.coe.int/eng?i=001-57533.

35. Рішення ЄСПЛ у справі P.G. and J.H. v UK, заява 44787/98, 25/09/2001, URL: http://hudoc.echr.coe.int/eng?i= 001-59665.

36. Рішення ЄСПЛ у справі Perry v UK, заява 63737/00, 17/07/2003, URL: http://hudoc.echr.coe.int/eng?i=001-61228.

37. Рішення ЄСПЛ у справі Potaru v Romania, заява 28341/95, 04/05/2000, URL: http://hudoc.echr.coe.int/eng?i= 001-58586.

38. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20.01.2012 № 2-рп/2012. База даних «Законодавство України» /ВР України. URL: http://zakon1.rada.gov.ua/laws/show/v002p710-12.

39. Рішення Луцького міськрайонного суду Волинської області від 07 лютого 2018 року у справі № 161/18512/17. URL: http://www.reyestr.court.gov.ua/Review/72248664.

40. Рішення Жовтневого районного суду м. Харкова від 26 липня 2013 року у справі № 639/4355/13-ц. URL: http://www.reyestr.court.gov.ua/Review/34565599.

41. Constitutional Court, Karlsruhe. URL: http://www.datenschutzberlin.de/gesetze/sonstige/volksz.htm.

42. Decision of the First Senate of 15 December 1983 - 1 BvR 209/83 et al. Federal.

43. The Regional Court of Berlin judgment of 16 January 2018 (docket no. 16 O 341/15).

Наукова література:

44. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. – К.: К.І.С., 2015.

45. Бєлова Ю. Умови дійсності згоди на обробку персональних даних / Ю. Бєлова // Підприємництво, господарство і право. — 2017. —№ 11. — Р. 14–18.

46. Брижко В. М. Про приведення інформаційного законодавства України у відповідність до положень європейського права / В Брижко // Правова інформатика. - № 1(25)/2010. – С. 14-22.

47. Брижко В. М. Про упорядкування законодавства України із захисту персональних даних / В. М. Брижко // Правова інформатика. – 2008. – № 1(17). – С. 20-34.

48. Кохановська О.В. До питання про захист персональних даних в Україні // Вісник Верховного Суду України. - 2011. - № 6. - С. 28-33. URL: http://nbuv.gov.ua/UJRN/vvsu_2011_6_8.

49. Пазюк А. В. Міжнародно-правовий захист права людини на приватність персоніфікованої інформації : автореф. дис. на здобуття наук. ступеня канд. юр. наук : спец. 12.00.11 "міжнародне право" / Пазюк Андрій Валерійович – Київ, 2004. – 13 с.

50. Пилипчук, В. Г.. Реформування і розвиток системи захисту персональних даних в Україні [Текст] / Пилипчук В. Г., Брижко В. М. // Інформація і право : наук. журн.. - 2017. - N 3. - С. 5-21.

51. Посібник з європейського права у сфері захисту персональних даних. — К.: К.І.С., 2015.

52. Право фізичної особи на власні персональні дані в цивільному праві України : автореф. дис. ... канд. юрид. наук : 12.00.03 / О. А. Дмитренко; Акад. прав. наук України, НДІ приват. права і підприємництва. - К., 2010. - 19 с.

53. A Comparative Analysis in Relation to Informational Self-Determination and Privacy: The Icelandic Health Sector Database Decision and The German Census Act Decision. 2007. URL: https://www.duo.uio.no/bitstream/handle/10852/21511/8003.pdf?sequence=1.

54. Ajana, Btihaj. (2009). Reinventing data protection? Springer Netherlands.

55. Brownsword R. (2009) Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality. In: Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S. (eds) Reinventing Data Protection? Springer, Dordrecht.

56. Hermstruwer, Yoan, ‘Contracting around Privacy: The (Behavioral) Law and Economics of Consent and Big Datamics of Consent and Big Data’, JlPlTEC, 8 (2017), 9–26.

57. Holland, H. Brian, Privacy Paradox 2.0 (April 4, 2010). Widener Law Journal, Forthcoming. URL: https://ssrn.com/abstract=1584443.

58. Hutton L, Henderson T. "I didn't sign up for this!": Informed consent in social network research. In Proceedings of the 9th International AAAI Conference on Web and Social Media (ICWSM). 2015. p. 178-187.

59. Jammet Adrien, The Evolution of EU Law on the Protection of Personal Data, Centre for European Law and Legal Studies (CELLS) Online Papers (2014) URL: http://ssrn.com/abstract=2501417.

60. Kosta, E. (2011). Unravelling consent in European data protection legislation - a prospective study on consent in electronic communications.

61. Lambrecht, A. (2013) The Economics of Pricing Services Online. In S.N. Surlauf & L.E. Blume (Eds.), The New Palgrave Dictionary of Economics.

62. Mayer-Schönberger, V. C. K. (2013). Big data: a revolution that will transform how we live, work, and think. Boston: Houghton Mifflin Harcourt: 173-175.

63. McDonald, A. M., & Cranor, L.F. (2008). The Cost of Reading Privacy Policies. A Journal of Law and Policy for the Information Society. 4, 541.

64. Misek Jakub, ‘Consent to Personal Data Processing - The Panacea or the Dead End’, Masaryk University Journal of Law and Technology, 8.1 (2014), 69–83.

65. Mozer J. Consent and contract under GDPR – Prohibition of consent bundling. URL: https://datareality.eu/consent-contract-gdpr-bundling/.

66. Murumaa-Mengel, Maria & Laas-Mikko, Katrin & Pruulmann-Vengerfeldt, Pille. (2015). “I Have Nothing to Hide”: A Coping Strategy in a Risk Society.URL: https://www.researchgate.net/publication/283713758_I_Have_Nothing_to_Hide_A_Coping_Strategy_in_a_Risk_Society.

67. Reidenberg, Joel & D. Breaux, Travis & Cranor, Lorrie & French, Brian & Grannis, Amanda & T. Graves, James & Liu, Fei & M. McDonald, Aleecia & B. Norton, Thomas & Ramanath, Rohan & Cameron Russell, N & Sadeh, Norman & Schaub, Florian. (2014). Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding.

68. Rikke Frank Joergensen, The unbearable lightness of user consent, The Danish Institute for Human Rights, Copenhagen, Denmark, Published on: 21 Oct 2014.

69. Schermer, Bart Willem and Custers, Bart and van der Hof, Simone, The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection (February 25, 2014). Ethics and Information Technology, Forthcoming. URL: https://ssrn.com/abstract=2412418.

70. Solove D. J. Privacy self-management and the consent dilemma / D. J. Solove // Harvard Law Review. — 2013. — Vol. 126, No. 7. — P. 1880–1903.

71. Solove, Daniel J., A Brief History of Information Privacy Law. Proskauer On Privacy, PLI, 2016; GWU Law School Public Law Research Paper No. 215. URL: https://ssrn.com/abstract=914271.

72. Spears V. P. The case that started it all: Roberson v. the Rochester folding box company / V. P. Spears // Privacy & Data Security Law Journal. — 2008. — Vol. 11. — P. 1043–1050.

73. Tommaso Scannicchio PhD Thesis Google's Faustian Bargain: Contested Issues On The Interface Between Privacy And Contract. URL: https://uniba-it.academia.edu/TommasoScannicchio/Thesis-Chapters.

74. van Dijck, J. (2014). Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology. Surveillance & Society. 12(2), 199-208.

75. Warren S. D., Brandeis L. D. The Right to Privacy // Harvard Law Review. — 1890. — Vol. 4. — P. 193–220.

76. Wendler, D. (1996). Deception in Medical and Behavioral Research: Is It Ever Acceptable? The Milbank Quarterly. 74 (1), 87-114.

77. Yeung, Karen, '"Hypernudge": Big Data as a Mode of Regulation by Design'', Information, Communication & Society, 1 (2016), 31.

78. Zarsky, Tal Z., ‘Incompatible: The GDPR in the Age of Big Data’, Seton Hall Law Review, 47 (2017), 995–1020.

79. Zuiderveen Borgesius, Frederik, Consent to Behavioral Targeting in European Law - What are the Policy Implications of Insights from Behavioral Economics? (July 27, 2013). Amsterdam Law School Research Paper No. 2013-43. URL: https://ssrn.com/abstract=2300969.

Інші джерела:

80. Політика конфіденційності Google. URL: https://policies.google.com/privacy?hl=uk#infocollect.

81. Facebook не має вимагати справжні імена при реєстрації — суд Берліна. «Центр інформації про права людини». URL: https://humanrights.org.ua/material/facebook_ne_maje_vimagati_spravzhni_imena_pri_rejestraciji__sud_berlina_postanoviv_shho_.

82. 7,500 Online Shoppers Unknowingly Sold Their Souls. FoxNews. URL: https://www.foxnews.com/tech/7500-online-shoppers-unknowingly-sold-their-souls.

83. Adequacy of the protection of personal data in non-EU countries. European Commission. URL: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

84. Complaint under article 77(1) GDPR on Google to CNIL (France). URL: https://noyb.eu/wp-content/uploads/2018/05/complaint-android.pdf.

85. GDPR: noyb.eu filed four complaints over “forced consent” against Google, Instagram, WhatsApp and Facebook URL: https://noyb.eu/4complaints/.

86. German court issues important judgment on consent and transparency in Facebook case. Technology Law Dispatch. URL: https://www.technologylawdispatch.com/2018/03/privacy-data-protection/german-court-issues-important-judgment-on-consent-and-transparency-in-facebook-case/.

87. Guidelines for obtaining meaningful consent, Canada, 2018. URL: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/.

88. Information Commissioner's Office, 'Lawful Basis for Processing Consent', 2018.

89. Insurance policies tracking fitness, diet, sleep have alarming discrimination and privacy risks, experts say. URL: https://www.sbs.com.au/news/the-feed/insurance-policies-tracking-fitness-diet-sleep-have-alarming-discrimination-and-privacy-risks-experts-say.

90. Privacy Glossary URL: https://www.gov.il/he/Departments/Guides/glossary?chapterIndex=1.

91. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, The Guardian, 27.03.2018. URL: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

92. TRUSTe, GB Consumer Privacy Index, 2016.

93. What happens when life insurance companies track fitness data? The Verge. URL: https://www.theverge.com/2018/9/26/17905390/john-hancock-life-insurance-fitness-tracker-wearables-science-health.