АНАЛІЗ СУДОВОЇ ПРАКТИКИ ЩОДО ЗАСТОСУВАННЯ ЗАКОНОДАВСТВА УКРАЇНИ ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

Володимир Венгер
Андрій Кошман
Олександр Шевчук

2021

Європейський Союз та Рада Європи працюють разом задля посилення операційної спроможності Омбудсмана у захисті прав людини

Фінансується Європейським Союзом та Радою Європи

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Впроваджується Радою Європи

АНАЛІЗ СУДОВОЇ ПРАКТИКИ ЩОДО ЗАСТОСУВАННЯ ЗАКОНОДАВСТВА УКРАЇНИ ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

ПІДГОТУВАЛИ
національні експерти Спільного проєкту Європейського Союзу та Ради Європи «Європейський Союз та Рада Європи працюють разом задля посилення операційної спроможності Омбудсмана у захисті прав людини»
Володимир ВЕНГЕР
Андрій КОШМАН
Олександр ШЕВЧУК

Київ – 2021

Ця публікація виготовлена за фінансової підтримки Європейського Союзу та Ради Європи. Погляди, викладені в цьому документі, не відображають офіційну позицію Європейського Союзу та Ради Європи.

Верстка, дизайн обкладинки та друк: «К.І.С.»

Фото: © Shutterstock

Council of Europe Publishing
F-67075 Strasbourg Cedex
(http://book.coe.int)

ЗМІСТ

ВСТУП

Захист персональних даних в Україні – відносно нова сфера правового регулювання, що перебуває на етапі становлення та потребує досить ретельного аналізу не тільки відповідних міжнародних стандартів, але й національної практики нормозастосування.

Сьогодні в Україні напрацьовано досить великий досвід щодо аналізу основних недоліків та проблем імплементації міжнародних стандартів у сфері захисту персональних даних. За підтримки міжнародних партнерів проведено низку прикладних досліджень, як комплексних, так і доволі точкових, щодо ефективності застосування приписів Закону України «Про захист персональних даних». Разом з тим досі нема системних аналітичних напрацювань щодо судової практики в цій сфері.

Цей аналіз має на меті зробити перший крок у цьому напрямку та запропонувати загальний огляд основних напрямків і ключових тенденцій застосування українськими судами загальної юрисдикції Закону України «Про захист персональних даних». Предметом дослідження є аналіз рішень судів різних юрисдикцій та інстанцій, що істотно ускладнює методологію та засади проведення аналізу та узагальнення його результатів. Адже особливості захисту персональних даних у, наприклад, провадженнях в цивільних справах та в кримінальних провадженнях мають надзвичайно багато відмінностей.

Водночас автори свідомо залишили таке відносно масштабне охоплення для аналізу, щоб сконцентрувати дослідження саме на персональних даних. Деякі питання, що могли б бути набагато детальніше представлені крізь призму спеціального законодавства у відповідній сфері, залишилися поза основним фокусом. Це зроблено задля чіткішого виокремлення векторів застосування законодавства про захист персональних даних, його розуміння і сприйняття суддями та іншими учасниками судових процесів, труднощів узгодження приписів законів із підзаконними актами, а також спрямованості відповідної адміністративної (управлінської) практики органів державної влади та органів місцевого самоврядування.

Для проведення цього дослідження експерти опрацювали близько 10 000 судових рішень, з яких для ретельного дослідження дібрано понад 500, на частину з них зроблено прямі посилання в тексті аналізу. Усі рішення добиралися з Єдиного державного реєстру судових рішень з використанням різних критеріїв та методів пошуку. Водночас це дослідження не має на меті запропонувати статистично точний аналіз, що навряд чи можливо, щонайменше з огляду на постійно змінювану судову практику та брак достатньої кількості сформованих правових позицій у цій сфері. Автори намагалися представити основні тенденції розвитку судової практики у сфері гарантування захисту персональних даних в Україні.

Виокремлені тенденції обумовили й особливу структуру цього аналізу. Традиційно в Україні дослідження щодо захисту персональних даних структуруються відповідно до системи Закону України «Про захист персональних даних» або ж на основі міжнародних документів (зазвичай за зразком аналітичних матеріалів). У цьому аналізі зроблено спробу структурувати матеріал відповідно до принципів, що мають діяти у сфері захисту персональних даних. Перелік принципів насправді нормативно не визначений. Адже приписи Закону України «Про захист персональних даних» тільки визначають зміст окремих принципів у цій сфері, але їх не називають, а тим більше не формують у єдину систему. Аналіз міжнародних стандартів та матеріалів, підготовлених для їх представлення, також дає підстави для різного тлумачення принципів захисту персональних даних.

За таких обставин, автори аналізу, опираючись на попередні дослідження, що велися за підтримки Ради Європи[1], сформулювали узагальнений каталог принципів захисту персональних даних, що може бути використаний в українських політико-правових реаліях. До переліку увійшли такі принципи: законність, цілеспрямованість, пропорційність, точність, підзвітність, захист персональних даних. Кожен з цих принципів має додаткові складники, які глибше розкривають їх зміст та спрямованість регулювання.

Для більш глибокого розуміння природи походження та практичного застосування положень Закону України «Про захист персональних даних» важливо проаналізувати саме принципи обробки персональних даних. Виокремлення принципів, а не окремих сфер регулювання, має також вкрай важливе світоглядне значення. Адже через недосконалість законодавчого регулювання подолання колізій і прогалин, а також «вихід за межі» закону з метою захисту прав людини може відбуватися ефективно тільки через принципи права. Однак, попри наявність принципів обробки персональних даних, вони практично не представлені в національній судовій практиці, на них не опираються адвокати при формулюванні позовних вимог (принаймні цього не прослідковується в проаналізованих судових рішень). Саме тому автори при формуванні структури цього аналізу спиралися на позицію, що елементи захисту персональних даних (наприклад, підстави обробки персональних даних та права суб'єктів персональних даних) це фактично логічне продовження, розвиток та деталізація принципів і повинні тлумачитися в їх світлі[2]. Тому представлений тут матеріал структурований відповідно до змісту означених вище принципів та поширення їх використання в судовій практиці..

Тут також слід зазначити, що, на жаль, далеко не всі вимоги міжнародних стандартів і навіть не всі приписи національного законодавства вдалося проілюструвати через судову практику, бо вона поки що украй обмежена. Однак, цей аналіз, як певне узагальнення судової практики, містить бачення суддів щодо алгоритмів застосування тих чи інших норм права в конкретних практичних ситуаціях. Таким чином, аналіз виконує інформативно-орієнтаційну функцію для суддів та сприятиме глибшому і правильному застосуванню судами законодавства про захист персональних даних.

Судовий захист є одним із основоположних механізмів побудови зручного та справедливого режиму захисту персональних даних. Спільно із якісною правовою базою та належною адміністративною практикою, реальний судовий захист прав суб'єктів персональних даних є вирішальним для визнання на міжнародному рівні України як держави, яка забезпечує належний рівень захисту персональних даних. Варто відзначити, що національна судова практика захисту персональних даних відрізняється від розвинених юрисдикцій значно меншою кількістю судових справ, що в жодному разі не означає меншу кількість порушень відповідного законодавства. Невелика кількість судових справ є наслідком низької правової обізнаності громадян щодо власних персональних даних та механізмів їх захисту.

З огляду на зазначене, даний аналіз сприятиме забезпеченню конституційного права на повагу до приватного життя через підвищення рівня правової обізнаності громадян щодо можливостей судового захисту персональних даних.

1. Див. Посібник з європейського права у сфері захисту персональних даних. URL: https://rm.coe.int/16805966a8.
2. Захист персональних даних: правове регулювання та практичні аспекти. Науково-практичний посібник/ М. Бем та І. Городиський/ Рада Європи, 2021. С. 44. URL: https://rm.coe.int/handbook-pers-data-protect-2021-web/1680a37a69.

ЗАКОННІСТЬ І СПРАВЕДЛИВІСТЬ

Принцип законності у сфері захисту персональних даних означає вимогу наявності якісного нормативного регулювання правовідносин щодо збирання, обробки та використання персональних даних. Цей принцип спрямований насамперед на суб'єктів здійснення публічної влади для чіткого визначення їх повноважень та допустимих меж обмеження прав людини.

Разом з тим принцип законності має поширюватися і на приватних суб'єктів правовідносин. Саме тому тут пропонується його дещо уточнене формулювання з додаванням поняття «справедливість».

У державах з добре розвиненими демократичними традиціями розуміння «правового закону», як справедливого і безумовно спрямованого на захист прав людини, традиційне і не піддається сумнівові. В українській практиці нормозастосування, на жаль, досі переважають пострадянські підходи до праворозуміння із застосуванням жорстких позитивістських аргументів при оцінюванні якості закону і мети його регулювання. Саме тому в цьому розділі принцип законності та справедливості буде представлений за такими його складовими елементами:

- передбаченість законом – це класичне розуміння законності, коли йдеться про те, що закон (а не підзаконний чи інший акт) – основна підстава для обмеження прав людини, а у проаналізованій сфері саме закон – інструмент визначення меж втручання в приватне життя; будь-яке втручання повинно базуватися на приписах закону і бути передбачуваним;
- якість закону – це складник принципу законності, що коректніше виражається через юридичну визначеність як елемент верховенства права; тут ідеться про те, що регулювання має вестися з чітким розумінням меж нормативного втручання держави в реалізацію прав людини; якість означає також справедливість регулювання, обґрунтованість глибини втручання в приватне життя людини на основі ухваленого закону.

Передбачено законом

Принцип законності має особливо чіткі форми виразу щодо діяльності суб'єктів владних повноважень. Тут повинна безумовно діяти формула припису частини другої статті 19 Конституції України, відповідно до якої органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України. Дотримання цієї вимоги особливо важливе, коли йдеться про обмеження прав людини, зокрема, про втручання в приватне життя особи та захист персональних даних. Тут показовою може бути справа № 804/4069/17, у якій Верховний Суд досить чітко наголосив на необхідності вкрай чіткого застосування формули «якщо не заборонено, то дозволено».

У цій справі йшлося про оскарження позивачем (фізичною особою) дій керівника органу, де вона раніше працювала (роботодавця), в частині направлення вже після її звільнення запитів про надання інформації щодо стану здоров'я позивачки. У таких запитах були відкрито зазначені, а відповідно й розголошені персональні дані позивачки, а саме: місце проживання та дата

народження. Суд першої[3] інстанції задовольнив позов частково і визнав такі дії відповідача протиправними. Проте суд апеляційної інстанції не погодився з таким рішенням і, скасувавши рішення суду першої інстанції, ухвалив нове, яким у задоволенні позовних вимог відмовив, так це мотивуючи:

«… персональні дані працівника, які містяться в паспорті або документі, що посвідчує особу, в трудовій книжці, документі про освіту (спеціальність, кваліфікацію), документі про стан здоров'я та інших документах, які він подав при укладенні трудового договору, обробляються володільцем бази[4] персональних даних на підставі статті 24 Кодексу законів про працю України виключно для здійснення повноважень володільця бази персональних даних у сфері правовідносин, які виникли в нього з працівником на підставі трудового договору (контракту).

Суд апеляційної інстанції враховує, що керівником апарату Софіївського районного суду Дніпропетровської області не витребовувалася інформація щодо безпосереднього стану здоров'я або діагнозу можливого захворювання позивача, спеціалізації лікаря.

З урахуванням викладеного та фактичних обставин справи, суд апеляційної інстанції доходить висновку що, керівник апарату Софіївського районного суду Дніпропетровської області під час здійснення запиту до медичних закладів щодо ОСОБА_1 діяла в службових інтересах, в межах посадових повноважень та не порушила права та охоронювані законом інтереси позивача в сфері захисту персональних даних»[5].

З цієї аргументації видно, зокрема, що суд апеляційної інстанції сконцентрував увагу більше на змісті запитів від колишнього роботодавця, а не на самому факті направлення запитів після припинення трудових правовідносин, меті таких дій, а головне – необхідності/обґрунтованості внесення персональних даних до таких запитів. З огляду на це, Верховний Суд не погодився з такою позицією, підтримавши аргументацію суду першої інстанції. Зокрема, Суд зазначив:

«31. Таким чином, лише фізична особа, якої стосується конфіденційна інформація, відповідно до конституційного та законодавчого регулювання права особи на збирання, зберігання, використання та поширення конфіденційної інформації має право вільно, на власний розсуд визначати порядок ознайомлення з нею інших осіб, держави та органів місцевого самоврядування, а також право на збереження її у таємниці…

37. Верховний Суд зазначає, що виконання службових обов'язків, не дозволяє посадовій особі діяти в межах «якщо не заборонено, то дозволено», оскільки недотримання чітко визначених повноважень, або відповідних процедурних правил, є свавіллям з боку уповноважених осіб»[6].

Така правова позиція додатково підтверджує вимогу максимально чіткого та безумовного дотримання органами державної влади, органами місцевого самоврядування, їхніми посадовими та службовими особами вимог закону. Суб'єкти владних повноважень повинні мати мінімальну свободу розсуду, коли йдеться про обмеження прав людини. При цьому за дотриманням меж такого розсуду має також вестися регулярний та ефективний контроль.

---

3. Постанова Дніпропетровського окружного адміністративного суду у справі № 804/4069/17 від 27 вересня 2017 року: https://reyestr.court.gov.ua/Review/70592868.
4. Додатково слід зазначити, що у тексті Закону України «Про захист персональних даних» слова «володілець бази персональних даних» і «розпорядник бази персональних даних» у всіх відмінках і числах замінено відповідно словами «володілець персональних даних» і «розпорядник персональних даних» у відповідному відмінку і числі згідно із Законом № 5491-VI від 20.11.2012 р.
5. Постанова Дніпропетровського апеляційного адміністративного суду у справі № 804/4069/17 від 18 січня 2018 року: https://reyestr.court.gov.ua/Review/72000379.
6. Постанова Верховного Суду у справі №804/4069/17 від 16 квітня 2020 року: https://reyestr.court.gov.ua/Review/88815240.

Збір персональних даних має вестися відповідно до вимог закону. Закон України «Про захист персональних даних» передбачає, що приписи щодо заборони обробки чутливих персональних даних (про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях та професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних) не застосовуються, якщо обробка персональних даних необхідна для цілей 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.

При цьому деталізація відповідних положень на рівні закону чи навіть підзаконних актів далеко не завжди достатньо точна та конкретна. Суб'єкти надання медичних послуг доволі часто вдаються до збирання додаткової інформації про особу пацієнта, а в окремих випадках і про третіх осіб (членів сім'ї, родичів, близьких осіб), звернення до яких може бути необхідним в екстрених ситуаціях.

Як приклад, справа № 592/12477/20, яку розглядали Ковпаківський районний суд м. Сум та Сумський апеляційний суд у частині зобов'язання Комунального некомерційного підприємства Сумської обласної ради «Сумська обласна клінічна лікарня» знищити всі персональні дані третіх осіб та всі номери телефонів, які містяться в медичній справі фізичної особи (позивача). Суть справи полягає в тому, що пацієнт в момент госпіталізації подав низку персональних даних не тільки щодо себе, але й щодо третіх осіб (матері і брата). Згодом звернувся з вимогою видалити персональні дані цих третіх осіб, у задоволенні такої вимоги йому було відмовлено. Суди першої та апеляційної інстанції проаналізували відповідне законодавство і визначили, що персональні дані стосовно позивача збирали працівники закладу з метою надання медичної допомоги. Зокрема відомості вносили в Медичну карту стаціонарного хворого форми №003/о та форму 003-6/о. При цьому досить чітко встановлено, що ані спеціальним законом, але підзаконними актами не передбачено обов'язкової вимоги у відповідній ситуації збирати персональні дані третіх осіб. Зокрема, суд першої інстанції встановив:

«Наказом Міністерства охорони здоров'я України 14.02.2012 № 110 затверджено форму 003/о «Медична карта стаціонарного хворого № » та Інструкцію її заповнення. Згідно цього нормативного акту форма та Інструкція передбачають внесення конференційної інформації про пацієнта, прізвище, ім'я, по батькові хворого, стать (чоловіча, жіноча), дата народження (число, місяць, рік), вік (кількість повних років, для дітей: до 1-го року – місяців; до 1-го місяця – днів), назва та номер документа, що посвідчує особу, код країни, громадянином якої є хворий, постійне місце проживання/перебування. Строк зберігання форми № 003/о – 25 років. Втім зазначені документи не передбачають внесення відомостей про номер телефону та імен родичів і їх телефонів»[7]. При цьому ані суд першої інстанції, ані суд апеляційної інстанції не дали правової оцінки законності підстав збирання відповідної інформації. Ба більше, у Постанові апеляційного суду зазначено:

«Щодо внесеної до медичної карти стаціонарного хворого інформації про матір та брата позивача, а також їх номерів телефону, то ОСОБА_1 не є суб'єктом цих персональних даних в розумінні Закону України «Про захист персональних даних», а тому не має права пред'являти вимоги про їх вилучення або знищення.

7. Рішення Ковпаківського районного суду м. Сум у справі № 592/12477/20 від 05 лютого 2021 року: https://reyestr.court.gov.ua/Review/94684114#

Позивачем у своїх доводах взагалі не обґрунтовано, яким чином зазначення вказаної персональної інформації щодо третіх осіб в медичній документації впливає на його законні права та інтереси»[8].

Щодо національного законодавства цікавим є приклад, коли суди, визначаючи межі обмеження прав людини в сфері захисту персональних даних посилаються не тільки на національне законодавство, але й міжнародні стандарти, які не можуть безпосередньо застосовуватися в Україні (згоду на обов'язковість не надано Верховною Радою України, не ратифіковано). Наприклад, документи Європейського Союзу, зокрема Хартія основних прав Європейського Союзу (2000/С 364/01)[9]. Бажання застосувати в аргументації судового рішення як додатковий (але не основний) аргумент документи ЄС як зразок підвищених стандартів у сфері персональних даних загалом можу бути прийнятним. Проте тоді коректнішим було б посилання на спеціальні акти, наприклад на 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)[10]. Все ж за таких обставин доцільнішим було б посилання на спеціальні акти, згоду на обов'язковість яких надала Верховна Рада України у відповідній сфері правового регулювання, зокрема на Конвенцію про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних[11] та практику її застосування, а вже згодом для додаткової аргументації можливе використання й інших міжнародних актів.

В контексті аналізу судової практики важливе не тільки належне регулювання законом правовідносин у тій чи іншій сфері, але й коректне застосування приписів відповідних законів судами. Як приклад, у справі № 950/3050/19 Верховний Суд встановив, що через неправильне розуміння законодавства про захист персональних даних, а також законодавства про нотаріат суди першої та апеляційної інстанції фактично зобов'язували нотаріуса допустити неправомірне поширення персональних даних та порушення нотаріальної таємниці.

У цій справі позивач (фізична особа) оскаржував відмову приватного нотаріуса надати дозвіл на ознайомлення та фотографування матеріалів спадкової справи після смерті його матері. Суд першої інстанції[12] та суд апеляційної інстанції[13] зайняли таку позицію:

«…ОСОБА_1 , як особа, на підставі заяви якої приватним нотаріусом було заведено спадкову справу та вчинялися відповідні нотаріальні дії, має право на ознайомлення з матеріалами спадкової справи…

…надаючи заявнику на ознайомлення матеріали спадкової справи приватний нотаріус не позбавлений можливості вжити заходів для захисту персональних даних інших осіб, які не є учасниками нотаріальної дії та для захисту отриманої при оформленні спадкової справи інформації, що не стосується прав заявника на отримання спадщини після смерті його матері»[14].

8. Постанова Сумського апеляційного суду у справі № 592/12477/20 від 30 березня 2021 року: https://reyestr.court.gov.ua/Review/95893145.
9. Див., наприклад, Постанову Верховного Суду у справі № 760/8719/17 від 04 грудня 2019 року: https://reyestr.court.gov.ua/Review/86162369.
10. 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): https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679.
11. Конвенція про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 р. № 108: https://zakon.rada.gov.ua/laws/show/994_326.
12. Рішення Лебединського районного суду Сумської області у справі № 950/3050/19 від 17 лютого 2020 року: https://reyestr.court.gov.ua/Review/87787555.
13. Постанова Сумського апеляційного суду у справі № 950/3050/19 від 09 квітня 2020 року: https://reyestr.court.gov.ua/Review/88734897.
14. Текст з Постанови Сумського апеляційного суду у справі № 950/3050/19 від 09 квітня 2020 року: https://reyestr.court.gov.ua/Review/88734897.

Верховний Суд скасувавши відповідні рішення судів нижчих інстанцій, серед іншого, зазначив:

«Суди попередніх інстанцій зазначених положень чинного законодавства не урахували та не звернули увагу, що у матеріалах спадкової справи, крім відомостей, наданих позивачем як особою, за дорученням якої вчинялися нотаріальні дії, можуть знаходитися витяги із закритих для загального доступу Реєстрів та інші документи, отримані нотаріусом при здійсненні дій з пошуку інформації про зареєстровані речові права спадкодавця та їх обтяження, у тому числі документи, що містять персональні дані інших спадкоємців, а також персональні дані осіб з тотожними із спадкодавцем відомостями про особу, які безпосередньо не стосуються позивача як учасника нотаріальної дії, та не можуть бути розголошені нотаріусом в силу положень частин другої та четвертої статті 8 Закону України «Про нотаріат».

Викладені у відзиві ОСОБА_1 аргументи на спростування доводів касаційної скарги, зокрема, що у приватного нотаріуса Жураховського Д. В. не було правових підстав для відмови у наданні йому спадкової справи для ознайомлення, оскільки вона не містила відомостей про персональні дані інших осіб, а персональні дані його сестри не є для нього конфіденційною інформацією, оскільки вона відмовилась від спадщини, є неспроможними, оскільки статті 5, 8 Закону України «Про нотаріат» покладають на нотаріуса обов'язок зберігати нотаріальну таємницю, навіть якщо їх діяльність обмежується наданням правової допомоги чи ознайомленням з документами і нотаріальна дія або дія, яка прирівнюється до нотаріальної, не вчинялася.

Узагальнюючи наведене, обґрунтованими є доводи касаційної скарги про неправильне застосування судами попередніх інстанцій частини сьомої статті 8 Закону України «Про нотаріат», що призвело до помилкового висновку про задоволення позовних вимог ОСОБА_1 в частині визнання протиправними дій приватного нотаріуса щодо ненадання матеріалів спадкової справи на ознайомлення, та зобов'язання його вчинити зазначені дії»[15].

Отже, вкрай важливе є забезпечення однакового та змістовно єдиного тлумачення судами законодавства про захист персональних даних та, як наслідок, єдність відповідної судової практики.

Категорія «Спори, що виникають із договорів позики, кредиту, банківського вкладу» найпоширеніша серед судових справ, що стосуються захисту персональних даних із застосування Закону України «Про захист персональних даних». Переважно звернення в суд відбуваються у зв'язку з вимогою визнати договір недійсним повністю чи в частині, бо були порушені її права як споживача. Найчастіше такі справи стосуються кредитних договорів, особливо так званих «швидких кредитів», де умови кредитування зазвичай вкрай невигідні для споживачів таких фінансових послуг.

При цьому позивачі обґрунтовують свої вимоги та вказують на суперечність умов договору законодавству, зокрема, але не виключно, Цивільному кодексові України, законам «Про захист прав споживачів» та «Про захист персональних даних». Щодо захисту персональних даних, то на підставі порушення вимог щодо отримання згоди на обробку персональних даних позивачі намагаються визнати кредитні договори недійсними.

Тут слід зауважити, що в значній кількості проаналізованих рішень посилання на порушення законодавства про захист персональних даних були вкрай необґрунтовані, а в окремих випадках й зовсім їх нема. Власне, суди й звертають на це увагу, наприклад, у такому форматі:

«Відсутність у кредитному договорі пункту щодо пред'явлення вимоги володільцю персональних даних із запереченням проти обробки своїх персональних даних та/або відкликання згоди на обробку персональних даних не є підставою для визнання спірного пункту договору недійсним.

15. Постанова Верховного Суду у справі № 950/3050/19 від 03 березня 2021 року: https://reyestr.court.gov.ua/Review/96071002.

Крім того, відкликання згоди чи заперечення проти обробки своїх персональних даних можливе лише стосовно майбутньої обробки персональних даних, але не тих даних, які вже були оброблені. Рішення та процеси, які були здійснені під час обробки персональних даних, не можуть бути анульованими. А тому твердження позивача щодо порушення відповідачем вимог Закону України «Про захист персональних даних» не знайшли свого підтвердження під час розгляду справи.

Суд вважає, що під час укладення спірного договору дотримано вимог Закону України «Про захист персональних даних», а тому вимога позивача про визнання […] договору до задоволення не підлягає»[16].

У такій категорії справ суди також досить часто спростовують поширену позицію, про те, що надання згоди на обробку персональних даних – окремий правочин і потребує додаткового самостійного оформлення. Суди зазвичай зазначають таке:

«Твердження позивача щодо обов'язкового укладення правочину для надання згоди для обробки персональних даних спростовуються самим Законом України «Про захист персональних даних», який таких вимог не містить»[17].

Кредитні договори такого типу також часто містять положення про безстроковість та безвідкличність згоди на обробку персональних даних, що суперечить вимогам закону. При цьому, суди доволі часто визнають договори недійсними тільки в цій частині, відмовляючи в задоволенні інших позовних вимог (насамперед у частині виконання основного зобов'язання за кредитним договором). Наприклад, Кілійський районний суд Одеської області при розгляді однієї зі справ у такій категорій визначив:

«…Таким чином, зважаючи на підписання позивачем Договору він дав згоду на обробку його персональних даних. Однак така згода надається виключно до сформульованої мети їх обробки, як зазначено у п. 6.4 Договору.

Водночас, згідно п. 11 ч. 2 ст. 8 Закону України «Про захист персональних даних» № 2297-VI від 1 червня 2010 року суб'єкт персональних даних має право відкликати згоду на обробку персональних даних.

А тому положення п. 6.4 Договору про те, що позичальник надає свою саме безвідкличну згоду на обробку його персональних даних суперечать вищенаведеним вимогам Закону. Відповідно за змістом положень ч. 1 ст.203, ч. 1 ст. 215 ЦК України є недійсними. Однак спірний правочин був би вчинений і без включення до нього такого положення, а тому недійсність такого положення не має наслідком недійсності інших його частин і правочину в цілому»[18].

Разом з тим є й приклади, де в таких ситуаціях аргументація суду щодо порушення законодавства про захист персональних даних стає додатковою до встановлених порушень цивільного та/або фінансового законодавства і спричиняє визнання відповідних кредитних договорів недійсними не тільки в частині порушення законодавства про персональні дані, але й щодо змісту

16. Рішення Монастирищенського районного суду Черкаської області у справі № 702/279/21 від 31.05.2021 року: https://reyestr.court.gov.ua/Review/97261860.
17. Рішення Новозаводського районного суду м. Чернігова у справі № 748/1374/20 від 01 жовтня 2020 року: https://reyestr.court.gov.ua/Review/92062236.
18. Рішення Кілійського районного суду Одеської області у справі № 502/1011/20 від 15 лютого 2021 року: https://reyestr.court.gov.ua/Review/94881392.

фінансових правовідносин[19]. Хоч згодом відповідна аргументація може скасувати суд апеляційної інстанції[20] або ж підтвердити навіть Верховний Суд[21].

Проте найпоширеніші рішення, коли суд не розглядає в таких категоріях справ[22] порушення законодавства про захист персональних даних, зокрема, з міркувань, що вони не порушують істотних умов відповідних договорів[23]. Наприклад, Жовтневий районний суд Миколаївської області у справі з відповідної категорії зазначив: «Посилання на порушення при використанні персональних даних не є обставиною, яка тягне за собою скасування договору або визнання його недійсним. Захист права позивача у цьому разі, у разі наявності такого порушення, може бути реалізоване іншим видом судочинства, зокрема, кримінальним чи адміністративним»[24]. Відповідну позицію у цій справі підтримали суди апеляційної та касаційної інстанції.

Межі та спосіб застосування положень Закону України «Про захист персональних даних» суди інколи визначають не стільки з огляду на системне їх тлумачення, скільки беручи до уваги, зокрема, інформаційні листи, роз'яснення чи інші документи, нормативна природа яких не очевидна. Доволі поширене посилання судів[25] на лист Міністерства юстиції щодо відкликання згоди на обробку персональних даних[26]. В окремих випадках суди посилаються на лист Міністерства юстиції майже як на самостійне джерело права[27]. Суди зазвичай дослівно повторюють у своїх рішеннях аргументи (текст) відповідного листа, чим фактично створюють нову норму та спрямовують правозастосування в досить звуженому напрямку.

Зокрема, за такого підходу відкликання згоди можливе лише стосовно майбутньої обробки персональних даних, але не тих даних, які вже були оброблені; рішення та процеси, які відбулися під час обробки персональних даних, не можуть бути анульованими. Хоч з відповідністю саме такого тлумачення до приписів статей 8 та 11 Закону України «Про захист персональних даних» можна погодитися далеко не в усіх випадках. Очевидно, відповідні питання мали б бути ретельніше врегульованими в тексті закону.

У судовій практиці можна знайти й цікаві приклади викривленого тлумачення органами державної влади законодавства про захист персональних даних у ситуаціях притягнення до адміністративної відповідальності посадових і службових осіб. Як приклад, у справі № П/811/1192/14 Державна фінансова інспекція в Кіровоградській області (позивач) звернулася з позовом до Служби

19. Див., наприклад, Рішення Цюрупинського районного суду Херсонської області у справі №664/1261/16-ц від 08 лютого 2017 року: https://reyestr.court.gov.ua/Review/64605811; Рішення Броварського міськрайонного суду Київської області у справі № 361/3511/20 від 03 листопада 2020 року: https://reyestr.court.gov.ua/Review/93968247.
20. Постанова Київського апеляційного суду у справі № 361/3511/20 від 15 липня 2021 року: https://reyestr.court.gov.ua/Review/98593168.
21. Див., наприклад, Постанова Верховного Суду у справі № 664/1261/16-ц від 06 грудня 2019 року: https://reyestr.court.gov.ua/Review/86205971; Постанова Верховного Суду у справі № 752/10234/16-ц від 16 жовтня 2019 року: https://reyestr.court.gov.ua/Review/85135423.
22. Див., наприклад, Рішення Голосіївського районного суду м. Києва у справі № 752/10234/16-ц від 05 грудня 2016 року: https://reyestr.court.gov.ua/Review/63816244; Рішення Корсунь-Шевченківського районного суду Черкаської області у справі № 754/6091/18 від 05 березня 2019 року: https://reyestr.court.gov.ua/Review/80550371 та ін.
23. Див., наприклад, Постанови Верховного Суду у справі № 607/2398/16-ц від 12 листопада 2018 року: https://reyestr.court.gov.ua/Review/77910787; у справі № 477/991/15-ц від 11 грудня 2018 року: https://reyestr.court.gov.ua/Review/78495991; у справі № 524/5035/16 від 13 червня 2019 року: https://reyestr.court.gov.ua/Review/82420406; та ін.
24. Рішення Жовтневого районного суду Миколаївської області у справі № 477/991/15-ц від 21 липня 2016 року: https://reyestr.court.gov.ua/Review/59327238.
25. Див., наприклад, Рішення Дубенського міськрайонного суду Рівненської області у справі № 559/362/20 від 31 травня 2021 року: https://reyestr.court.gov.ua/Review/97360691#.
26. Лист Міністерства юстиції України № 5543-0-33-13/6.1 від 26.04.2013 року: https://zakon.rada.gov.ua/laws/show/v5543323-13#Text.
27. Див., наприклад, Постанову Київського апеляційного суду у справі № 361/3511/20 від 15 липня 2021 року: https://reyestr.court.gov.ua/Review/98593168.

автомобільних доріг у Кіровоградській області (відповідач) з вимогою визнання протиправною бездіяльності відповідача щодо ненадання інформації, необхідної для складення протоколів про адміністративне правопорушення щодо конкретних посадових осіб відповідача. Інформацію відповідач не надавав, посилаючись на те, що нема згоди цих осіб на обробку їхніх персональних даних. В аналогічних справах суди інколи займали помилкову позицію щодо неможливості поширення відповідних персональних даних[28]. Разом з тим у цій справі суд першої інстанції досить коректно застосував приписи Закону України «Про захист персональних даних», зокрема зазначивши:

«Згідно з ч. 4 ст. 19 Закону №2297-VI органи державної влади та органи місцевого самоврядування мають право на безперешкодний і безоплатний доступ до персональних даних відповідно до їх повноважень.

Відповідно до ч. 1 п. 2, ч. 2 ст. 21 Закону №2297-VI, про передачу персональних даних третій особі володілець персональних даних протягом десяти робочих днів повідомляє суб'єкта персональних даних, якщо цього вимагають умови його згоди або інше не передбачено законом. Повідомлення, зазначені у частині першій цієї статті, не здійснюються зокрема у разі виконання органами державної влади та органами місцевого самоврядування своїх повноважень, передбачених законом.

Аналіз вказаних норм свідчить, що у разі, якщо обробка персональних даних стосується здійснення державним органом повноважень, визначених законом, вона не потребує згоди суб'єкта персональних даних»[29].

Таку ж позицію у цій справі зайняв і суд апеляційної інстанції та суди в інших аналогічних справах[30]. Важливо наголосити, що інше тлумачення законодавства про захист персональних даних у цій ситуації фактично унеможливило б не тільки здійснення законних повноважень органу державної влади (тут – Державної фінансової інспекції в Кіровоградській області), але й викривило б природу відповідних адміністративних процедур. Зловживання правом на захист персональних даних не може бути інструментом захисту від настання юридичної відповідальності. Інше розуміння відповідних процедур порушуватиме вимоги юридичної визначеності та пропорційності як складників верховенства права.

Якість закону

Законодавство, відповідно до якого ведеться збір, обробка та використання персональних даних повинне з достатньою чіткістю передбачати не тільки алгоритм дій суб'єктів відповідних правовідносин і адміністративних процедур, але й відповідати вимогам суспільства в частині його юридичної визначеності, передбачуваності та пропорційності. Показова в цьому аспекті справа № 580/1751/19, де оскаржується відмова у вклеюванні в паспорт громадянина України у формі книжечки нової фотокартки, що відповідає віковій, у зв'язку із досягненням 45-річного віку. Суд першої інстанції некоректно застосував положення законодавства про захист персональних

28. Див, наприклад, Постанову Окружного адміністративного суду міста Києва у справі № 826/729/14 від 05 березня 2014 року: https://reyestr.court.gov.ua/Review/37646583 та в цій же справі Ухвалу Вищого адміністративного суду України від 23 липня 2015 року: https://reyestr.court.gov.ua/Review/47799591.
29. Постанова Кіровоградського окружного адміністративного суду у справі № П/811/1192/14 від 28 травня 2014 року: https://reyestr.court.gov.ua/Review/38986180.
30. Див. Постанова Кіровоградського окружного адміністративного суду у справі № 811/3717/13-а від 20 січня 2014 року: https://reyestr.court.gov.ua/Review/36909793; Ухвали Дніпропетровського апеляційного адміністративного суду у справах № П/811/2184/14 від 19 березня 2015 року: https://reyestr.court.gov.ua/Review/43612864; № 811/3717/13-а від 15 квітня 2015 року: https://reyestr.court.gov.ua/Review/43882856; № П/811/1192/14 від 28 травня 2015 року: https://reyestr.court.gov.ua/Review/45403830; та ін.

даних. При цьому суд апеляційної інстанції доволі ґрунтовно та змістовно подав свою правову позицію не тільки на основі системного аналізу національного законодавства, але й з урахуванням міжнародних стандартів. Суд зазначив:

«… суд першої інстанції зазначив, що принципами обробки персональних даних є відкритість і прозорість, відповідальність, адекватність та не надмірність їх складу та змісту стосовно визначеної мети їх обробки, а підставою обробки персональних даних є згода суб'єкта персональних даних. Однак законодавство у регулюванні спірних відносин не є якісним, позаяк не врегульовано питання щодо наслідків відмови особи від обробки її персональних даних, відсутня альтернатива вибору, що обумовлює порушення конституційних прав такої особи.

Крім того, суд першої інстанції виходив з того, що реалізація державних функцій має здійснюватися без примушення людини до надання згоди на обробку персональних даних, їх обробка повинна здійснюватися, як і раніше, в межах і на підставі тих законів і нормативно-правових актів України, на підставі яких виникають правовідносини між громадянином та державою. Технології не повинні бути безальтернативними і примусовими. Особи, які відмовилися від обробки їх персональних даних, повинні мати альтернативу – використання традиційних методів ідентифікації особи»[31].

Такою аргументацією суд апеляційної інстанції дав свою оцінку аргументам суду першої інстанції щодо «якості» законодавства та системного тлумачення відповідних приписів у частині захисту персональних даних і охорони приватного життя. При цьому суд ухвалив нове рішення в цій справі, яким інакше розтлумачив відповідні приписи законодавства. Зокрема, суд зазначив:

«Оформлення паспорта громадянина України належить до випадків обробки персональний даних в силу вимог закону, адже отримання такого документа є обов'язковим, а його оформлення без обробки персональних даних – неможливе.

За таких обставин колегія суддів приходить до висновку про те, що громадянин України не наділений правом відмовитися від обробки його персональних даних, необхідних для оформлення паспорта громадянина України у цілому. У нього відсутня свобода розсуду у вирішенні зазначеного питання, адже обробка персональних даних є обов'язковою передумовою оформлення зазначеного документа.

Разом з тим, […] громадянин України може заперечувати проти обробки його персональних даних за умови недотримання вимог ст. 6 Закону України «Про захист персональних даних»…

…Колегія суддів враховує, що незгода ОСОБА_1 із обробкою її персональних даних за допомогою засобів Єдиного державного демографічного реєстру обумовлена обсягом інформації, що вноситься до нього. Фактично позивач не погоджується із тим, що за результатами ідентифікації особи формується унікальний номер запису в Єдиному державному демографічному реєстрі…

…Законом України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» визначено, що формування унікального номеру запису в реєстрі є результатом завершення ідентифікації особи.

Колегією суддів не встановлено підстав для висновку про те, що формування унікального номеру запису в Єдиному державному демографічному реєстрі не відповідає меті обробки персональних даних, є неадекватним чи надмірним заходом.

31. Постанова Шостого апеляційного адміністративного суду у справі № 580/1751/19 від 12 грудня 2019 року: https://reyestr.court.gov.ua/Review/86425640.

Однак колегія суддів враховує, що для окремої суспільної групи генерація за наслідками обробки персональних даних унікального номеру запису в Єдиному державному демографічному реєстрі може становити надмірне втручання у їх особисте життя.

Такий висновок узгоджується з правовою позицією Великої Палати Верховного Суду, що викладена в постанові від 19 вересня 2018 року у зразковій справі № 806/3265/17. У вказаній справі суд визнав вимогу щодо оформлення паспорта з обробкою персональних даних у Єдиному державному демографічному реєстрі та формуванням унікального номеру запису в реєстрі надмірним втручанням у особисте життя осіб, які внаслідок своїх релігійних переконань, мають побоювання та заперечення щодо присвоєння цифрового ідентифікатора…

…З огляду на викладене колегія суддів допускає, що для окремих груп можуть бути встановлені винятки із загального правила щодо оформлення паспорта громадянина України з використанням засобів Єдиного державного демографічного реєстру.

Разом з тим, обов'язок довести приналежність до таких соціальних груп покладається саме на позивача»[32].

Цей приклад, а також аналогічні справи щодо збирання, обробки і використання персональних даних АТ «Укрпошта»[33] доволі показово ілюструють різні підходи до тлумачення закону та особливостей його практичного застосування. Попри різні позиції суду першої та апеляційної інстанції, для цього блоку аналізу важливо наголосити, що зазначений спір мав би інший масштаб та, можливо, інші правові наслідки, за умови ретельнішого та виваженішого законодавчого регулювання. З огляду на це, у законодавстві про захист персональних даних питання якості закону, його відповідності до складників верховенства права (юридичної визначеності, пропорційності, рівності та недискримінації тощо) особливо гострі й потребують ґрунтовнішого і зваженішого регулювання, а згодом і нормозастосування.

Тут додатково слід зазначити про позицію Верховного Суду у зразковій справі (про оформлення паспорта громадянина України), якою досить чітко продемонстровано бачення Суду щодо співвідношення права на свободу совісті та механізмів його реалізації у зв'язку з обробкою персональних даних а також оцінки якості закону, що мали б виправлятися в законодавчому порядку. Зокрема, Верховний Суд зазначив:

«Щодо релігійних переконань як позивачки, так і релігійної організації, про її приналежність до якої зазначено в позовній заяві та письмових поясненнях, з приводу присвоєння унікального номера, якщо паспорт громадянина України нового зразка оформлятиметься засобами Реєстру, то цей аргумент, незважаючи на усю його значимість для як для ОСОБА_1, так і для багатьох інших громадян України, які поділяють такі ж релігійні погляди й переконання, не може слугувати підставою для того, щоб порушувати/не виконувати вимоги Закону № 5492-VI та/чи робити з нього винятки. На думку суду, такий підхід є недопустимим, оскільки суперечитиме наведеним конституційним положенням статей 24 і 35 Основного Закону, а також може призвести до зловживань з боку окремих осіб та/або їх груп з метою уникнення виконання покладених на них законом обов'язків.

Організаційні засади створення і функціонування Єдиного державного демографічного реєстру, види персональних даних, які підлягають обробці засобами Реєстру і мета цієї обробки визначені

32. Постанова Шостого апеляційного адміністративного суду у справі № 580/1751/19 від 12 грудня 2019 року: https://reyestr.court.gov.ua/Review/86425640.
33. Див., наприклад, Рішення Вінницького міського суду Вінницької області у справі № 127/13877/19 від 24 січня 2020 року: https://reyestr.court.gov.ua/Review/87308345 та Постанову Вінницького апеляційного суду у справі № 127/13877/19 від 24 червня 2020 року: https://reyestr.court.gov.ua/Review/90109587.

на законодавчому рівні, оскільки сфера цих суспільних відносин, за статтею 92 Конституції України, є предметом виняткового законодавчого регулювання.

Водночас повноваження щодо прийняття законів належить виключно парламенту, і законодавча діяльність цього конституційного органу не може піддаватися оскарженню в порядку адміністративного судочинства. Звідси випливає висновок, що вирішити питання співвідношення і балансу особистих релігійних переконань особи та суспільних інтересів, на користь яких на загальнодержавному рівні встановлено єдиний (однаковий для всіх) порядок оформлення документа, що посвідчує громадянство України (зокрема, форми цього документа) чи будь-яким чином змінити правове регулювання цих відносин в інший спосіб, ніж внесення у встановленому порядку змін до чинних на сьогодні законодавчих та підзаконних нормативно-правових актів у цій частині, на переконання суду, не видається можливим. У межах судового розгляду цього спору обирати форму такого документа, як паспорт громадянина України, і зобов'язувати/змушувати державний орган діяти всупереч встановленому законом правовому порядку в цій сфері правовідносин суперечитиме не лише завданням адміністративного судочинства України і функції судового контролю, а й конституційному принципу поділу влади.

Суд наголошує, що предметом спору в цій справі є правомірність відмови територіального органу ДМС в оформленні паспорта громадянина України у вигляді (формі) паспортної книжечки з мотивів, про які було зазначено. Правову оцінку цим діям/рішенням відповідачів суд надає на предмет їхньої відповідності критеріям, установленим у частині другій статті 2 КАС, зокрема перевіряє, чи такі вчинено/прийнято на підставі, в межах повноважень та у спосіб, що визначені Конституцією та законами України. Незгода з тим, як держава врегулювала ці правовідносини, у порівнянні з тим, яке їх правове регулювання було раніше, а також небажання виконувати приписи законодавчих та урядових нормативно-правових актів при оформленні паспорта громадянина України із згаданих мотивів, не може слугувати переконливим аргументом протиправності дій суб'єкта владних повноважень, як і не може бути для особи підставою, для того щоб не виконувати/не дотримуватися приписів законодавства»[34].

Такий підхід доволі чітко відмежовує нормозастосування, що реалізовується суд, від нормотворчості, якою займається насамперед парламент (законодавча влада). Попри це, виходячи з розуміння якості інструментів захисту персональних даних, а не тільки гарантування свободи совісті та віросповідання, суди в аналогічних справах мають враховувати й особливості дії Закону України «Про захист персональних даних» та відповідних міжнародних стандартів у цій сфері. Адже було б вкрай небезпечне застосування підходу, коли суд міг би відмовити в захисті порушеного права через неналежну якість закону. Це особливо важливо у сфері захисту персональних даних.

Щодо справедливості як елемента принципу законності обробки персональних даних, то вона доволі складний компонент, який мають досліджувати суди доволі ретельно та враховувати весь комплекс обставин кожної справи. Як приклад – рішення судів у справі № 603/160/20. Тут ідеться про те, що відповідач (фізична особа) встановила на фасаді свого будинку відеокамеру постійного спостереження, що направлена лише на належне позивачеві (фізичній особі) домогосподарство і цілодобово фіксує його приватне життя. Крім того, ще одну відеокамеру постійного спостереження відповідачка встановила на фасаді гаража, за допомогою якої спостерігає за в'їздом до домоволодіння позивача, фіксує все, що відбувається на подвір'ї, біля воріт і на вулиці. Відеоматеріали з коментарями свого чоловіка відповідачка викладає в соціальні мережі без згоди позивача. У цій ситуації йдеться про збирання, обробку і поширення персональних даних, що фактично обумовлюють надмірне втручання в приватне життя.

34. Рішення Верховного Суду у справі № 806/3265/17 від 26 березня 2018 року: https://reyestr.court.gov.ua/Review/73139306.

Суд першої інстанції[35] позов задовольнив і зобов'язав відповідачку власним коштом демонтувати дві відеокамери зовнішнього спостереження, що розташовані на належній їй земельній ділянці. Аргументація суду хоч і була вкрай коротка, проте достатня для ухвалення відповідного рішення.

Суд апеляційної інстанції дійшов висновку, «що інформація про особисте життя особи це будь-які відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Відеозйомка це щонайменше збирання, зберігання та використання інформації про особисте життя фізичної особи, тобто персональних даних такої особи, що може становити недозволене втручання в особисте життя певної особи. Щоб таке втручання було законним, воно повинно відбуватися за згодою відповідної фізичної особи»[36].

При цьому, важливо те, що відеоспостереження відповідачка вела з метою забезпечення належними доказами іншого судового провадження, де вона позивачка щодо свого сусіда (у справі про заборону використовувати житловий будинок для промислового виробництва, виготовлення столярних виробів і дерев'яних меблів, використовуючи легкозаймисті фарби та лаки). Суд першої та апеляційної інстанцій взяли до уваги повний спектр обставин та досить чітко зазначили на непропорційності порушення права на приватне життя (через незаконне збирання, обробку та поширення персональних даних) з іншою (можливо, й правомірною) метою. При цьому суд апеляційної інстанції змінив рішення суду першої інстанції, визначивши вимогу демонтувати відеокамери надмірною:

«…аналіз зібраних в матеріалах справи доказів дає підстави прийти до висновку, що відеоспостереження встановлено відповідачкою виключно з метою захисту її прав та членів її сім'ї на життя та здоров'я, створення безпечних умов проживання, охорони житлового будинку та прибудинкової території, протиправного проникнення на її територію сторонніх осіб.

За таких обставин, зобов'язання відповідача демонтувати відеокамери зовнішньої системи відеонагляду, які встановленні на фасадах житлового будинку та гаражу, є безпідставними»[37].

Врешті відповідачка була тільки зобов'язана припинити відеознімання житлового будинку та прибудинкової території позивача. Отже, суди взяли до уваги не тільки сам факт необхідності захисту персональних даних однієї особи, але й врахували й інші обставини справи.

Також важливе з цього погляду розуміння питань глибини втручання в приватне життя та поширення персональних даних. Традиційний тут пошук балансу між суспільним (публічним) інтересом і необхідністю захисту приватного життя та відповідних персональних даних. Показове та цікаве для аналізу поширення персональних даних і приватної інформації з посиланням на стороннє джерело, яке може належати, наприклад, до джерел, доступних для загального відкритого використання. У таких випадках суди мають досліджувати не тільки джерело інформації, але й її первинне походження, суб'єкта створення та поширення. Загалом, судова практика демонструє, що суди зазвичай проводять такий аналіз доволі ретельно. Наприклад, у справі № 761/44774/17[38], де йшлося про вимогу позивачки припинити поширювати щодо неї певні інформаційні матеріали (статті, відео та ін.), відповідач, обґрунтовуючи правомірність своєї позиції, посилався на те, що розміщені відео та стаття, були взяті з ютюбу, який доступний для загального

35. Рішення Монастириського районного суду Тернопільської області у справі № 603/160/20 від 19 жовтня 2020 року: https://reyestr.court.gov.ua/Review/92447961.
36. Постанова Тернопільського апеляційного суду у справі № 603/160/20 від 03 березня 2021 року: https://reyestr.court.gov.ua/Review/95528417.
37. Постанова Тернопільського апеляційного суду у справі № 603/160/20 від 03 березня 2021 року: https://reyestr.court.gov.ua/Review/95528417.
38. Рішення Шевченківського районного суду м. Києва у справі № 761/44774/17 від 23 січня 2019 року: https://reyestr.court.gov.ua/Review/79881631.

використання та служить підставою для вільного використання. Суд при аналізі обставин цієї справи проаналізував, зокрема, умови користування ютюбом (https://www.youtube.com/t/terms) і дійшов висновку, що сталося порушення вимог законодавства щодо поширення персональних даних позивачки.

Отже, справедливість як один з елементів принципу законності вимагає ретельного аналізу не тільки самого факту порушення прав особи, але й коректності посилання сторонами відповідних правовідносин на певні обставини, інструменти чи техніки справляння впливу на зміст та обсяг персональних даних. Це особливо важливо, коли йдеться про визначення вірогідності інформації, певних подій і фактів, законності джерела походження інформації тощо.

ЦІЛЕСПРЯМОВАНІСТЬ

Принцип цілеспрямованості не традиційний для виокремлення в законодавстві про захист персональних даних. Його зазвичай позначають через характеристику мети збирання, обробки і використання персональних даних. Тут ідеться не просто про законну мету (закон може за певних обставин бути некоректним, наприклад, застарілим), а саме про легітимну мету, яка може бути встановлена (деталізована) судом у кожній конкретній ситуації.

Власне таке змістовне наповнення цього принципу тут і представлено. Разом з тим аналіз мети поза визначенням підстав обробки персональних даних може бути неповним. З огляду на це, у цьому розділі представлено два компоненти:

- визначеність мети і її чіткість – ідеться про те, що мета збирання, обробки і використання персональних даних повинна бути передбаченою законом (відповідати встановленим законом обмеженням), а також відповідати засадам справедливості в демократичному суспільстві, тобто бути легітимною;
- наявність підстав збирання, обробки та використання персональних даних – мета обумовлює зміст і спосіб застосування підстав обробки персональних даних; підстави досить чітко визначені Законом України «Про захист персональних даних» і їх можна розподілити на два основних блоки: надання згоди суб'єктом персональних даних і обробка персональних даних на підставі закону[39]. Окремо слід аналізувати застосування підстав обробки щодо чутливих персональних даних.

Визначення мети, її чіткість

Мета обробки персональних даних має бути пов'язаною з підставою, на основі якої проводиться збирання, обробка та використання персональних даних. Показовим прикладом тут може бути передання кредитором персональних даних позичальників за договором про відступ права вимоги третій особі (новому кредиторові). У таких ситуаціях суди зазвичай опираються на пов'язаність підстав обробки персональних даних однією метою та, відповідно, правомірне передання інформації від одного суб'єкта до іншого.

39. Закон виокремлює шість підстав для обробки. В залежності від того, чи вони базуються на підставі згоди, чи закону, їх умовно можна розділити на дві групи.
    Згода
    - згода суб'єкта персональних даних на обробку його персональних даних;
    - 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.

    Закон
    - дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень;
    - захист життєво важливих інтересів суб'єкта персональних даних;
    - необхідність виконання обов'язку володільця персональних даних, який передбачений законом;
    - необхідність захисту законних інтересів володільців персональних даних, третіх осіб, крім випадків, коли суб'єкт персональних даних вимагає припинити обробку його персональних даних та потреби захисту персональних даних переважають такий інтерес.

    Вказаний перелік підстав обробки персональних даних є вичерпним.

Наприклад, у справі № 559/362/20 Дубенський міськрайонний суд Рівненської області визначив, що «… уклавши спірний кредитний договір, позивач надав кредитору свою згоду збирати, зберігати, використовувати, поширювати і отримувати інформацію – дані про неї, відомі кредитору 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»[40].

Таку ж позицію зайняв і Верховний Суд в аналогічній справі, зазначивши:

«Відповідно до частини першої статті 517 ЦК України первісний кредитор у зобов'язанні повинен передати новому кредиторові документи, які засвідчують права, що передаються, та інформацію, яка є важливою для їх здійснення.

На виконання вищевказаних положень закону ПАТ «Кредитпромбанк» передало, а ПАТ «Дельта Банк» прийняло документи на підтвердження зобов'язань ОСОБА_4, в тому числі її персональні дані, необхідні для виконання взятих нею зобов'язань.»[41]

Мета збирання та обробки персональних даних має бути чітко відстежуваною та стосуватися конкретного суб'єкта персональних даних. Неприпустимі випадки, коли в межах реалізації мети обробки персональних даних щодо однієї особи одночасно виконуються аналогічні дії щодо інших, третіх осіб. Як приклад, у справі № 520/5575/19 суди всіх інстанцій встановили незаконне збирання, зберігання, використання та поширення конфіденційної інформації – персональних даних про особу в ході службового розслідування, яке її не стосувалося. Верховний Суд у цій справі зазначив:

«57. Відтак, як було встановлено судами попередніх інстанцій, службове розслідування проводилось відповідачем стосовно ОСОБА_3 , а не у відношенні позивача. Однак, висновок Міжрегіонального управління Національного агентства України з питань державної служби у Харківській та Сумській областях за результатами службового розслідування стосовно ОСОБА_3 , 1970 року народження, начальника Головного управління державної фіскальної служби у Харківській області (керівника державної служби) від 30.11.2018 року містить здебільшого аналіз правомірності дій ОСОБА_1 , а не особи, у відношенні якої призначено службове розслідування.

58. При цьому, під час проведення вказаного службового розслідування була використана інформація, отримана і застосована без належних на це підстав.

59. Суди першої і апеляційної інстанції дійшли висновків, з якими погоджується Верховний Суд, що наведене в сукупності свідчить про наявність з боку відповідача протиправних дій щодо незаконного збирання, зберігання, використання та поширення конфіденційної інформації – персональних даних про особу ОСОБА_1 , зокрема відносно його освіти без його згоди, що можна розцінити, як втручання в особисте життя при проведенні службового розслідування стосовно ОСОБА_3 , начальника Головного управління державної фіскальної служби у Харківській області (керівника державної служби)»[42].

Окремо слід звернути увагу на використання персональних даних після завершення договірних правовідносин з метою їх належного оформлення (завершення всіх процедур, настання

40. Рішення Дубенського міськрайонного суду Рівненської області у справі № 559/362/20 від 31 травня 2021 року: https://reyestr.court.gov.ua/Review/97360691#.
41. Постанова Верховного Суду у справі № 477/991/15-ц від 11 грудня 2018 року: https://reyestr.court.gov.ua/Review/78495991.
42. Постанова Верховного Суду у справі 520/5575/19 від 21 жовтня 2021 року: https://reyestr.court.gov.ua/Review/100471074.

правових наслідків тощо). Така підстава обробки персональних даних випливає з пункту третього частини першої статті 11 Закону України «Про захист персональних даних» – укладення та виконання правочину, сторона якого – суб'єкт персональних даних або який укладено на користь суб'єкта персональних даних чи для вжиття заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних. При застосуванні цієї норми йдеться не тільки про згоду на укладення правочинів, але й про дію згоди й на етапі виконання відповідного договору чи завершення його дії.

Тут показовим може бути приклад у справі № 182/4540/20, де йдеться про відкриття рахунку в банку особі на підставі персональних даних, які особа безпосередньо не надавала і згоду на їх обробку не оформляла. У цій справі банк на виконання рішення суду зарахував на рахунок позивача (фізичної особи) кошти – грошову компенсацію за невикористані календарні дні додаткової відпустки, як учасникові бойових дій, за певний період, у зв'язку із звільненням його (позивача) з військової служби в запас. Суд у цій ситуації зазначив:

«Зі змісту цитованих положень Закону № 2297-VI [Закону України «Про захист персональних даних»] вбачається, що підставою для обробки персональних даних може бути не тільки згода суб'єкта персональних даних на це, а й, зокрема, укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на користь суб'єкта персональних даних, необхідність виконання обов'язку володільця персональних даних, який передбачений законом…

… У даному випадку відповідачі, здійснюючи обробку персональних даних позивача діяли з метою виконання рішення суду та були направлені насамперед на відновлення порушених прав самого позивача, зокрема, нарахування та виплату позивачу грошової компенсації за невикористані календарні дні додаткової відпустки, як учаснику бойових дій, за період з 2016 року по 2018 рік, виходячи з грошового забезпечення кулеметника військової частини А1126 Збройних Сил України, станом на день звільнення з військової служби 06 вересня 2018 року.

Суд вважає, що Військовою частиною А1126 та Акціонерним Товариством

«Укрсиббанк» дотримано вимог Закону України «Про захист персональних даних», а твердження позивача, що для надання та обробки персональних даних обов'язково необхідна виключно його особиста згода спростовуються самим Законом України «Про захист персональних даних»»[43].

«Службова», спеціальна мета збирання, обробки і використання персональних даних не повинна змінювати природу та межі розуміння поняття «персональні дані». Це важливий аспект, бо доволі часто в практичному нормозастосуванні дію спеціальних законів (у сфері оподаткування, запобігання корупції, кримінально-процесуального законодавства, про адвокатуру тощо) юристи сприймають як пріоритетну (першочергову), тоді як дія законодавства про персональні данні обмежується або ж і зовсім не застосовується в конкретних правовідносинах.

Доволі ілюстративною тут може бути справа № 825/1440/14, де йдеться про дію Закону України «Про адвокатуру та адвокатську діяльність» у співвідношенні з законодавством про захист персональних даних у частині його поширення на інформацію, що міститься в дисциплінарній справі щодо адвоката. У цій справі позивач (адвокат) вимагав визнати протиправним направлення матеріалів дисциплінарної справи до кваліфікаційно-дисциплінарної комісії іншої області та зобов'язати відповідну кваліфікаційно-дисциплінарну комісію адвокатури знищити дисциплінарну справу, яка містить персональні дані про позивача і які оброблялися, на його думку, незаконно.

43. Рішення Нікопольського міськрайонного суду Дніпропетровської області у справі № 182/4540/20 від 16 березня 2021 року: https://reyestr.court.gov.ua/Review/95531903.

Суд першої та суд апеляційної інстанції, ухваливши рішення в цій справі, дійшли висновку, що інформація щодо дисциплінарного провадження стосовно адвоката не персональні дані. Суд першої інстанції зазначив:

«Щодо твердження позивача про те, що дії КДКА Закарпатської області щодо здійснення дисциплінарного провадження є обробкою персональних даних, суд зазначає наступне.

Відповідно до абзацу 2 статті 1 Закону України «Про захист персональних даних» цей Закон поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів.

Згідно статті 2 Закону України «Про захист персональних даних» обробка персональних даних – будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем.

У свою чергу, згідно статті 2 даного Закону, персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Дії КДКА Закарпатської області щодо здійснення дисциплінарного провадження по відношенню до адвоката, перевірка інформації щодо здійснення адвокатом дисциплінарного проступку, не є персональними даними»[44].

Слід зазначити, що однією з ключових ознак віднесення інформації до персональних даних тут суд назвав використання «інформаційних (автоматизованих) систем» обробки персональних даних. Такий підхід очевидно помилковий. Проте з такою аргументацією погодився і суд апеляційної інстанції[45]. Верховний Суд, погодившись із кінцевим рішенням судів першої та апеляційної інстанцій, звернув увагу на хибність такого тлумачення і застосування законодавства про захист персональних даних. Власне в цій частині Верховний Суд змінив мотивувальні частини судів, зокрема, зазначивши:

«Конституційним Судом України у рішенні від 20 січня 2012 року 2-рп/2012 розширено поняття «інформація про особу» до якого входить, у тому числі й інформація про професійну діяльність.

Збирання, зберігання, використання та поширення державою, органами місцевого самоврядування, юридичними або фізичними особами конфіденційної інформації про особу без її згоди є втручанням в її особисте та сімейне життя, яке допускається винятково у визначених законом випадках і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Як встановлено з наданих доказів, дисциплінарне провадження проводилось у визначеному Законом порядку та в інтересах захисту прав людини…

…Однак, висновок судів в мотивувальній частині рішення про те, що в силу абзацу 2 статті першої та статті 2 Закону України «Про захист персональних даних» дії КДКА Закарпатської області щодо здійснення дисциплінарного провадження по відношенню до адвоката, перевірка

44. Постанова Чернігівського окружного адміністративного суду у справі № 825/1440/14 від 02 липня 2014 року: https://reyestr.court.gov.ua/Review/39618974.
45. Ухвала Київського апеляційного адміністративного суду у справі № 825/1440/14 від 09 жовтня 2014 року: https://reyestr.court.gov.ua/Review/41066241.

інформації щодо здійснення адвокатом дисциплінарного проступку, не є персональними даними є помилковим»[46].

Мета збирання та обробки персональних даних має бути достатньо верифікованою та не може піддаватися розширювальному тлумаченню, навіть у споріднених ситуаціях, що породжують спільні наслідки. Як приклад, надання згоди на обробку персональних у цивільно-правовому договорі не означає автоматично, що така згода може поширюватися на всі наслідки застосування відповідного договору. У справі № 910/15262/19 йшлося про можливість використання положень договору страхування для збирання додаткової інформації страховиком про страхувальника в разі настання страхового випадку.

Договором добровільного страхування наземного транспорту передбачено «…право страховика робити запити про відомості, пов'язані із страховим випадком до правоохоронних органів, банків та інших підприємств, установ і організацій, що володіють інформацією про обставини страхового випадку, а також самостійно з'ясовувати причини і обставини страхового випадку»[47]. Після настання страхового випадку з метою перевірки наданих страхувальником пояснень страховик звернувся до Приватного акціонерного товариства «Київстар» із запитом, у якому просив надати інформацію чи дійсно був дзвінок на службу 102 із мобільного телефона страхувальника. У відповідь на вказаний запит направлено лист, у якому, посилаючись на статтю 34 Закону України «Про телекомунікації», вказано на брак правових підстав для надання відомостей щодо обслуговування відповідного номера. Відповідна відмова стала предметом судового спору.

Суд першої інстанції відмовив у задоволенні позову, аргументувавши, що положення договору страхування в цій ситуації не можуть тлумачитися як такі, що уповноважують страховика отримувати додаткові персональні дані від третіх осіб в інших правовідносинах, зокрема від Приватного акціонерного товариства «Київстар». Суд істотно акцентував на необхідності охорони таємниці телефонних розмов, телеграфної чи іншої кореспонденції, що передаються технічними засобами телекомунікацій, та інформаційній безпеці телекомунікаційних мереж. Попри це, також зроблено не зовсім обґрунтований та аргументований висновок, що:

«Натомість у пункті 6.3.3 Договору сторонами погоджене право страховика робити запити про відомості, пов'язані із страховим випадком, а не право на обробку та збір персональних даних, тим більше які є конфіденційними або таємними.

В той же час, відповідно письмової згоди від 23.04.2019 ОСОБА_1 надано згоду на використання персональних даних, а не на їх обробку.

У відповідності до наявного у статті 2 Закону України «Про захист персональних даних» визначення обробка персональних даних – будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем.

Частиною першою статті 12 Закону України «Про захист персональних даних» визначено, що збирання персональних даних є складовою процесу їх обробки, що передбачає дії з підбору чи впорядкування відомостей про фізичну особу.

Тобто, згода на використання персональних даних є вужчим поняттям ніж обробка персональних даних та не включає в себе надання згоди на збирання персональних даних.

---

46. Постанова Верховного Суду у справі № 825/1440/14 від 31 липня 2019 року: https://reyestr.court.gov.ua/Review/83356666.
47. З тексту Постанови Північного апеляційного господарського суду у справі № 910/15262/19 від 20 травня 2020 р.: https://reyestr.court.gov.ua/Review/89346817.

З огляду на наведене, суд приходить до висновку, що позивачем не доведено, що ОСОБА_1 було надано йому письмову згоду на збирання щодо нього персональної інформації, тим більше конфіденційної чи таємної, а відтак відсутні підстави вважати, що третьою особою надано письмову згоду на поширення інформації про себе, як споживача телекомунікаційних послуг.»[48]

Суд апеляційної інстанції дещо відкоригував аргументацію і підтримав позицію суду першої інстанції. У цій ситуації суди, загалом, правильно застосували положення Закону України «Про захист персональних даних», разом з тим, аргументація позиції була вкрай загальна та не зовсім коректно відображала сутність законодавства про захист персональних даних. Твердження: «… згода на використання персональних даних є вужчим поняттям ніж обробка персональних даних та не включає в себе надання згоди на збирання персональних даних» мало б бути аргументованішим та обґрунтованішим.

Підстави обробки персональних даних

Згода

Важливе також не завжди коректне розуміння обсягу та змісту поняття «згода на обробку персональних даних». При цьому помилкове тлумачення застосовують як особи, що звертаються до судів, так і суди. Основна тут інколи надмірна «абсолютизація» такої згоди, що, на жаль, доволі часто підтримується (встановлюється і деталізується) навіть на рівні підзаконних актів. Наприклад, приписами Положення «Про порядок призначення житлових субсидій»[49] встановлено, що заява і декларація щодо отримання субсидії вважаються такими, що не подані, у разі, коли до них не додана (відсутня) згода на обробку персональних даних про членів домогосподарства та членів сім'ї осіб із складу домогосподарства, доходи яких враховуються під час призначення субсидії, даних про доходи та майно. За такого підходу, отримання згоди на обробку персональних даних покладалося на самого суб'єкта звернення по отримання відповідної публічної послуги. Суди, застосовуючи відповідні положення доволі загально аналізували ці вимоги в частині дотримання законодавства про захист персональних даних і зазвичай це не впливало на зміст відповідних рішень.

Наприклад, у справі № 340/570/20 суд першої інстанції зазначив:

«Позивачем із заявою про призначення субсидії не надано до відповідача згоду на обробку персональних даних про членів домогосподарства та членів сім'ї осіб із складу домогосподарства, доходи яких враховуються під час призначення субсидії, даних про доходи та майно.

Суд зазначає, що позивач помилково вважає, що він має надати згоду на обробку персональних даних щодо себе, однак, згідно листа відповідача позивач не надав, саме згоду на обробку персональних даних про членів домогосподарства та членів сім'ї осіб із складу домогосподарства, доходи яких враховуються під час призначення субсидії, даних про доходи та майно.

Частиною 2 статті 19 Конституції України встановлено, що органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України.

48. Рішення Господарського суду міста Києва у справі № 910/15262/19 від 17.12.2019 р.: https://reyestr.court.gov.ua/Review/86568737.
49. Положення «Про порядок призначення житлових субсидій», затверджено Постановою Кабінету Міністрів України «Про спрощення порядку надання населенню субсидій для відшкодування витрат на оплату житлово-комунальних послуг, придбання скрапленого газу, твердого та рідкого пічного побутового палива» від 21 жовтня 1995 р. № 848: https://zakon.rada.gov.ua/laws/show/848-95-%D0%BF#Text.

Суд враховуючи зазначені вище положення чинного законодавства України, приходить до висновку, що відповідачем правомірно, з дотриманням положень ч. 2 ст. 2 КАС України, відмовлено у призначені субсидії з лютого 2020 року на підставі абз.4 пункту 46 Постанови Кабінету Міністрів України від 21 жовтня 1995 р. № 848 «Про спрощення порядку надання населенню субсидій для відшкодування витрат на оплату житлово-комунальних послуг, придбання скрапленого газу, твердого та рідкого пічного побутового палива»»[50].

У цій справі суди апеляційної[51] та касаційної[52] інстанцій не проводили відповідного аналізу ситуації з боку необхідності дотримання законодавства про захист персональних даних та необхідності отримання згоди власне від суб'єкта персональних даних, а не сторонньої особи. Судова практика знає й приклади, коли позивачі (фізичні особи) оскаржували відмову в наданні субсидії через неподання персональних даних (певної інформації) щодо інших осіб[53]. Слід зазначити, що відповідні приписи Положення «Про порядок призначення житлових субсидій» змінено й тепер надання згоди щодо членів сім'ї не вимагається[54]. В окремих випадках суди досить ретельно аргументували свою позицію і задовольняли позови з вимогами про надання соціального захисту (наприклад, у вигляді виплати державної соціальної допомоги) навіть за умови браку згоди на обробку персональних даних або навіть у разі подання особою заяви про ненадання згоди на обробку персональних даних. Наприклад, у справі № 161/18512/17 суд зазначив:

«Статтею 4 Закону України «Про державну соціальну допомогу малозабезпеченим сім'ям» установлено, що місцеві державні адміністрації для мети цього Закону мають право користуватися всіма офіційними джерелами інформації, в тому числі й інформацією органів доходів і зборів.

На виконання п.27 Порядку призначення і виплати державної соціальної допомоги малозабезпеченим сім'ям органи соціального захисту населення мають право робити запити та у строк до 15 календарних днів з дня надходження відповідного запиту безоплатно отримувати від територіальних органів ДФС, інших органів виконавчої влади та органів місцевого самоврядування інформацію, необхідну для перевірки достовірності даних, отриманих від осіб, які звертаються за призначенням державної соціальної допомоги малозабезпеченим сім'ям. Для підтвердження даних про доходи (відсутність доходів) використовуються відомості ДФС з Державного реєстру фізичних осіб – платників податків у порядку, встановленому Мінсоцполітики та Мінфіном.

Таким чином, вказаним Порядком передбачено повноваження Управління на збір та обробку персональних даних без згоди особи, якій вони належать, а в силу самої вказівки закону.

Аналіз наведених положень Закону вказує на те, що 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.

---

50. Рішення Кіровоградського окружного адміністративного суду у справі № 340/570/20 від 30 березня 2020 року: https://reyestr.court.gov.ua/Review/88491910.
51. Постанова Третього апеляційного адміністративного суду у справі № 340/570/20 від 23 червня 2020 року: https://reyestr.court.gov.ua/Review/90148533.
52. Ухвала Верховного Суду у справі № 340/570/20 від 17 серпня 2020 року: https://reyestr.court.gov.ua/Review/91036684.
53. Див., наприклад, Рішення Харківського окружного адміністративного суду у справі № 520/2536/19 від 01 липня 2019 року: https://reyestr.court.gov.ua/Review/82931582.
54. Постанова Кабінету Міністрів України «Деякі питання призначення житлових субсидій» від 19 травня 2021 р. № 505: https://zakon.rada.gov.ua/laws/show/505-2021-%D0%BF#n34.

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…

Тобто, для призначення державної соціальної допомоги малозабезпеченій сім'ї не потрібна згода заявника на збір та обробку персональних даних.

Подана заявником ОСОБА_2 17.07.2017 заява про відмову дати згоду на збір та обробку персональних даних взагалі не передбачена законом і не може бути взята до уваги при вирішенні питання про призначення допомоги у установленому законом порядку.

Виходячи з вищевикладених положень законодавства, суд вважає, що відповідач безпідставно відмовив позивачу у призначенні державної соціальної допомоги малозабезпеченій сім'ї, у зв'язку з відмовою дати згоду на збір і обробку персональних даних.

Разом з тим, суд вважає необхідним застосувати інший спосіб захисту прав позивача, який не суперечить закону і забезпечує ефективний захист таких прав. А саме: рішення про відмову у призначенні ОСОБА_2 державної соціальної допомоги слід визнати протиправним та скасувати, зобов'язати відповідача призначити ОСОБА_2 державну соціальну допомогу відповідно до Закону України «Про державну соціальну допомогу малозабезпеченим сім'ям» без згоди на збір та обробку персональних даних»[55].

В аналогічній справі Сумський окружний адміністративний суд зазначив:

«Крім того, суд звертає увагу відповідача на те, що ст. 11 Закону України «Про захист персональних даних» визначає підстави для обробки персональних даних. Так, п. 2 ч. 1 ст. 11 ЗУ «Про захист персональних даних», де йдеться про обробку персональних даних володільцем «відповідно до закону виключно для здійснення його повноважень», що можливо тільки в діяльності державно-владних суб'єктів.

Відповідач, як суб'єкт владних повноважень, діє в даному випадку від імені суспільства, задля забезпечення суспільних інтересів, у межах повноважень (прав та обов'язків) чітко передбачених законом. Відтак, якщо володілець має визначені законом повноваження, реалізація яких потребує обробки персональних даних, то це вже є достатньою законною підставою. При цьому обробці підлягає тільки обсяг персональних даних, який є необхідним і достатнім для досягнення законної мети обробки, тобто для забезпечення виконання конкретних завдань/повноважень володільця, передбачених законом»[56].

Ці та інші приклади57 з судової практики додатково доводять, що надмірна «абсолютизація» згоди на обробку персональних даних у діяльності органів державної влади, а інколи й у законодавстві, надмірна і непропорційна. Органи публічної влади не можуть і не повинні «ставати

55. Рішення Луцького міськрайонного суду Волинської області у справі № 161/18512/17 від 07 лютого 2018 року: https://reyestr.court.gov.ua/Review/72248664.
56. Рішення Сумського окружного адміністративного суду у справі № 480/3526/19 від 05 листопада 2019 року: https://reyestr.court.gov.ua/Review/85396099.
57. Див., наприклад, Постанову Дубенського міськрайонного суду Рівненської області у справі № 559/451/14-а від 26 лютого 2014 року: https://reyestr.court.gov.ua/Review/37336087; Постанову Ратнівського районного суду Волинської області у справі N 166/1494/15-а від 14 грудня 2015 року: https://reyestr.court.gov.ua/Review/54446035; Постанову Вінницького міського суду Вінницької області у справі № 127/14353/15-а від 27 серпня 2015 року: https://reyestr.court.gov.ua/Review/49397907; Постанову Знамянського міськрайонного суду Кіровоградської області у справі № 389/2267/17 від 22 листопада 2017 року: https://reyestr.court.gov.ua/Review/70722428; Постанову Володимир-Волинського міського суду Волинської області у справі № 154/364/17 від 27 лютого 2017 року: https://reyestr.court.gov.ua/Review/64983331; Рішення Деснянського районного суду м. Чернігова у справі № 750/5535/17 від 04 жовтня 2017 року: https://reyestr.court.gov.ua/Review/69305331 та ін.

заручниками» некоректного сприйняття поняття «згода на обробку персональних даних» при здійсненні свої повноважень передбачених законом. Ключовою рисою згоди є її добровільність, в той час, як функціонування публічної влади в більшості випадків може здійснюватися і без добровільного залучення особи до такої діяльності органу публічної влади. Надання згоди на обробку персональних даних не може ставати умовою діяльності органу в інтересах самої людини. Наприклад, вимога одержання згоди особи як умова надання їй же адміністративної послуги у більшості випадків порушуватиме Закон України «Про захист персональних даних», права людини та може спричинити інші, вкрай негативні наслідки. Відповідні підходи, підтвердженні судовою практикою, потребують більшого поширення та врахування як на рівні нормозастосування, так і в нормотворчій діяльності.

Щодо добровільності надання згоди на обробку персональних даних важливі приклади судових рішень у справах щодо публічних договорів (договори приєднання), коли договір фактично може і не укладатися, а сам факт настання правовідносин вважається приєднанням і, відповідно, укладенням договору.

Наприклад, у справах щодо судових спорів громадян із компаніями-постачальниками газу постає не тільки питання обробки персональних даних споживачів, але й внесення їх до спеціальних реєстрів (систем обліку, баз даних тощо) з одночасним присвоєнням ідентифікатора (спеціального номера, коду, штрих-коду тощо) у відповідному реєстрі. Останній аспект часто сприймають окремі споживачі як такий, що порушує їхнє право на свободу віросповідання:

«Позивачі зазначали, що вони у силу своїх релігійних переконань відмовились від умов заяви-приєднання до умов договору постачання природного газу побутовим споживачам та відмовились від присвоєння їм EIC-коду. При цьому вказали, що дають згоду на облік і ведення всієї необхідної документації стосовно них, як побутових споживачів, за прізвищем, ім'ям, по батькові та місцем фактичного проживання. Тому вважали, що відповідачі самовільно присвоїли їм ідентифікатори: EIC код, штрихкод, розрахунковий рахунок, який умисно змінено з п'ятизначного на десятизначний з метою трансформувати його в штрих-код. Такі дії для православного християнина є неприйнятними, порушують вимоги чинного законодавства про захист прав споживачів»[58].

У цитованій тут справі видно досить цікаве тлумачення згоди на обробку персональних даних. Брак безпосередньої згоди, з одного боку, унеможливлює укладення договору, а з іншого – може порушувати права споживачів. Вінницький міський суд Вінницької області[59] та Апеляційний суд Вінницької області[60] зайняли позицію, що згідно ч. 6 ст. 6 Закону України «Про захист персональних даних» у цій ситуації не допускається обробка даних про фізичну особу, які становлять конфіденційну інформацію, без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

При цьому Апеляційний суд Вінницької області ухвалив рішення про

«зобов'язання ПАТ «Вінницягаз» та ТОВ «Вінницягаз Збут» видалити з бази даних присвоєний EIC-код та інші цифрові ідентифікатори стосовно ОСОБА_3, ОСОБА_4, ОСОБА_5, ОСОБА_2 та вести облік і всю необхідну документацію стосовно ОСОБА_3, ОСОБА_4, ОСОБА_5, ОСОБА_2, як побутового споживача за прізвищем, ім'ям, по батькові та місцем фактичного проживання, без збору

58. Постанова Верховного Суду у справі № 127/10831/17 від 25 липня 2018 року: https://reyestr.court.gov.ua/Review/75528552.
59. Рішення Вінницького міського суду Вінницької області у справі № 127/10831/17 від 27.09.2017 року: https://reyestr.court.gov.ua/Review/69229516.
60. Рішення Апеляційного суду Вінницької області у справі № 127/10831/17 від 10 листопада 2017 року: https://reyestr.court.gov.ua/Review/70230738.

та обробки їх персональних даних…»[61]. Верховний Суд, не розглядаючи безпосередньо всі обставини справи в частині законодавства про захист персональних даних, передав справу на новий розгляд до суду апеляційної інстанції. Врешті в цій справі Апеляційний суд Вінницької області позов задовольнив частково і постановив:

«Скасувати присвоєний ОСОБА_6, ОСОБА_7, ОСОБА_3, ОСОБА_5 EIC-код, штрихкод, десятизначний рахунок споживачів, номер запису у реєстрі (УЗНР) та зобов'язати Публічне акціонерне товариство «Вінницягаз», Товариство з обмеженою відповідальністю «Вінницягаз Збут» виключити їх з баз даних.

Вести облік, всю необхідну документацію стосовно ОСОБА_6, ОСОБА_7, ОСОБА_3, ОСОБА_5 як побутових споживачів за прізвищем, ім'ям, по батькові, місцем проживання, без збору та обробки їх персональних даних»[62].

Аналогічний підхід відображено і в іншій Постанові Верховного Суду[63], хоч тут і зроблено більший акцент на захисті персональних даних, проте не проаналізовано їх природи та мети створення чи використання. Зокрема, не проведено аналізу щодо розмежування персональних даних особи та технологічних інструментів, що ідентифікують безпосередньо вузол обліку природного газу, розміщеного на об'єкті споживача.

У цій та інших аналогічних справах суди застосовують законодавство про захист персональних даних, опираючись на законодавство про свободу совісті та релігійні організації. Натомість належної правової оцінки автоматичності надання згоди на обробку персональних даних суди не надали. Ба більше, опираючись на потребу захисту релігійних прав конкретних осіб, суд повністю заборонив вести обробку персональних даних при наданні послуг відповідним споживачам, що видається фактично нереалістичним до виконання.

Додатково слід згадати про позицію Верховного Суду в зразковій справі (про оформлення паспорта громадянина України), якою досить чітко продемонстровано бачення Суду щодо співвідношення права на свободу совісті та механізмів його реалізації у зв'язку з обробкою персональних даних. Зокрема, Верховний Суд зазначив:

«Щодо релігійних переконань як позивачки, так і релігійної організації, про її приналежність до якої зазначено в позовній заяві та письмових поясненнях, з приводу присвоєння унікального номера, якщо паспорт громадянина України нового зразка оформлятиметься засобами Реєстру, то цей аргумент, незважаючи на усю його значимість для як для ОСОБА_1, так і для багатьох інших громадян України, які поділяють такі ж релігійні погляди й переконання, не може слугувати підставою для того, щоб порушувати/не виконувати вимоги Закону № 5492-VI та/чи робити з нього винятки. На думку суду, такий підхід є недопустимим, оскільки суперечитиме наведеним конституційним положенням статей 24 і 35 Основного Закону, а також може призвести до зловживань з боку окремих осіб та/або їх груп з метою уникнення виконання покладених на них законом обов'язків»[64].

Договірна форма надання згоди на обробку персональних даних може бути внесена не тільки до основного тексту (тіла) договору, але й міститися в супровідних (додаткових) документах. У справах № 761/8791/19 суди всіх інстанцій підтвердили можливість отримання згоди суб'єкта персональних даних не тільки в договорі, але й через погодження інших супровідних документів.

61. Рішення Апеляційного суду Вінницької області у справі № 127/10831/17 від 10 листопада 2017 року: https://reyestr.court.gov.ua/Review/70230738.
62. Рішення Апеляційного суду Вінницької області у справі № 127/10831/17 від 25 жовтня 2018 року: https://reyestr.court.gov.ua/Review/77481988.
63. Постанова Верховного Суду у справі № 579/806/19 від 21 квітня 2021 року: https://reyestr.court.gov.ua/Review/96501519.
64. Рішення Верховного Суду у справі № 806/3265/17 від 26 березня 2018 року: https://reyestr.court.gov.ua/Review/73139306.

У цій справі позивач (фізична особа) вимагав в АТ «Альфа-Банк», ПАТ «Міжнародне бюро кредитних історій», ПАТ «Перше всеукраїнське бюро кредитних історій», ТОВ «Українське бюро кредитних історій» вилучити (видалити) всю інформацію про себе, що міститься в кредитній історії за укладеними між ним (позивачем) та АТ «Альфа-Банк» кредитними договорами.

Складність справи полягає в тому, що частину кредитного договору («Розділ 2. Загальні умови кредитування фізичних осіб в ПАТ «Альфа-Банк») рішенням Шевченківського районного суду м. Києва від 20 лютого 2018 року у справі № 761/31008/14-ц визнано недійсним. А також заочним рішенням Шевченківського районного суду м. Києва від 20 липня 2017 року у справі № 761/43389/16-ц встановлено, що сторони не погодили в письмовій формі Розділ 2. Договору «Загальні умови кредитування фізичних осіб в ПАТ «Альфа-Банк» та відповідно до закону він нікчемний. Відповідні частини договору власне містили положення щодо згоди на обробку персональних даних.

Попри це, позивач при укладенні договору кредитування також заповнив Анкету-Заяву на отримання кредиту, якою фактично надав свою письмову безумовну згоду на доступ банку до його кредитної історії, вчинення Банком будь-яких дій та/або сукупності дій, що пов'язані зі збиранням, реєстрацією, накопиченням, зберіганням, адаптуванням, зміною, доповненням, використанням і поширенням (розповсюдженням, реалізацією, передачею), знеособленням, знищенням інформації. Відповідно, Шевченківський районний суд м. Києва[65], Київський апеляційний суд[66] та Верховний Суд[67] встановили, що заповнена Анкета-Заява достатня з огляду на дотримання письмової форми та поінформованості особи (позивача) про можливі наслідки – використання та розповсюдження персональних даних через бюро кредитних історій інформації про нього порядком, визначеним Законом України «Про організацію формування та обігу кредитних історій» з метою ухвалення банком рішення щодо можливості надання кредиту.

Закон як підстава для обробки персональних даних

На підставі закону обробка персональних ведеться в межах реалізації наданих органові публічної влади повноважень. Традиційний тут підхід, коли одержання згоди від суб'єкта персональних даних на обробку його персональних даних не вимагається у разі витребування таких даних суб'єктом владних повноважень у межах наданих йому повноважень. Така позиція не тільки поширена в діяльності органів державної влади та органів місцевого самоврядування, але й підтверджується судовою практикою. У справі № 520/4861/19 Верховний Суд, погодившись з позиціями судів першої та апеляційної інстанцій, зазначив:

«Враховуючи встановлені судами попередніх інстанцій обставини Верховний Суд погоджується з висновками судів попередніх інстанцій про те, що ці запити не містять відомостей щодо збирання конфіденційної інформації безпосередньо стосовно позивача, зокрема щодо його освіти, оскільки інформація щодо порядку зарахування, умов збереження заробітної плати на час навчання, період та графік навчального процесу, яка була предметом листування, не є такою, що згідно з Закону України «Про захист персональних даних» належить до конфіденційної.

39. Також Верховний Суд вважає, що суди правильно врахували крім іншого, що у разі, якщо до посади, пов'язаної з виконанням функцій держави або органів місцевого самоврядування, встановлені кваліфікаційні чи інші обов'язкові для займання цієї посади вимоги, такі як

65. Рішення Шевченківського районного суду м. Києва у справі № 761/8791/19 від 07 серпня 2019 року: https://reyestr.court.gov.ua/Review/83817241.
66. Постанова Київського апеляційного суду у справі № 761/8791/19 від 19 листопада 2019 року: https://reyestr.court.gov.ua/Review/85804485#.
67. Постанова Верховного Суду у справі № 761/8791/19 від 11 листопада 2020 року: https://reyestr.court.gov.ua/Review/92934787.

освіта, досвід роботи, знання іноземної мови, відсутність судимості тощо, то така інформація не є конфіденційною.

40. Крім цього, Верховний Суд звертає увагу, що спірні правовідносини виникли між ОСОБА_1 як працівником та Головним управлінням ДФС у Харківській області як роботодавцем. Отже, ці правовідносини перед усім стосуються проходження позивачем публічної служби та виникли у зв'язку з виконанням відповідачем приписів законодавства щодо належного забезпечення ним як роботодавцем такого проходження. З вказаного висновується, що ці правовідносини мають специфічних характер і запити Головним управлінням ДФС у Харківській області інформації не можу вважатись збиранням інформації щодо освіти позивача»[68].

Окрім приписів пункту 2 частини першої статті 11 Закону України «Про захист персональних даних» (дозвіл на обробку персональних даних, наданий володільцеві персональних даних відповідно до закону лише для здійснення його повноважень), важливий також припис частини четвертої статті 19 цього ж закону, яким передбачено, що органи державної влади та органи місцевого самоврядування мають право на безперешкодний і безоплатний доступ до персональних даних відповідно до їхніх повноважень. Власне, діяльність органів публічної влади в цій частині, зазвичай не ставиться під сумнів. Разом з тим є приклади судових рішень, коли суб'єкти персональних даних намагаються поставити під сумнів можливість відповідної діяльності суб'єктів владних повноважень. У справі № 331/811/20 позивач (фізична особа) намагався заборонити органам державної влади збирати та використовувати його персональні дані, що збиралися з метою ведення державного контролю у сфері земельних правовідносин та можливого притягнення його (позивача) до юридичної відповідальності. У цій справі суд першої інстанції зазначив:

«Враховуючи вищенаведене, суд приходить до висновку, що оскільки відповідач отримав паспорт ОСОБА_1 при здійсненні ним своїх владних повноважень при здійсненні ним своїх функцій, твердження позивача про порушення останнім вимог Закону України «Про захист персональних даних», «Про інформацію» є безпідставним, а позовні вимоги в частині визнання протиправними дії відповідача щодо збору персональних даних про ОСОБА_1 у вигляді усного запиту до сільради про надання копії паспорту громадянина України ОСОБА_1 і ідентифікаційного коду ОСОБА_1 , визнання протиправними дій відповідача щодо поширення розповсюдження персональної інформації про ОСОБА_1 , надання копії паспорту громадянина України ОСОБА_1 та її ідентифікаційного коду у судовій справі 280/4481/19 судді Васильченко В. В. справа №318/2377/19 і в судді Кіяшко В. О. справа 314/3496/19 та невизначеному колу осіб, зобов'язання відповідача, утримуватися від будь якого збирання, зберігання, використання та поширення персональної інформації про особу позивача та особу ОСОБА_2 , а саме інформацію щодо освіти, сімейного стану, стану здоров'я, адреси, дати місця народження, майнового стану, документи та інші персональні дані без його попередньої письмової на це згоди є безпідставними»[69].

Суд апеляційної інстанції[70] підтримав позицію суду першої інстанції.

На підставі закону отримувати доступ до персональних даних (збирати та обробляти їх) можуть не тільки посадові та службові особи органів державної влади, але й інші уповноважені на це суб'єкти. Наприклад, у справі № 750/6287/17 йшлося про можливість отримувати персональні

68. Постанова Верховного Суду у справі № 520/4861/19 від 23 грудня 2020 року: https://reyestr.court.gov.ua/Review/93791888.
69. Рішення Жовтневого районного суду м. Запоріжжя у справі № 331/811/20 від 21 вересня 2020 року: https://reyestr.court.gov.ua/Review/91766748.
70. Постанова Запорізького апеляційного суду у справі № 331/811/20 від 17 березня 2021 року: https://reyestr.court.gov.ua/Review/95731172.

дані фізичної особи від її роботодавця на запит адвоката. Цікаве те, що суд першої та апеляційної інстанції зайняли протилежні позиції. Деснянський районний суд м. Чернігова зазначив:

«Адвокат ОСОБА_5 звертався до відповідача із адвокатським запитом у справі за позовом ОСОБА_6 до ОСОБА_3 про відшкодування шкоди, для перевірки можливості останньої відшкодовувати завдану шкоду, оскільки вона повідомляла суд про низькі доходи та відсутність можливості відшкодовувати шкоду. Даний адвокатський запит направлявся в рамках розгляду Деснянським районним судом міста Чернігова цивільної справи № 750/7594/16-ц. Правомірність цього запиту та наявність підстав для надання за ним відповідної інформації перевірялась з урахуванням положень ст. ст. 20, 23, 24 Закону України «Про адвокатуру і адвокатську діяльність». При цьому за неправомірну відмову в наданні інформації, несвоєчасне або неповне надання інформації, надання інформації, що не відповідає дійсності, у відповідь на адвокатський запит, передбачено адміністративну відповідальність згідно ст. 212-3 Кодексу України про адміністративні правопорушення.

Крім цього, надання вказаної інформації на адвокатський запит не є розкриттям персональних даних позивача, оскільки сума заборгованості по заробітній платі та компенсації за затримку розрахунку при звільненні була стягнута ОСОБА_3 з ПАТ «БК «Домобудівник» в судовому порядку, а згідно частини другої статті 2 Закону України «Про доступ до судових рішень», усі судові рішення є відкритими та підлягають оприлюдненню в електронній формі не пізніше наступного дня після їх виготовлення і підписання»[71].

Водночас, Апеляційний суд Чернігівської області постановив:

«…апеляційний суд доходить висновку про те, що подання відповідачем на запит адвоката ОСОБА_8, в якому було запрошено інформацію з обмеженим доступом, листа за № 02/32/1/263 від 19 листопада 2016 року за підписом головного бухгалтера ПАТ «Домобудівник» ОСОБА_5, який містив інформацію про невиконані боргові зобов'язання ПАТ «Будівельна компанія «Домобудівник» перед ОСОБА_2, про стан виконання зазначених грошових зобов'язань, отримані останньою грошові суми є поширенням без згоди ОСОБА_2 інформації про її майновий стан, яка за ступенем захисту віднесена до конфіденційної.

Такі дії ПАТ «Будівельна компанія «Домобудівник» є протиправними, оскільки всупереч положенням ч.2 ст. 14 Закону України «Про захист персональних даних» ним було допущено поширення персональних даних (відомостей про майновий стан) без згоди на те суб'єкта персональних даних, чим порушено конституційне право ОСОБА_2 на недоторканність особистого і сімейного життя»[72].

Верховний Суд у цій справі зайняв позицію суду першої інстанції та скасував рішення суду апеляційної інстанції, зазначивши:

«Відмовляючи у задоволенні позову, суд першої інстанції обґрунтовано виходив із того, що надана відповідачем на адвокатський запит інформація про стан боргових зобов'язань перед позивачем не є розкриттям персональних даних останньої та не є конфіденційною відповідно до положень Закону України «Про захист персональних даних», оскільки сума заборгованості по заробітній платі та компенсації за затримку розрахунку при звільненні була стягнута з ПАТ «БК «Домобудівник» на користь ОСОБА_1 в судовому порядку, а згідно з частиною другою статті 2 Закону України «Про доступ до судових рішень» усі судові рішення є відкритими та підлягають оприлюдненню в електронній формі не пізніше наступного дня після їх виготовлення і підписання.

71. Рішення Деснянського районного суду м. Чернігова у справі № 750/6287/17 від 15 серпня 2017 року: https://reyestr.court.gov.ua/Review/68373375.
72. Рішення Апеляційного суду Чернігівської області у справі № 750/6287/17 від 22 вересня 2017 року: https://reyestr.court.gov.ua/Review/69133281.

Суд першої інстанції обґрунтовано виходив із того, що інформація, яку запитав адвокат, стосувалась виконання судового рішення, оприлюдненого та такого, що набрало законної сили, відповідач не мав будь-яких підстав не відповідати на запит адвоката, ця інформація була пов'язана з розглядом справи, де стороною є позивач, інформація надана у відповіді на адвокатський запит не може бути визнана конфіденційною у розумінні зазначених вимог закону.

Оскільки під час дослідження доказів та встановлення фактів у справі, судом першої інстанції не були порушені норми процесуального права, правильно застосовані норми матеріального закону, тому рішення суду є законним і обґрунтованим»[73].

Цей аспект застосування законодавства про захист персональних даних доволі складний для практичної реалізації. В окремих випадках суди доволі буквально застосовують положення відповідного законодавства та визнають законною відмову в наданні інформації на адвокатський запит навіть стосовно клієнта за відповідним договором. Наприклад, у справі № 802/2149/17-а суд першої інстанції[74], а згодом і апеляційний[75] суд відмовили в оскарженні адвокатом відмови в наданні інформації про клієнта. При цьому суди проводили навіть аналіз договору про надання правової допомоги. З огляду на різні підходи тут набагато частіше трапляються ситуації, коли суди першої та вищих інстанцій займають різні позиції, зокрема з обґрунтуванням власної позиції обставинами справи[76].

Разом з тим є чимало прикладів судових рішень, де застосовується підхід і аргументація, аналогічні до висловлених Верховним Судом у цитованій вище справі № 750/6287/17[77]. Це досить чіткий приклад того, як аргументована позиція Верховного Суду стає орієнтиром та основою для структуризації судової практики в певній сфері.

На окрему увагу заслуговує аналіз обробки чутливих даних. Адже збирання та обробка персональних даних вимагає ретельнішого як нормативного регулювання зазначених питань, так і відповідних адміністративних (управлінських) процедур. Найчастіше проблемні питання виникають із захистом персональних даних у сфері охорони здоров'я. На жаль, досить часто по-різному тлумачать і застосовують приписи Закону України «Про захист персональних даних» не тільки посадові особи органів публічної влади та/або співробітники закладів охорони здоров'я, але й суди.

Доволі поширене хибне розуміння змісту та обсягу можливих дій з чутливими персональними даними, коли йдеться про необхідність вжиття заходів органами публічної влади в інтересах самої особи чи близьких їй осіб (наприклад, встановлення опіки чи піклування щодо особи). У таких ситуаціях як органи публічної влади, так і співробітники закладів охорони здоров'я досить вільно трактують приписи Закону України «Про захист персональних даних» в частині

73. Постанова Верховного Суду у справі № 750/6287/17 від 20 листопада 2019 року: https://reyestr.court.gov.ua/Review/85836173.
74. Постанова Вінницького окружного адміністративного суду у справі № 802/2149/17-а від 06 грудня 2017 року: https://reyestr.court.gov.ua/Review/71146277.
75. Постанова Вінницького апеляційного адміністративного суду у справі № 802/2149/17-а від 22 березня 2018 року: https://reyestr.court.gov.ua/Review/73041740.
76. Див., наприклад, справу № № 823/1244/17 (Постанова Черкаського окружного адміністративного суду від 01 листопада 2017 року: https://reyestr.court.gov.ua/Review/69999117 та Постанову Київського апеляційного адміністративного суду від 13 грудня 2017 року: https://reyestr.court.gov.ua/Review/71073598); справу № 260/1349/18 (рішення Закарпатського окружного адміністративного суду від 23 січня 2019 року: https://reyestr.court.gov.ua/Review/79340144 та Постанова Восьмого апеляційного адміністративного суду від 27 травня 2019 року: https://reyestr.court.gov.ua/Review/82194085).
77. Див., наприклад, Рішення Львівського окружного адміністративного суду у справі № 380/11843/20 від 17 лютого 2021 року: https://reyestr.court.gov.ua/Review/94966560; Рішення Харківського окружного адміністративного суду у справі № 520/8073/21 від 14 липня 2021 року: https://reyestr.court.gov.ua/Review/98335992; Рішення Донецького окружного адміністративного суду у справі № 200/12018/21 від 18 жовтня 2021 року: https://reyestr.court.gov.ua/Review/100400945 та ін.

розголошення персональних даних (інформації про особу, відомостей медичного характеру, зокрема діагнозу, строків та особливостей лікування тощо) та поширюють документи, що містять персональні дані, не вдаючись до отримання згоди суб'єкта персональних даних, а інколи й всупереч вимогам спеціального законодавства. На жаль, до такого ж способу тлумачення часто вдаються й суди.

Як приклад, у справі № 359/7520/17 суд першої інстанції оцінив надсилання головним лікарем Бориспільської ЦРЛ листа з діагнозом позивачки («шизотиповий розлад») та відповідного акта судово-психіатричного експерта до міського голови, іншого закладу охорони здоров'я та судів як таке, що не порушує вимоги законодавства про захист персональних даних. Бориспільський міськрайонний суд Київської області мотивував своє рішення тим, що поширення відповідних персональних даних велося з метою захистити права іншої особи (матері позивачки), щодо якої позивачка виконувала функції законного опікуна, а через виявлений розлад здоров'я надалі не могла цього робити. Суд, зокрема, зазначив:

«5.2. Дійсно, починаючи з 2014 року ОСОБА_1 перебувала на консультативному обліку у лікаря-психіатра в Бориспільській ЦРЛ. Рішенням Бориспільського міськрайонного суду від 12 серпня 2015 року було відмовлено ОСОБА_1 у задоволенні позову про зняття її з консультативного обліку. Тому звернення головного лікаря Бориспільської ЦРЛ ОСОБА_7 до Бориспільського міського голови Федорчука А.С. та направлення йому акту судово-психіатричного експерта №664 від 12 серпня 2014 року було спрямовано виключно на захист прав недієздатної ОСОБА_6 . Ці обставини переконливо свідчать про те, що дії головного лікаря Бориспільської ЦРЛ повністю кореспондуються з ч.2 ст.11 Закону України «Про інформацію» та п.6 ч.2 ст.7, ч.2 ст.14, ч.1 ст.25 Закону України «Про захист персональних даних». Крім того, направлення посадовими особами Бориспільської ЦРЛ копій акту судово-психіатричного експерта №664 від 12 серпня 2014 року до Бориспільського міськрайонного суду та Апеляційного суду Київської області є способом виконання процесуального обов'язку з подання доказів, а не незаконною обробкою та поширенням персональних даних ОСОБА_1 .

5.3. 12 листопада 2015 року генеральний директор КЗ КОР «Обласне психіатрично-наркологічне об'єднання» Зільберблат Г.М. надіслав головному лікарю Бориспільської ЦРЛ ОСОБА_7 лист (а.с.19 т.1), в якому він просив надіслати копію акту судово-психіатричного експерта №664 від 12 серпня 2014 року. Однак в матеріалах цивільної справи відсутні докази на підтвердження того, що головний лікар Бориспільської ЦРЛ ОСОБА_7 надіслав генеральному директору КЗ КОР «Обласне психіатрично-наркологічне об'єднання» Зільберблату Г.М. копію вказаного акту. Крім того, допитана у судовому засіданні ОСОБА_1 показала, що вона не надавала посадовим особам Бориспільської ЦРЛ згоду на обробку та поширення її персональних даних, що містяться в акті судово-психіатричного експерта №664 від 12 серпня 2014 року. Водночас, за правилом ч.2 ст.11 Закону України «Про інформацію» та п.6 ч.2 ст.7, ч.2 ст.14, ч.1 ст.25 Закону України «Про захист персональних даних» потреба в отриманні від позивача такої згоди була відсутньою. Тому показання ОСОБА_1 є неналежним доказом в розумінні ст.77 ЦПК України.

4.4. З огляду на це суд вважає, що підстави для визнання незаконною обробку та пши5ення Бориспільською ЦРЛ персональних даних ОСОБА_1 , а також для знеособлення та знищення її персональних даних відсутні. Тому у задоволенні пред'явленого нею позову належить відмовити»[78].

У цій ситуації суд першої інстанції доволі широко розтлумачив приписи пункту 6 частини другої статті 7, частини другої статті 14 та частини першої статті 25 Закону України «Про захист персональних даних». Власне, суд положення законодавства щодо можливості обмеження дії гарантій захисту персональних даних в інтересах захисту прав і свобод суб'єктів персональних даних чи

78. Рішення Бориспільського міськрайонного суду Київської області у справі № 359/7520/17 від 28 жовтня 2020 року: https://reyestr.court.gov.ua/Review/92712245.

інших осіб застосував доволі загально, без дослідження всіх обставин справи та належної аргументації. На це звернув увагу згодом і суд апеляційної інстанції:

«Відмовляючи у задоволенні позову […] суд першої інстанції виходив з того, що такі дії були спрямовані виключно на захист прав недієздатної ОСОБА_8 . Потреба в отриманні від позивача згоди на обробку та поширення її персональних даних за правилами ч.2 ст.11 Закону України «Про інформацію», п.6 ч.2 ст.7 , ч. 2ст.14, ч.1 ст.25 Закону України «Про захист персональних даних» була відсутньою…

Колегія суддів не може погодитись з висновками суду першої інстанції з огляду на таке.

… Запит […] щодо направлення копії акту судово-психіатричної експертизи «в порядку виключення» не містить жодного обґрунтування необхідності отримання інформації, що стосувалася здоров'я позивача, без отримання згоди останньої.

Відповідачем також не доведено, що направлення вказаного акту по запиту генерального директора Зільберблата Г. М. від 12.11.2015 та в додатку до листа № 165 від 02.09.2015 Бориспільському міському голові ОСОБА_5 було необхідним в цілях охорони здоров'я, встановлення медичного діагнозу, для забезпечення піклування чи лікування або надання медичних послуг, функціонування електронної системи охорони здоров'я тощо…

Обробка персональних даних позивача у даних випадках не могла здійснюватися без згоди суб'єкта персональних даних.

Випадків, визначених законом, для надіслання персональних даних позивача вказаним особам судом не встановлено.

Матеріали справи також не містять доказів, що таке поширення персональних даних позивача здійснювалася в інтересах національної безпеки, економічного добробуту та прав людини»[79].

Це досить яскравий приклад, коли суди, застосовуючи обмеження гарантій безпеки персональних даних, не вдаються до детального та глибокого обґрунтування вжитих заходів. Особливо складне в цій ситуації те, що йдеться про чутливі персональні дані, які дійсно можуть вплинути на соціальний статус, репутацію та відчуття власної гідності особи.

Інший цікавий приклад, коли здійснене медичним працівником «… надання інтерв'ю сторонній особі і розголошення відомостей про пацієнта із зазначенням його прізвища, проведення операції, знеболення сибазоном, вживання твердження, що пацієнт є наркоманом, вживає наркотичні засоби і в нього були ломки» суд першої інстанції не оцінив як незаконне поширення персональних даних. Проте на рівні апеляційної та касаційної інстанцій відповідне помилкове тлумачення обставин було виправлене[80].

Показовий приклад віднесення інформації до категорії з обмеженим доступом представлено в страві № 806/4543/14, де йдеться про оскарження позивачем (фізичною особою) дій начальника колишнього роботодавця (Державної інспекції сільського господарства в Житомирській області) щодо направлення до лікарні запиту про «повідомлення коли та о котрій годині звернувся та чи взагалі звертався до ЦМЛ №1 ОСОБА_3, якою була підстава для звернення, який діагноз

79. Постанова Київського апеляційного суду у справі № 359/7520/17 від 10 лютого 2021 року: https://reyestr.court.gov.ua/Review/94886593.
80. Див. Рішення Заводського районного суду м. Миколаєва у справі № 487/1982/17 від 26 березня 2018 року: https://reyestr.court.gov.ua/Review/73131097; Постанова Апеляційного суду Миколаївської області у справі № 487/1982/17 від 23 травня 2018 року: https://reyestr.court.gov.ua/Review/74202704 та Постанова Верховного Суду у справі № 487/1982/17 від 20 травня 2019 року: https://reyestr.court.gov.ua/Review/81925629.

був встановлений та чи прийом відбувався в порядку попереднього запису чи живої черги». Суд першої інстанції позов задовольнив, зазначивши:

«Отже, незаконним збиранням інформації – є обробка, тобто збирання без згоди фізичної особи інформації про її стан здоров'я, факт звернення за медичною допомогою, діагноз, а також про відомості, одержані при медичному обстеженні.

В судовому засіданні представник позивача зазначив, що ОСОБА_3 не давав відповідачу своєї згоди чи дозволу на збирання інформації про стан його здоров'я та інші свої персональні дані медичного характеру, тим більше, не надавав йому згоди на збирання ним такої інформації, що становить таємницю про стан здоров'я людини. Представником відповідача дана обставина не спростована.

Крім того, згідно статті 39-1 Основ законодавства України про охорону здоров'я, людина має право на таємницю про стан свого здоров'я, факт звернення за медичною допомогою, діагноз, а також про відомості, одержані при його медичному обстеженні. Вимагати інформацію про діагноз та методи лікування пацієнта забороняється.

Отже, збирання та зберігання інформації про стан здоров'я особи без її попередньої згоди є неправомірним»[81].

При цьому суд апеляційної інстанції тільки частково погодився з такою аргументацією і зазначив, що до інформації з обмеженим доступом можуть належати лише відомості про діагноз особи (позивача), проте, всі інші відомості, які запитував відповідач, на думку суду, не можуть належати до конфіденційної інформації. У рішенні суду апеляційної інстанції зазначено:

«Отже, інформація про стан здоров'я особи підлягає захисту як одна із найвразливіших складових персональних даних, оскільки охоронюваним законодавством інтересом особи є захист її приватності від будь-якого стороннього втручання. Така інформація є конфіденційною, відомою лише обмеженому колу осіб, які отримали до неї доступ внаслідок виконання своїх професійних обов'язків. Надання зазначеної інформації на запит призводитиме до її розголошення та поширення на невизначене коло осіб, що становитиме втручання у приватність особи, приверне пильну увагу до стану її здоров'я, спричинить моральний дискомфорт та переживання.

Тому, колегія суддів погоджується із висновком суду першої інстанції в частині щодо визнання неправомірними дій відповідача, що полягали в незаконному збиранні та зберіганні конфіденційної інформації про медичний діагноз позивача шляхом направлення відповідного запиту до медичної установи, чим допущено порушення його основоположних прав.

В решті – дії відповідача щодо збирання та зберігання інформації про час звернення ОСОБА_3 до медичної установи, підставу такого звернення та порядок проведення його прийому в медичній установі є правомірними, оскільки така інформація не може відноситись до категорії конфіденційної, а обмеження доступу до неї не є винятковим. Така інформація не може виключатися із загального режиму доступу, що ґрунтується на постулаті відкритості, та не може суперечити основоположному праву на доступ до інформації як такому. Доступ обмежується лише в тому обсязі, який є необхідним і відповідає законодавчо встановленим умовам, наявність яких вимагається для обмеження допуску до інформації. Тому, колегія суддів вважає, що у вказаній частині дії відповідача вчинені на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України.

81. Постанова Житомирського окружного адміністративного суду у справі № 806/4543/14 від 02 березня 2015 року: https://reyestr.court.gov.ua/Review/42988141.

Доводи апелянта щодо покладення відповідальності за поширення інформації про позивача на її володільця – медичну установу є безпідставними, оскільки предметом спору є дії щодо збирання та зберігання такої інформації, що не є тотожними, а є відмінними за своєю правовою природою. Згода позивача на адресу роботодавця про збір та обробку персональних даних випливає та пов'язана із правовідносинами у сфері законодавства щодо реалізації його права на державну службу, а тому не може розцінюватися згодою на обробку конфіденційної інформації про стан здоров'я особи, якої стосується запитувана інформація»[82].

Таке рішення суду апеляційної інстанції вмотивоване, напевно, додатковими обставинами конкретної справи, які обумовили потребу розмежування рівня захисту інформації про факт і обставини звернення по медичну допомогу від діагнозу. Хоч і в цьому випадку аргументація суду могла б бути глибшою та розгорнутішою, бо йдеться про чутливі дані, тож мета та інструменти втручання в приватне життя мають бути ретельно обґрунтованими.

82. Постанова Житомирського апеляційного адміністративного суду у справі № 806/4543/14 від 06 квітня 2015 року: https://reyestr.court.gov.ua/Review/43479414.

ПРОПОРЦІЙНІСТЬ

Пропорційність у сфері персональних даних проявляється у вимозі пошуку розумного балансу між приватним та суспільним інтересом; між метою регулювання та обставинами практичної реалізації відповідних нормативних приписів; між визначеним способом втручання в приватне життя й очікуваними результатами в низці інших аспектів.

Ключове тут сумірне обмеження прав людини з безумовним урахуванням легітимної мети такого обмеження та постійним контролем доречності (релевантності) встановлених меж. Цей принцип також характеризують через вимоги адекватності, відповідності та ненадмірності. Тут запропоновано аналіз крізь призму двох основних складників:

- пропорційність обсягу обмеження – йдеться про межі, визначені законом для допустимого в демократичному суспільстві втручання в приватне життя. Загалом йдеться про мінімізацію обробки персональних даних – там, де відповідної мети можна досягнути без втручання в приватне життя, це має бути реалізовано без обробки персональних даних;
- пропорційність інструментів – ідеться про можливість застосування обмежень лише способом, відповідним меті та передбаченим законом без застосування надмірних форм впливу на персональні дані і, як наслідок, на глибину втручання в приватне життя.

Застосування «трискладового» тесту щодо меж обмеження прав людини, або ж інший спосіб верифікації допустимої глибини втручання в приватне життя має відбуватися в кожному конкретному випадку з урахуванням усіх обставин справи. Так, наприклад, при здійсненні обробки персональних даних для легітимного інтересу володілець має застосовувати принцип балансу інтересів, а саме володільцю необхідно порівняти потенційну шкоду для особи (суб'єкт даних) від розголошення персональних даних з правом громадськості (суспільний інтерес) знати цю інформацію в інтересах національної безпеки, економічного добробуту чи прав людини. Якщо ця шкода не переважає суспільний інтерес в доступі до особистої інформації, то інформація може бути розголошена і доступ до неї не може бути обмежений.

Пропорційність обсягу обмеження

Питання обсягу втручання в приватне життя доволі делікатне та потребує ретельного аналізу в кожному конкретному випадку. Суди далеко не завжди вдаються до глибокого аналізу змісту/обсягу персональних даних і сумірності їх використання з визначеною метою. Особливо складні випадки, коли це стосується спорів щодо обробки електронних даних чи персональних даних в інтернеті. Як приклад, справа № 752/1042/21, що її розглядали Голосіївський районний суд м. Києва[83] та Апеляційний суд м. Києва[84].

У цій справі позивач (фізична особа), який користується поштовим сервісом Товариства з обмеженою відповідальністю «Укрнет», вважає надмірним і непропорційним збирання та обробку певних персональних даних. Він зазначає, що « …відповідно до п. 4 Угоди про конфіденційність, володілець здійснює збір та обробку персональних даних користувача будь-якими способами з метою належного надання користувачу послуг електронної пошти FREEMAIL (ідентифікація,

83. Рішення Голосіївського районного суду м. Києва у справі № 752/1042/21 від 17.05.2021 року: https://reyestr.court.gov.ua/Review/97431732#.
84. Постанова Київського апеляційного суду у справі № 752/1042/21 від 07 жовтня 2021 року: https://reyestr.court.gov.ua/Review/100214431.

аутентифікація, авторизація, відновлення пароля, надсилання інформаційних матеріалів за підпискою користувача, відповідей на запити та листи користувача, а також – для інших дій, що час від часу необхідні для належного надання послуг Сервісу), проте, обробка персональних даних – log-файлів є надмірною відносно зазначеної мети»[85].

При розгляді цієї справи як суд першої інстанції, так і суд апеляційної інстанції не досліджували питання пропорційності (сумірності) мети збору персональних даних та їх обсягу, передбаченого Угодою про конфіденційність. Очевидно, одна з причин цього те, що позивач не брав безпосередньо участі в судових засіданнях і не додав необхідних судові доказів та аргументів власної позиції. «Позивач не довів належними засобами доказування, що обробка спірних персональних даних є невідповідною, неадекватною та є надмірною стосовно мети, визначеної Угодою про конфіденційність»[86]. Відповідно, у кожному із зазначених рішень суди з посиланням на відповідні приписи Цивільного процесуального кодексу України відмовили в задоволенні вимог позивача.

Разом з тим детальний аналіз сумірності мети та обсягу збирання персональних даних (у частині розгляду мети та спрямованості використання log-файлів при функціонуванні поштового сервісу) за належної глибини аналізу міг би вплинути на аргументацію судового рішення, а можливо, й на зміст остаточних рішень судів.

Традиційні для характеристики принципу пропорційності в цій сфері справи щодо пошуку балансу між втручанням у приватне життя особи та суспільним інтересом. Найчастіше цей делікатний баланс судам доводиться шукати у справах щодо приватного життя публічних осіб та/або членів їхніх сімей. У цій частині міжнародні стандарти та практика ЄСПЛ доволі обширні та детальні. Суди в Україні доволі часто саме в цій категорії справ вдаються до безпосереднього використання аргументації з рішень ЄСПЛ. При цьому оцінювання всіх обставин саме пропорційності втручання проводиться не завжди достатньо глибоко та/або з використанням теоретичних елементів (складників) принципу пропорційності. Показовим тут можу бути справа № 761/44774/17, де суд зазначив:

«Проте суд не може взяти до уваги зазначені пояснення так як інформація особисто про ОСОБА_8 не є виправданим втручанням в особисте сімейне життя позивача ОСОБА_2 та відповідне поширення таких даних. Опублікування фотографій, поширення даних про сімейний стан померлого ОСОБА_8, його близькі відносини з іншими особами, майновий стан напряму стосується Позивача, як його дружини, та є явно надмірним і непропорційним втручанням у приватність.

Крім того суд не може взяти до уваги посилання відповідача, що так як ОСОБА_8 був публічною особою, тому інформація викладена в статті має великий суспільний інтерес, оскільки в статті не висвітлюється діяльність ОСОБА_8 як публічної особи, а висвітлюються особисті стосунки, майнові відносини спадкоємців. Крім того, дружина померлого ОСОБА_8 не є публічною особою.

Таким чином, в поширеному відео та в самих статтях Відповідачем протиправно поширювалась інформація про приватне життя позивача та персональні дані Позивача і членів її сім'ї»[87].

У цій справі суд загалом коректно застосував відповідні приписи національного законодавства та зробив доволі широке посилання на міжнародні стандарти. Попри це, характеристиці самої пропорційності (розумного балансу між приватним життям і суспільним (публічним) інтересом) приділено уваги (аналізові обставин справи та відповідній аргументації) не так багато.

85. Текст із Постанови Київського апеляційного суду у справі № 752/1042/21 від 07 жовтня 2021 року: https://reyestr.court.gov.ua/Review/100214431.
86. Текст з Рішення Голосіївського районного суду м. Києва у справі № 752/1042/21 від 17.05.2021 року: https://reyestr.court.gov.ua/Review/97431732#.
87. Рішення Шевченківського районного суду м. Києва у справі № 761/44774/17 від 23 січня 2019 року: https://reyestr.court.gov.ua/Review/79881631.

Приписи частини другої статті 14 Закону України «Про захист персональних даних» досить часто тлумачать надміру широко, чим уможливлюють поширення персональних даних без достатніх законних підстав. Відповідно до означеного припису поширення персональних даних без згоди суб'єкта персональних даних або уповноваженої ним особи дозволяється у випадках, визначених законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини. Власне кажучи, «в інтересах прав людини» доволі часто сприймається досить широко. Принцип пропорційності вимагає комплексного оцінювання всіх обставин кожної конкретної справи та дозволяє вдаватися до обмеження захисту персональних даних – поширення без згоди їх суб'єкта, як виняток, тільки в ситуації, якщо іншим способом досягнути необхідної мети неможливо.

Показова тут справа № 681/336/14-а, де позивач (фізична особа) звернувся з вимогою до Головного управління Пенсійного фонду України у Хмельницькій області щодо надання йому довідки про те, чи отримує соціальну допомогу його колишня дружина на їхню спільну дочку. Очевидно, на звичайне звернення позивача адміністративним порядком відповідач відмовив. Разом з тим судовим порядком вимога позивача була задоволена. Аргументація суду в цій ситуації була доволі лаконічна, без згадування принципу пропорційності, але з фактичним застосуванням його елементів. Суд, зокрема, проаналізував інші можливі способи захисту права людини (позивача), наприклад, через поширення на відповідні правовідносини дії Закону України «Про доступ до публічної інформації». Не знайшовши іншого способу захистити право особи на соціальний захист, суд вдався до обмеження гарантій персональних даних в інтересах права людини. Зокрема, суд зазначив:

«Інформація про звертання ОСОБА_4 за соціальною допомогою на неповнолітню дитину не належить до публічної інформації, тому що така інформація не являється метою та предметом виконання УПСЗ своїх владних повноважень.

Дані про звертання ОСОБА_4 до УПСЗ за соціальною допомогою на неповнолітню дитину є конфіденційною інформацією з обмеженим доступом, а не публічною інформацією.

ОСОБА_5 не має іншої можливості захисти свої права, крім як отримання персональних даних ОСОБА_4 Отримання ним персональних даних ОСОБА_4 у вигляді інформації з УПСЗ не порушують прав, свобод чи інтересів ОСОБА_4 Право позивача ОСОБА_5 отримати ці персональні дані передбачено законом. Тому позовні вимоги є обґрунтованими і підлягають задоволенню»[88].

При здійсненні повноважень органи державної влади можу витребувати інформацію лише обсягом, необхідним для конкретних адміністративних (управлінських) дій. Вимога надати непропорційно великий обсяг інформації, що містить персональні дані, повинна бути визнана незаконною. Тут показовою може бути справа № 820/10192/15, де за результатами перевірки підприємства державною податковою інспекцією витребувано не тільки первинні документи, але й відносно великий масив даних щодо членів відповідної організації (йдеться про Книжковий клуб «Клуб сімейного дозвілля», який поширює книжки у відносно великих масштабах), для яких робилися знижки. А саме вимагався «перелік членів Клубу, яким надавались знижки з вказанням ПІБ, ідентифікаційного номеру, номеру картки, переліку придбаної продукції з вказанням розміру знижки за 2013–2014 роки в розрізі місяців; по кожному члену Клубу надати обґрунтування розміру наданої знижки»[89]. Такий обсяг витребовуваної інформації суд визнав необґрунтованим. Зокрема, він зазначив:

88. Постанова Полонського районного суду Хмельницької області у справі № 681/336/14-а від 09 квітня 2014 року: https://reyestr.court.gov.ua/Review/38145429.
89. З тексту Постанови Харківського окружного адміністративного суду у справі № 820/10192/15 від 29 жовтня 2015 року: https://reyestr.court.gov.ua/Review/53324994.

«Також, суд зазначає, що відповідно до положень ст. 1 Закону України «Про захист персональних даних» від 01.06.2010 року №2297-VI, персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована; розпорядник персональних даних – фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця; суб'єкт персональних даних – фізична особа, персональні дані якої обробляються.

Згідно до ст. 10 вищевказаного Закону, використання персональних даних передбачає будь-які дії володільця щодо обробки цих даних, дії щодо їх захисту, а також дії щодо надання частково-го або повного права обробки персональних даних іншим суб'єктам відносин, пов'язаних із персональними даними, що здійснюються за згодою суб'єкта персональних даних чи відповідно до закону.

А отже, запитувана контролюючим органом в листі від 01.07.2015 року інформація щодо членів Клубу є персональною інформацією, розголошення якої допустимо лише за згодою суб'єкта персональних даних та у випадках, визначених законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини, а тому позивач відмовляючи відповідачу в наданні даної інформації діяв в межах закону, при цьому, не порушуючи охоронюваних прав та інтересів членів Клубу»[90].

Відповідне рішення підтримали суди апеляційної та касаційної інстанцій.

Пропорційність інструментів

Обиратися релевантний спосіб використання даних має ретельно та вкрай обережно в кожній конкретній ситуації. При цьому значення має не тільки спосіб використання, а й пошук розумного його (способу) балансу з метою такого використання.

Доречним тут може бути приклад щодо обов'язкового поширення певного виду інформації, наприклад, на виконання рішення суду. У справі № 622/224/21 суд першої інстанції досить чітко та однозначно розтлумачив зміст і спрямованість Закону України «Про захист персональних даних» в аспекті його застосування до оприлюднення резолютивної частини рішення суду в засобах масової інформації.

У цій справі йшлося про те, що позивач (фізична особа) в іншому судовому провадженні отримав судове рішення, яким серед іншого відповідача (Золочівську селищну раду Богодухівського району Харківської області) зобов'язано опублікувати резолютивну частину рішення суду у виданнях, у яких оскаржуваний нормативно-правовий акт був або мав бути офіційно оприлюднений. На виконання цих вимог відповідач оприлюднив резолютивну часину рішення повним обсягом, зокрема і з персональними даними позивача. Це і стало предметом наступного (аналізованого тут) судового позову щодо визнання незаконними дій Золочівської селищної ради Харківської області щодо поширення персональних даних позивача.

За результатами розгляду справи суд досить чітко розмежував вимоги закону щодо виконання судового рішення та вимоги законодавства про захист персональних даних. Не вдаючись до використання терміна «пропорційність» (баланс, сумірність чи аналогічних) суд досить добре застосував зміст відповідного принципу. У цій справі зважено зміст різних за своїм змістом нормативних вимог і, як результат, визнано незаконним обраний інструмент поширення персональних даних. Суд, зокрема, зазначив:

90. Постанова Харківського окружного адміністративного суду у справі № 820/10192/15 від 29 жовтня 2015 року: https://reyestr.court.gov.ua/Review/53324994.

«Згідно ч.1, 2 ст.14 Закону України «Про захист персональних даних» поширення персональних даних передбачає дії щодо передачі відомостей про фізичну особу за згодою суб'єкта персональних даних. Поширення персональних даних без згоди суб'єкта персональних даних або уповноваженої ним особи дозволяється у випадках, визначених законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини.

Відповідно до ч.2 ст.2 Закону України «Про доступ до судових рішень» судові рішення також можуть публікуватися в друкованих виданнях із додержанням вимог цього Закону.

Згідно п.1 ч.1 ст.7 Закону України «Про доступ до судових рішень» у текстах судових рішень, що відкриті для загального доступу, не можуть бути розголошені такі відомості як, зокрема місце проживання або перебування фізичних осіб із зазначенням адреси, реєстраційні номери облікової картки платника податків. Такі відомості замінюються літерними або цифровими позначеннями…

… Відповідачем не надано доказів того, що персональні дані позивача були поширені за згодою позивача, у відповідності до вимог закону, в інтересах національної безпеки, економічного добробуту та прав людини, відповідні документи та докази про існування згоди на це від позивача відсутні.

Таким чином, судом встановлено, що відповідачем незаконно здійснено поширення персональних даних позивача»[91].

Відповідне рішення суду не оскаржувалося апеляційним порядком.

Пропорційність має стосуватися не тільки інструментів збирання та обробки, але й використання чи поширення персональних даних. Особливо цікаві для аналізу справи, де використання чи поширення персональних даних ведеться у відповідь на втручання в приватне життя. Тут слід зазначити, що оцінювання пропорційності вжитих заходів суб'єктом персональних даних чи їхнім володільцем має робити суд у кожній конкретній ситуації з чітким розмежуванням окремих фактів (обставин, подій, епізодів тощо).

Змішування чи іншим способом «розмивання» оцінки змісту дій щодо кожного конкретного випадку можливого порушення вимог законодавства про захист персональних даних може призвести до помилкових висновків або й зовсім некоректного застосування приписів Закону України «Про захист персональних даних», або інших актів національного законодавства, або й міжнародних стандартів.

Наприклад, у справі № 757/15585/20-ц як суд першої інстанції[92], так і апеляційний[93] суд розглянули заявлене незаконне поширення персональних даних у взаємозв'язку з іншим порушенням законодавства про персональні дані тими ж суб'єктами але у зворотному порядку. Оцінка судом кожного з епізодів окремо могла б подати інші аргументи щодо правової характеристики цих ситуацій, а можливо, й привести суди й до іншого рішення за результатами розгляду справи.

Відповідно, коректне застосування принципу пропорційності вимагає системного та комплексного врахування всіх обставин справи, проте не може допускати змішування кількох різних за своєю природою та фактичними особливостями справ в одне провадження.

---

91. Рішення Золочівського районного суду Харківської області у справі № 622/224/21 від 15 квітня 2021 року: https://reyestr.court.gov.ua/Review/96374080.
92. Рішення Печерського районного суду м. Києва у справі № 757/15585/20-ц від 31 серпня 2020 року: https://reyestr.court.gov.ua/Review/91234408.
93. Постанова Київського апеляційного суд у справі № 757/15585/20-ц від 14 грудня 2020 року: https://reyestr.court.gov.ua/Review/93737901.

Пропорційність інструментів проявляється, зокрема й через вимогу строковості (обмеження конкретними часовими проміжками) зберігання та обробки персональних даних. Персональні дані підлягають зберіганню у формі, яка уможливлює ідентифікацію суб'єкта таких даних, не довше, ніж це необхідно для цілей, з якими персональні дані обробляються (обмеження зберігання). Судові спори щодо часу зберігання інформації трапляються відносно рідко. Хоч питання допустимого (необхідного) часу зберігання та використання персональних даних постає в судових рішеннях доволі часто. У справі № 761/8791/19 позивач ставив під сумнів не тільки факт надання ним згоди на обробку персональних даних (детальніше див. приклади щодо підстав для обробки персональних даних), але й питання про строковість використання інформації про нього в бюро кредитних історій. Попри загалом слушну правову оцінку основного питання спору, суди[94] окремого оцінювання тексту згоди на обробку персональних даних у процесі застосування Закону України «Про організацію формування та обігу кредитних історій» не робили.

Важливо звернути увагу на тлумачення судами часу дії згоди на обробку персональних даних. Судова практика свідчить про однозначне її поширення на нові правовідносини, тобто перспективне застосування після її надання. Разом з тим, щодо моменту відкликання і початку припинення дії згоди на обробку персональних даних у разі інформування суб'єктом персональних відповідного володільця (розпорядника), суди зазвичай займають позицію, що відкликання згоди можливе лише стосовно майбутньої обробки персональних даних, але не тих даних, які вже були оброблені; рішення та процеси, які були виконані під час обробки персональних даних, не можуть бути анульованими[95]. Щоправда, у таких ситуаціях суди, на жаль, часто користуються посиланням на лист Міністерства юстиції щодо відкликання згоди на обробку персональних даних[96], а не оперують положеннями Закону України «Про захист персональних даних» чи відповідними міжнародними стандартами.

94. Див. Рішення Шевченківського районного суду м. Києва у справі № 761/8791/19 від 07 серпня 2019 року: https://reyestr.court.gov.ua/Review/83817241; Постанову Київського апеляційного суду у справі № 761/8791/19 від 19 листопада 2019 року: https://reyestr.court.gov.ua/Review/85804485#; Постанову Верховного Суду у справі № 761/8791/19 від 11 листопада 2020 року: https://reyestr.court.gov.ua/Review/92934787.
95. Див., наприклад, Рішення Дубенського міськрайонного суду Рівненської області у справі № 559/362/20 від 31 травня 2021 року: https://reyestr.court.gov.ua/Review/97360691; Постанову Київського апеляційного суду у справі № 361/3511/20 від 15 липня 2021 року: https://reyestr.court.gov.ua/Review/98593168 та ін.
96. Лист Міністерства юстиції України № 5543-0-33-13/6.1 від 26.04.2013 року: https://zakon.rada.gov.ua/laws/show/v5543323-13#Text.

ТОЧНІСТЬ

Принцип точності персональних даних передбачає встановлення чітких критеріїв віднесення інформації до тієї, на яку поширюються гарантії законодавства про захист персональних даних. При цьому важливі вимоги до самих персональних даних, які мають бути точними, вірогідними (відповідати дійсності) та актуальними.

- Відповідність персональних даних – вимагає коректно відносити ту чи іншу інформацію до категорії «персональні дані», надаючи відповідні гарантії щодо збирання, обробки і використання такої інформації. Критерії розуміння поняття «персональні дані» повинні бути закріплені на рівні закону без можливості множинного, неоднозначного чи свавільного трактування їх змісту, інструментів використання чи меж обмеження.
- Точність та актуальність – персональні дані повинні бути якісними, тобто відповідати мінімальним критеріям їх релевантності меті збирання, обробки чи використання. Для цього персональні дані повинні підтримуватися постійно в актуальному стані, регулярно оновлюватися, піддаватися переглядові з розумною періодичністю. Це особливо важливо коли йдеться про функціонування державних (публічних) реєстрів, інформаційних систем, баз даних чи інших ресурсів масового збирання, обробки і використання персональних даних.

Водночас ці вимоги стосуються не тільки публічної влади, вони цілком чіткі й для приватних суб'єктів – володільців і розпорядників персональних даних.

Відповідність персональних даних

Досить часто для судів стає складністю відмежування персональних даних від інших видів інформації з іншими правовими режимами. Наприклад, відповідно до абзацу другого частини першої статті 5 Закону України «Про захист персональних даних» не належить до інформації з обмеженим доступом інформація про отримання в будь-якій формі фізичною особою бюджетних коштів, державного чи комунального майна, структуру, принципи формування та розмір оплати праці, винагороди, додаткового блага керівника, заступника керівника юридичної особи публічного права, керівника, заступника керівника, члена наглядової ради державного чи комунального підприємства або державної чи комунальної організації, що має на меті одержання прибутку, особи, яка постійно або тимчасово обіймає посаду члена виконавчого органу чи входить до складу наглядової ради господарського товариства, у статутному капіталі якого понад 50 відсотків акцій (часток, паїв) прямо чи опосередковано належать державі та/або територіальній громаді, крім випадків, передбачених статтею 6 Закону України «Про доступ до публічної інформації».

За таких обставин дуже практичне є питання чи може бути обмежений доступ до інформації про оплату праці працівників державних і комунальних підприємств; чи поширюються на таку інформацію гарантії щодо захисту персональних даних. Як приклад, тут можна навести справу № 645/545/17, де суди по-різному розтлумачили статус Харківського регіонального структурного підрозділу ДП «Украероруx», що врешті вплинуло на можливість застосування положень Закону України «Про захист персональних даних» та поширення відповідних гарантій на інформацію про умови оплати праці співробітників цієї структури.

У цій справі позивач в особі голови профкому ХППО ВП «Федерація профспілок авіапрацівників радіолокації, радіонавігації і зв'язку України» звертався до директора Харківського регіонального структурного підрозділу ДП «Украероруx» і просив надати інформацію, а саме копії наказів щодо виплати матеріальної допомоги працівникам. У ДП «Украероруx» вирішили, що зазначене питання буде розв'язуватися після проведення консультацій з працівниками стосовно надання згоди на поширення персональних даних з урахуванням Закону України «Про захист персональних даних». Врешті згоду на доступ до персональних даних, їх поширення та передання третім особам надали 15 осіб, не надали згоди 34 особи, 1 особа перебувала на лікарняному. Отже, відповідач надав запитувану інформацію щодо 15 осіб, які надали згоду на доступ до персональних даних, їх поширення та передання третім особам. Щодо решти працівників, 34 з яких згоду не надали, а один перебував на лікарняному, то в наданні відповідної інформації відмовлено[97].

Суд першої інстанції,[98] а згодом і Верховний Суд встановили, що Харківський регіональний структурний підрозділ ДП «Украероруx» – госпрозрахункове комерційне підприємство, яке самостійно веде господарську діяльність, отримує прибуток, за рахунок якого своїм працівникам виплачує заробітну плату, зокрема й матеріальну допомогу. Бюджетних коштів не отримує, лише майно підприємства – державна власність та закріплене за ним на праві господарського відання. Відповідно, застосування вимог Закону України «Про доступ до публічної інформації» у цій ситуації буде некоректне. Водночас апеляційний суд[99] висловив інше бачення щодо статусу регіонального структурного підрозділу ДП «Украероруx» (встановив його публічну природу) й обмежив поширення дії Закону України «Про захист персональних даних» на відповідні правовідносини.

Позиція Верховного Суду (як і суду першої інстанції) безпосередньо вплинула на зміст та обсяг поширення законодавства про захист персональних даних на інформацію про умови оплати праці співробітників Харківського регіонального структурного підрозділу ДП «Украероруx». Детального аналізу змісту персональних даних та віднесення інформації щодо виплати матеріальної допомоги працівникам суди детально не проводили. У рішенні Фрунзенського районного суду м. Харкова зазначено, що:

«Суд критично ставиться до висловлень позивача, стосовно можливості отримання інформації про фізичну особу без її згоди, так як працівники отримують матеріальну допомогу з бюджетних коштів, а така інформація є публічною і може надаватись без перешкод.

Суд погоджується з позицією відповідача стосовно неможливості поширення персональних даних відносно фізичних осіб – працівників Харківського РСП без надання згоди на таке розповсюдження…

… лише фізична особа, якої стосується конфіденційна інформація, відповідно до конституційного та законодавчого регулювання права особи на збирання, зберігання, використання та поширення конфіденційної інформації має право вільно, на власний розсуд визначати порядок ознайомлення з нею інших осіб, держави та органів місцевого самоврядування, а також право на збереження її у таємниці»[100].

Не менш важливе відмежування персональних даних від публічної інформації в сфері соціального захисту населення. Тут судова практика в різних сферах має деякі особливості. Суди зазвичай

97. Згідно з Постановою Верховного Суду у справі № 645/545/17 від 12 серпня 2020 року: https://reyestr.court.gov.ua/Review/91134733#.
98. Рішення Фрунзенського районного суду м. Харкова у справі № 645/545/17 від 29 вересня 2017 року: https://reyestr.court.gov.ua/Review/69339299.
99. Постанова Апеляційного суду Харківської області у справі № 645/545/17 від 12 квітня 2018 року: https://reyestr.court.gov.ua/Review/73528431.
100. Рішення Фрунзенського районного суду м. Харкова у справі № 645/545/17 від 29 вересня 2017 року: https://reyestr.court.gov.ua/Review/69339299.

коректно відмежовують персональні дані, використовуючи насамперед критерії оцінювання мети та підставі їх збору та обробки. Показовим тут може бути приклад справи щодо можливості обробки персональних даних органами соціального захисту населення при наданні соціальної допомоги особі, яка разом із заявою про отримання допомоги подала заяву про відмову від надання згоди на обробку персональних даних. В одній з таких ситуацій суд зазначив:

«… Наказом Міністерства соціальної політики України від 24.04.2014 № 245 (зареєстрований в Міністерстві юстиції України 14.05. 2014 за № 499/25276) внесено зміни до форми Заяви про призначення всіх видів соціальної допомоги, компенсацій, субсидій і пільг, затвердженої наказом Мінсоцполітики від 22.02.2012 № 96. Змінами передбачено виключення із заяви про призначення соцдопомоги вимоги, згідно з якою заявник і члени його сім'ї дають згоду на збір інформації і обробку персональних даних, відповідно до норм Закону України «Про захист персональних даних» зазначених ним у заяві і поданих разом із нею документами, а також збір необхідної для отримання соціальних виплат інформації про сім'ю, доходи, власність і майно. Виключення даної інформації пов'язано зі змінами в статтю 5 Закону України «Про захист персональних даних» (Закон України від 27 березня 2014 року № 1170-VII «Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Закону України «Про інформацію» та Закону України «Про доступ до публічної інформації»). Законом змінено визначення об'єкту захисту персональних даних. Раніше інформацією з обмеженим доступом вважалися всі персональні дані за винятком знеособлених. Згідно з новою редакцією закону інформація про отримання у будь-якій формі фізичною особою бюджетних коштів, державного чи комунального майна, не належить до інформації з обмеженим доступом. Порядок доступу третіх осіб до персональних даних, які знаходяться у володінні розпорядника публічної інформації, визначається Законом України «Про доступ до публічної інформації».

Тобто, для призначення державної соціальної допомоги малозабезпеченій сім'ї не потрібна згода заявника на збір та обробку персональних даних.

Подана заявником ОСОБА_2 17.07.2017 заява про відмову дати згоду на збір та обробку персональних даних взагалі не передбачена законом і не може бути взята до уваги при вирішенні питання про призначення допомоги у установленому законом порядку»[101].

Дещо інший аспект «абсолютизації» згоди на обробку персональних даних можна побачити і у справах щодо оскарження неможливості невикористання персональних даних при зверненні до суду. Наприклад, у справі № 199/405/20 позивач намагався довести, на його думку, порушення його прав через неможливість звернення до суду з позовом (апеляційною скаргою) без зазначення відомостей (реєстраційного номера облікової картки платника податків або номера та серії паспорта), що вимагаються процесуальним законодавством. Як суди апеляційної[102], так і суд касаційної інстанції тут не погодилися з доводами позивачів. Зокрема, Верховний Суд зазначив:

«Доводи заявника про те, що апеляційний суд не мав права вимагати в нього подання нової апеляційної скарги з підстав незазначення ним реєстраційного номера облікової картки платника податків або номера та серії паспорта, не заслуговують на увагу, оскільки незазначення такої інформації є невиконанням вимог закону щодо змісту апеляційної скарги та має наслідком залишення її без руху. Встановивши невідповідність апеляційної скарги вимогам частини другої статті 392 ЦПК України, апеляційний суд обґрунтовано вказав на недоліки скарги та залишив її без руху, надавши заявнику можливість усунути такі недоліки.

101. Рішення Луцького міськрайонного суду Волинської області у справі № 161/18512/17 від 07 лютого 2018 року: https://reyestr.court.gov.ua/Review/72248664.
102. Див., наприклад, Ухвалу Дніпровського апеляційного суду у справі № 199/405/20 від 10 лютого 2020 року: https://reyestr.court.gov.ua/Review/87479958; Ухвалу Дніпровського апеляційного суду у справі № 200/11630/19 від 05 вересня 2019 року: https://reyestr.court.gov.ua/Review/84089581.

Що стосується посилання заявника на порушення його конституційного права на захист персональних даних, то воно також є безпідставним з огляду на таке.

Відповідно до частин першої, другої статті 55 Конституції України права і свободи людини і громадянина захищаються судом. Кожному гарантується право на оскарження в суді рішень, дій чи бездіяльності органів державної влади, органів місцевого самоврядування, посадових і службових осіб.

Конституційний Суд України в рішенні від 14 грудня 2011 року № 19-рп/2011 роз'яснив, що положення частини другої статті 55 Конституції України необхідно розуміти так, що конституційне право на оскарження в суді будь-яких рішень, дій чи бездіяльності всіх органів державної влади, органів місцевого самоврядування, посадових і службових осіб гарантовано кожному. Реалізація цього права забезпечується у відповідному виді судочинства і в порядку, визначеному процесуальним законом.

Таким чином, саме процесуальним законодавством встановлюються порядок та строки на апеляційне оскарження судових рішень, що не суперечить положенням Конституції України»[103].

Таку ж позицію Верховний Суд зайняв в аналогічній справі[104]. Суд, не вдаючись до детальної аргументації, ухвалив загалом коректне рішення, що досить чітко відмежовує спосіб застосування законодавства про захист персональних у публічних правовідносинах щодо захисту права самого ж заявника. Разом з тим аргументація судів в частині з'ясування природи персональних даних та особливостей їх використання (зазначення) при зверненні до суду могла б бути ширшою.

Досить часто поняття «персональні дані» сприймають доволі широко, поширюючи його зміст й на правовідносини, які не підпадають під відповідні гарантії та обмеження. Загалом судам вдається доволі чітко проводити розмежування. Як приклад, у справі № 554/8424/18 суд досить чітко аргументував, що оголошення, в якому міститься інформація про розмір заборгованості за певною адресою (номер квартири) не персональні дані, відповідно, право на заборону поширення такої інформації не виникає. Як наслідок, підстав для відшкодування завданих збитків внаслідок розміщення оголошень про нараховану заборгованість (що, на думку позивачки, призвело до негативного впливу та тиску на неї з боку сусідів, через що їй була завдана моральна шкода) немає[105].

Інший вартий уваги приклад – застосування судами законодавства про захист персональних даних у кримінальних провадженнях щодо віднесення до персональних даних інформації про IP-адресу споживачів телекомунікаційних послуг в інтернеті. У справі № 644/4698/18, оцінюючи таку ситуацію, суд зазначив:

«Правові відносини, пов'язані із захистом і обробкою персональних даних, регулюються Законом України «Про захист персональних даних». Відповідно до статті 2 Закону персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Ключовим у вищенаведеному визначенні є поняття «ідентифікована особа». Ідентифікованою особа вважається, якщо її можна безпомилково виділити серед інших. Вирішення питання щодо того, чи належить та чи інша інформація до персональних даних повністю залежить від того, чи можна цю особу фактично ідентифікувати. Тобто, за загальним правилом, віднесення IP-адреси абонента до персональних даних залежить від форми правовідносин

103. Постанова Верховного Суду у справі № 200/11630/19 від 11 листопада 2020 року: https://reyestr.court.gov.ua/Review/92934719.
104. Постанова Верховного Суду у справі № 199/405/20 від 26 січня 2021 року: https://reyestr.court.gov.ua/Review/94591622.
105. Рішення Октябрського районного суду м. Полтави у справі № 554/8424/18 від 30 вересня 2019 року: https://reyestr.court.gov.ua/Review/84762057.

між абонентом та телекомунікаційним оператором (на умовах письмового договору або за передоплатою). Тобто, при укладенні з абонентом договору, IP-адреса абонента вважатиметься його персональними даними, адже даватимуть телекомунікаційному оператору змогу ідентифікувати такого абонента. Водночас IP-адреса особи, яка не є ідентифікованою (користується телекомунікаційними послугами без укладення письмового договору або добровільної особистої реєстрації на веб-сайті телекомунікаційного оператора), за загальним правилом, не належатиме до персональних даних»[106].

Такий підхід суду, зокрема, став основою для ухвалення виправдовувального вироку в цій справі, який залишено в силі і за результатами апеляційного оскарження[107].

Щодо дискусії про можливість поширення дії Закону України «Про захист персональних даних» на інформацію про юридичних осіб, яка за своєю природою може бути схожою на аналогічну щодо фізичних осіб, суд у справі № 826/6727/14 досить чітко встановив, що персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Зокрема, суд зазначив:

«Як зазначено вище, згідно ст. 2 Закону України «Про захист персональних даних» до персональних даних відносяться відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

На відомості про юридичних осіб та фізичних осіб-підприємців вимоги вказаного Закону не розповсюджуються, тому посилання відповідача на обмеження, запроваджені вказаним Законом, є необґрунтованим, оскільки в даному випадку запит позивача стосується інформації про виробника та продавця антивірусного забезпечення, що не стосується отримання персональних даних про фізичну особу, а стосується отримання інформації про суб'єкта підприємницької діяльності»[108].

Щоправда, у цій справі йдеться не тільки про хибне тлумачення приписів закону відповідачем, скільки, найпевніше, про намагання уникнути обов'язку надавати інформацію у відповідь на інформаційний запит, поданий відповідно до Закону України «Про доступ до публічної інформації».

Інший вартий уваги приклад – обмежене застосування законодавства про доступ до публічної інформації і використання законодавства про захист персональних даних із метою не розкриття певної інформації. Як приклад, справа № 821/4009/14, де позивач (фізична особа) оскаржує відмову органу державної влади в наданні інформації щодо результатів перевірки, проведеної на основі її скарги щодо незаконної самочинної забудови. Суд першої[109] та апеляційної інстанції досить чітко відмежували тут публічний інтерес від персональних даних і відповідні правові режими інформації. Суд апеляційної інстанції зазначив:

«З матеріалів справи вбачається, що позивач звернулась до відповідача з чітким поясненням мети щодо необхідності отримання зазначеної інформації, адже вона необхідна їй для захисту своїх цивільних прав, які, як встановлено самим відповідачем, були порушені. Так у відповіді на звернення ОСОБА_1 інспекція ДАБК у листі від 30.04.2014р. № 7/21-07-01-08/105-24 повідомила про

106. Вирок Орджонікідзевського районного суду м. Харкова у справі № 644/4698/18 від 01 березня 2021 року: https://reyestr.court.gov.ua/Review/95216818.
107. Ухвала Харківського апеляційного суду у справі №: 644/4698/18 від 18 травня 2021 року: https://reyestr.court.gov.ua/Review/97558943.
108. Постанова Окружного адміністративного суду міста Києва у справі № 826/6727/14 від 14 липня 2014 року: https://reyestr.court.gov.ua/Review/39914804.
109. Постанова Херсонського окружного адміністративного суду у справі № 821/4009/14 від 16 жовтня 2014 року: https://reyestr.court.gov.ua/Review/40988280.

встановлення в ході позапланової перевірки самовільного встановлення ОСОБА_2 туалету, вигрібної ями, каналізації та помпи, що стало підставою для складання відповідного акту, протоколу та припису про усунення порушень вимог законодавства у сфері містобудівної діяльності, будівельних норм, державних стандартів і правил (а.с.17).

Судова колегія погоджується з доводами суду першої інстанції, що запитувана інформація не може відноситися до конфіденційної, оскільки утворилась в ході розгляду заяви ОСОБА_1 від 08.04.2014р.

…

Акт перевірки, протокол про адміністративне правопорушення, припис про усунення порушень вимог законодавства у сфері містобудівної діяльності, будівельних норм, державних стандартів і правил складені відповідачем, як територіальним органом виконавчої влади на підставі наданих повноважень, встановлених Законом України «Про регулювання містобудівної діяльності» …

Аналіз наведених правових норм дає підстав для висновку, що не є конфіденційною або з обмеженим доступом інформація, яка створена, зокрема органами виконавчої влади, на виконання наданих повноважень зі здійснення владних управлінських функцій відповідно до законодавства.

До того ж судова колегія враховує, що відповідно до ст.18 Закону України «Про звернення громадян» громадянин, який звернувся зі скаргою чи заявою до органів державної влади, має право знайомитися з матеріалами перевірки.

Відтак, позивач, яка звернулась до інспекції ДАБК із заявою від 08.04.2014р. для вжиття заходів щодо припинення самочинного будівництва з боку її суміжного сусіда ОСОБА_2 (а.с.16), має право на ознайомлення з матеріалами перевірки, що передбачає отримання копії документів перевірки.

Враховуючи вищенаведене в сукупності, судова колегія приходить до висновку, що запитувана інформація є публічною, а тому має бути надана відповідачем, як належним розпорядником інформації, на запит позивача»[110].

Точність та актуальність

Розуміння змісту та обсягу поняття «персональні дані» доволі часто опирається на різні підходи та теоретико-правові напрацювання. Суди зазвичай доволі чітко відносять до персональних даних особисті фотографії особи.

«Таким чином, Європейським судом [авт. - ЄСПЛ] було підкреслено, що особисті фотографії особи складають її персональні дані та такі фотографії підпадають під сферу дії ст. 8 Конвенції. При цьому, особа має як виключне право на власні зображення, так і право контролювати використання таких зображень.

Опублікування фотографій із зображенням позивача та його дружини, поширення даних про сімейний стан, висвітлення особистих стосунків є явно надмірним і непропорційним втручанням у приватність. Таким чином, в поширених публікаціях та фото відповідачем протиправно поширювалась інформація про приватне життя позивача, його дружини та їх персональні дані»[111].

---

110. Постанова Одеського апеляційного адміністративного суду у справі № 821/4009/14 від 22 січня 2015 року: https://reyestr.court.gov.ua/Review/42495118.
111. Див., наприклад, Рішення Дарницького районного суду м. Києва у справі № 753/15830/18 від 28 травня 2020 року: https://reyestr.court.gov.ua/Review/89694900.

При цьому аргументація судів зазвичай опирається на практику Європейського суду з прав людини та міжнародні стандарти щодо розуміння змісту, сутності та соціального значення персональних даних. Відповідна аргументація також має у своїй основі аналіз прийнятних меж втручання в особисте та приватне життя особи.

Ще один аспект точності розуміння поняття персональних даних – сприйняття їх змісту та форми вираження. У справі № 643/9186/16-ц як суд першої інстанції, так і суд апеляційної інстанції зайняли позицію, що відеоматеріали, які містять зображення фізичної особи (відеозапис весілля) не містять персональних даних, відповідно, на них не можуть поширюватися гарантії, передбачені Законом України «Про захист персональних даних». У Рішенні Московського районного суду м. Харкова в цій справі зазначено:

«Матеріали справи доказів поширення відповідачем будь-якої інформації про позивача взагалі не містять, у спірному відео прізвища позивачів або інші персональні дані (ст. 2 Закону України «Про захист персональних даних», відповідно до якого персональними даними є відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована) не називаються»[112].

Суд апеляційної інстанції погодився з такою позицією, ба більше, свою аргументацію судді базували, зокрема, посилаючись на практику Європейського суду з прав людини:

«Європейський суд з прав людини зауважує, термін «приватне життя» є широким поняттям, що не має вичерпного визначення, і поширюється на безліч аспектів самоідентифікації людини, наприклад, на ім'я особи та зображення, і включає в себе її фізичну та психологічну цілісність. Репутація і честь людини є частиною її самоідентифікації і психологічної цілісності, а тому також охоплюються поняттям приватне життя (BOGOMOLOVA v. RUSSIA, № 13812/09, § 51, ЄСПЛ, 20 червня 2017 року).

Відносно фотографій Європейський Суд вказав, що зображення особи є одним із головних атрибутів її особистості, оскільки воно розкриває унікальні характеристики особи і відрізняє особу з-поміж інших. Право на захист свого зображення є, таким чином, однією з головних складових особистого розвитку. Воно передбачає, головним чином, право особи контролювати використання цього зображення, в тому числі і не дозволяти його опублікувати. Хоча головною метою статті 8 є захист особи від неправомірного втручання з боку державної влади, вона не лише зобов'язує державу утримуватись від такого втручання: окрім такого негативного заходу, можуть існувати позитивні зобов'язання, невід'ємні від ефективної поваги до приватного або сімейного життя особи. Ці зобов'язання можуть передбачати здійснення заходів, спрямованих на забезпечення поваги до приватного життя навіть у сфері відносин осіб між собою. Це стосується також захисту зображення особи від зловживання з боку інших осіб (VON HANNOVER v. GERMANY (No. 2), № 40660/08, 60641/08, § 96, 98, ЄСПЛ, 07 лютого 2012 року)»[113].

Отже, з використанням, зокрема, міжнародних стандартів суди аргументували, що «відео не містить прізвища позивачів або інші персональні дані». Такий підхід щонайменше дискусійний. При цьому, розглядаючи цю ж справу, Верховний Суд також не звернув уваги на цей момент (розуміння поняття «персональні данні») й зосередився тільки на процесуальних порушеннях, допущених судом апеляційної інстанції[114].

112. Рішення Московського районного суду м. Харкова у справі № 643/9186/16-ц від 13 грудня 2016 року: https://reyestr.court.gov.ua/Review/63509682#.
113. Постанова Харківського апеляційного суду у справі № 643/9186/16-ц від 12 листопада 2019року: https://reyestr.court.gov.ua/Review/85641740.
114. Постанова Верховного Суду у справі № 643/9186/16-ц від 03 липня 2019 року: https://reyestr.court.gov.ua/Review/83056326.

Щодо забезпечення актуальності, то питання оновлення персональних даних, зібраних та використовуваних органами державної влади, надзвичайно актуальне з огляду не тільки на необхідність виконання державою функцій з урахуванням дійсної (актуальної) інформації. Це вкрай важливо і щодо реалізації конкретних прав людини. Адже досить часто інформація з публічних (державних) реєстрів стає основою для реалізації інших прав та свобод. Показовим прикладом тут може бути справа № 818/2013/18, де позивач (фізична особа) оскаржував зміст виданої йому довідки про те, що в нього нема судимості. Таку довідку йому надали з одночасним внесенням до неї додаткових відомостей про вчинення кримінально-процесуальних дій щодо нього в минулому, але фактично не завершених досі (на території Автономної Республіки Крим, до її окупації). При цьому такі кримінально-процесуальні заходи не зумовлювали на теперішній час наявності судимості в цієї особи.

Очевидно в інтересах позивача було б видання інформації тільки із зазначенням відомостей, що в нього нема судимості, а от інша інформація може негативно вплинути на його репутацію та призведе до неправомірного поширення персональних даних і непропорційного втручання в його життя. Це і було предметом судового оскарження. Додатково позивач просив зобов'язати відповідача (Департамент інформатизації Міністерства внутрішніх справ України) вилучити з єдиної інформаційної системи Міністерства внутрішніх справ України всі відповідні відомості про нього.

У цій справі суди першої[115] та апеляційної[116] інстанцій досить чітко зайняли позицію, що внесення такої інформації до довідки вимагається умовами функціонування єдиної інформаційної системи Міністерства внутрішніх справ України й не може бути змінене. Верховний же Суд не погодився з таким тлумаченням та зазначив:

«50. Разом з цим, колегія суддів зауважує, що з урахуванням вимог пункту 9.9 Інструкції №823/188 та положень частини 1 статті 88 Кримінального кодексу України, відповідно до якої особа визнається такою, що має судимість, з дня набрання законної сили обвинувальним вироком і до погашення або зняття судимості, довідка про судимість (несудимість) повинна мати інформацію про відсутність або наявність у особи судимості згідно з обвинувальним вироком суду, який набрав законної сили (з урахуванням зазначених вище статей Кримінального кодексу України: стаття 5 – зворотна дія закону про кримінальну відповідальність у часі; стаття 89 – строки погашення судимості; стаття 108 – погашення та зняття судимості).

51. Отже, висновок судів попередніх інстанцій про те, що надання фізичній особі відомостей про неї не обмежується лише інформацією про відсутність (наявність) судимості, але й передбачає надання іншої інформації, що обробляється в оперативно-довідкових картотеках, не узгоджується з нормами діючого законодавства щодо змісту та обсягу даних довідки про судимість (несудимість) з огляду на заборону поширення конфіденційної інформації про особу без її згоди»[117].

Аналогічну позицію відображено і в інших рішеннях Верховного Суду[118]. Разом з тим він підтримав суди першої та апеляційної інстанції та відмовив у задоволенні вимог про вилучення з єдиної інформаційної системи Міністерства внутрішніх справ України відомостей про вжиті раніше заходи кримінально-процесуального характеру, зокрема, зазначивши:

---

115. Рішення Сумського окружного адміністративного суду у справі № 818/2013/18 від 01 серпня 2018 року: https://reyestr.court.gov.ua/Review/75727687.
116. Постанова Харківського апеляційного адміністративного суду у справі № 818/2013/18 від 04 грудня 2018 року: https://reyestr.court.gov.ua/Review/78425208.
117. Постанова Верховного Суду у справі № 818/2013/18 від 31 березня 2020 року: https://reyestr.court.gov.ua/Review/88507225.
118. Див., наприклад, Постанову Верховного Суду у справі №826/18484/16 від 18 грудня 2019 року: https://reyestr.court.gov.ua/Review/86459701; Постанову Верховного Суду у справі № 802/1587/18-а від 24 лютого 2020 року: https://reyestr.court.gov.ua/Review/87808548.

«64. Тобто, вилучення з оперативно-довідкових картотек Департаментом інформатизації при МВС та територіальних УОІ-ВОІ облікових документів осіб, окрім іншого, може мати місце у випадку їх переоформлення на підставі постанов органів слідства (дізнання) або ухвал судів про уточнення (зміну) анкетних даних осіб, що стоять на обліку, а також, якщо кримінальні справи стосовно осіб припинені на стадії досудового слідства на підставі реабілітації або відносно яких судом прийнято виправдувальний вирок.

65. Колегія суддів погоджується з висновком судів попередніх інстанцій, що оскільки матеріали справи не містять відповідних офіційних документів, які б доводили, що інформація, стосовно ОСОБА_1 в персонально-довідковому обліку, є неповною та неточною, відсутня також інформація, яка б слугувала підставою для внесення відповідних змін до персонально-довідкового обліку відносно позивача та у зв'язку з ненаданням позивачем відповідних доказів, які свідчили про необхідність вилучення з єдиної інформаційної системи Міністерства внутрішніх справ України інформації, яка, на його думку, є неправдивою, відсутні правові підстави для визнання протиправними дій відповідача щодо відмови у внесенні змін в персонально-довідковий облік щодо ОСОБА_1 до єдиної інформаційної системи Міністерства внутрішніх справ України та зобов'язання відповідача виключити з єдиної інформаційної системи Міністерства внутрішніх справ України відомості про вирок Залізничного районного суду м.Сімферополь АР Кримі, який скасовано ухвалою Апеляційного суду Автономної Республіки Крим та, відповідно, відсутність підстав для видачі позивачу нової довідки»[119].

Ці приклади дуже чітко ілюструють те, як рівень якості адміністрування інформації про особу в державних реєстрах (інформаційних системах, базах даних тощо) може безпосередньо впливати на реалізацію прав і свобод. При цьому позиція судів у кожному конкретному випадку може істотно відрізнятися в оціненні способу застосування тут законодавства про захист персональних даних.

119. Постанова Верховного Суду у справі № 818/2013/18 від 31 березня 2020 року: https://reyestr.court.gov.ua/Review/88507225.

ПІДЗВІТНІСТЬ

Із правового погляду принцип підзвітності в діяльності органів публічного адміністрування базується на конституційних положеннях статті 3 Конституції України, відповідно до якої людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю. Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини – головний обов'язок держави.

В сфері захисту персональних даних принцип підзвітності означає, що володілець персональних даних несе відповідальність за дотримання принципів захисту персональних даних та має бути здатним підтвердити факт їхнього дотримання. Отже, принцип підзвітності спрямований насамперед на забезпечення відповідального поводження з персональними даними в органах державної влади, органах місцевого самоврядування та інших суб'єктах, що можуть здійснювати публічну владу. Щодо приватних суб'єктів важливе створення державою належного нормативного регулювання, яке забезпечить не тільки ретельну обробку персональних даних, але й можливість ефективного державного та суспільного контролю за відповідними адміністративними (управлінськими) процедурами. Відповідно, тут можна виділити два основні складники:

- ретельність обробки персональних даних – полягає в належному законодавчому регулюванні адміністративних процедур, що унеможливить надмірну дискрецію (свободу розсуду) суб'єктів владних повноважень; відповідальне та усвідомлене збирання, обробку і використання персональних даних в інтересах їх збереження та недопущення надмірного втручання в реалізацію відповідних прав людини;
- прозорість – слід сприймати як необхідність забезпечити суспільству і кожній особі за допомогою певних засобів бачити діяльність органу публічної влади в частині обробки персональних даних наскрізь, тобто розуміючи всі внутрішні процеси, що впливають на спосіб, вид та строки ухвалення в кожній конкретній справі. Персональні дані повинні оброблятися «прозоро», що включає надання суб'єктам даних адекватної інформації про те, як обробляються їх дані.

Ретельність обробки

Робота органів публічної влади з персональними даними – питання окремого змістовного аналізу. Тут вкрай важливе не тільки забезпечення законності (дія на підставі, в межах та способом, визначеним законом), але й з дотримання належної адміністративної процедури. Передавання персональних даних від одного органу (структурного підрозділу, підпорядкованого підприємства тощо) до іншого може і повинно відбуватися з чітким дотриманням меж повноважень цих владних суб'єктів, а також з урахуванням законодавства про захист персональних даних. Передавання персональних даних від одного суб'єкта до іншого може вестися тільки за умови чітко визначеної мети та законної підстави таких дій. Інакше необхідно формувати нову базу даних (реєстр, інформаційну систему тощо) з обов'язковим одержанням згоди суб'єктів персональних даних.

Саме таку позицію зайняли суди у справі № 806/8576/13-а, де оскаржувалося рішення Виконавчого комітету Житомирської міської ради «Про створення бази персональних даних споживачів житлово-комунальних послуг», яким зобов'язано комунальні виробничі житлові

ремонтно-експлуатаційні підприємства, дочірні підприємства, комунальні підприємства видати бази персональних даних споживачів житлово-комунальних послуг на сервер комунального підприємства «Міський інформаційний центр» Житомирської міської ради та щотижня проводити їх оновлення. Зокрема, суд касаційної інстанції зазначив:

«… у разі зміни визначеної мети обробки персональних даних суб'єктом персональних даних має бути надана згода на обробку його даних відповідно до зміненої мети. Не допускається обробка даних про фізичну особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Згода суб'єкта персональних даних – будь-яке документоване, зокрема письмове, добровільне волевиявлення фізичної особи щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки (ч. 5 ст. 2 Закону України «Про захист персональних даних» №2297-VI).

Приймаючи оскаржуване рішення, Виконавчий комітет Житомирської міської ради фактично зобов'язував володільців персональних даних (КВЖРЕПи та інші юридичні особи) поширити наявні в них персональні дані шляхом їх передачі до КП «Міський інформаційний центр» Житомирської міської ради без згоди суб'єктів персональних даних, що суперечить вимогам ст. 14 Закону №2297-VI, якою визначено, що поширення персональних даних передбачає дії щодо передачі відомостей про фізичну особу з баз персональних даних за згодою суб'єкта персональних даних.

Як встановлено судами попередніх інстанцій, від суб'єктів персональних даних не отримана згода на обробку і використання їх персональних даних Комунальним підприємством «Міський інформаційний центр» Житомирської міської ради.

Враховуючи те, що у Комунального підприємства «Міський інформаційний центр» Житомирської міської ради відсутня згода від суб'єктів персональних даних на обробку і використання їх персональних даних та те, що рішення Виконавчого комітету Житомирської міської ради від 17.05.2012р. № 186 «Про створення бази персональних даних споживачів житлово-комунальних послуг» прийнято з метою сприяння в діяльності комунальних підприємств щодо забезпечення виконання мешканцями міста вимог з оплати наданих житлово-комунальних послуг, ефективної координації служб життєдіяльності міста на випадок виникнення надзвичайних ситуацій та ефективного використання інформаційних ресурсів підприємств, що надають житлово-комунальні послуги, тобто не стосується випадків, коли законодавчо дозволяється використання конфіденційної інформації, суди попередніх інстанцій дійшли обґрунтованого висновку про протиправність вказаного рішення»[120].

З огляду на таку аргументацію, вкрай важливе є забезпечення не тільки законного первинного збирання та обробки персональних даних, але й регулярне та ефективне стеження за дотриманням первинної мети обробки таких персональних даних у всіх можливих наступних правовідносинах чи адміністративних процедурах.

Належне здійснення повноважень посадовими особами інколи унеможливлює вчинення певних юридично значущих дій без впливу (можлива завдання шкоди) на збереження персональних даних. У вже проаналізованій вище справі № 950/3050/19 звернення спадкоємця до нотаріуса з вимогою надати дозвіл на ознайомлення та фотографування матеріалів спадкової справи після смерті його матері, на думку Верховного Суду, не можна було задовольнити без розкриття персональних даних третіх осіб. Суд зазначив:

120. Ухвала Вищого адміністративного суду України у справі № 806/8576/13-а від 09 жовтня 2014 року: https://reyestr.court.gov.ua/Review/41129767.

«Висновок суду апеляційної інстанції про можливість приватного нотаріуса вжити заходів для захисту персональних даних інших осіб, які не є учасниками нотаріальної дії, а також для захисту інформації, отриманої при оформленні спадкової справи, що не стосується прав заявника є помилковим, оскільки суд не урахував, що спадкова справа відповідно до положень пункту 11.2 Інструкції формується шляхом групування оригіналів документів, а у випадках, передбачених законодавством копій документів, оформлених та засвідчених в установленому законом порядку, на підставі яких було відкрито спадкову справу та видано свідоцтво про право на спадщину. Надання справи для ознайомлення означає надання всіх згрупованих оригіналів документів, які були отримані приватним нотаріусом при вчиненні нотаріальної дії, у тому числі оригіналів документів, які містять відомості, що не стосуються заявника та становлять нотаріальну таємницю»[121].

Ретельність обробки персональних даних особливо важлива, коли йдеться про чутливу інформацію, некоректне та/або незаконне поширення якої може завдати суттєвої шкоди правам та законним інтересам людини. Наприклад, поводитися з інформацією про стан здоров'я та іншими медичними даними щодо особи слід вкрай обережно. На жаль, не в усіх випадках суди достатньо ретельно вивчають обставини таких справ і визначають не тільки факт порушення, але й звертають увагу на процедурні (управлінські) моменти збирання, обробки і використання персональних даних. У справі № 760/8719/17 суди першої та апеляційної інстанції не звернули уваги не тільки на порушення процедур обробки персональних даних, але й не надали належної правової оцінки фактові порушення прав людини в частині незаконного поширення невірогідної інформації про психічний стан особи.

У цій справі йшлося про вимогу позивача (фізичної особи) зобов'язати відповідача (Київський міський психоневрологічний диспансер № 5) спростувати поширену інформацію про те, що «… позивач перебувала на обліку у лікаря-психіатра в період з 1972 року по 2003 рік з діагнозом про психічні розлади; зобов'язати відповідача вилучити довідки із недостовірною інформацією про її перебування на лікуванні в Диспансері № 5 з 1972 року по 2003 рік з поліції Солом'янського району, з Київської міської державної адміністрації, Київської місцевої прокуратури № 9 та з інших підприємств, установ, організацій, куди була розповсюджена інформація із супровідними листами про визнання цих довідок недійсними; зобов'язати відповідача припинити розповсюджувати незаконні довідки із недостовірною інформацією про перебування її на лікуванні у Диспансері №5 з 1972 року по 2003 рік»[122].

Суди першої[123] та апеляційної[124] інстанцій сконцентрувалися на встановленні вірогідності перебування позивачки на обліку в психоневрологічному диспансері (як встановив Верховний Суд, і з цим питанням не до кінця справедливо розібравшись), проте зовсім проігнорували незаконне поширення персональних даних.

Верховний Суд у цій справі досить чітко встановив не тільки факт порушення прав людини, але й акцентував на недоліках обліку інформації щодо позивачки в Київському міському психоневрологічному диспансері № 5 та недоліках відповідного законодавчого регулювання. Зокрема, Верховний Суд зазначив:

---

121. Постанова Верховного Суду у справі № 950/3050/19 від 03 березня 2021 року: https://reyestr.court.gov.ua/Review/96071002.
122. З тексту Постанови Верховного Суду у справі № 760/8719/17 від 04 грудня 2019 року: https://reyestr.court.gov.ua/Review/86162369.
123. Рішення Солом'янського районного суду м. Києва у справі № 760/8719/17 від 25 жовтня 2018 року: https://reyestr.court.gov.ua/Review/77740521.
124. Постанова Київського апеляційного суду у справі № 760/8719/17 від 08 квітня 2019 року: https://reyestr.court.gov.ua/Review/81135984.

«54. Встановлені фактичні обставини справи не свідчать про те, що збирання та використання даних щодо стану психічного здоров'я позивача у такій формі та в контексті, в якому вони були використані було правомірним, мета їх обробки не була виправданою, враховуючи, що ці дані стосувались подій 1972-2003 років, інформація, надана інспектору Солом'янського Управління Головного управління Національної поліції у м. Києві, віднесена до лікарської таємниці.

55. Крім того, наявність листа з вибаченнями Диспансера № 5 щодо ненавмисного втручання в життя позивача (т. 2 а. с. 112 зворот) дає підстави для висновку, що відповідно до пункту 2 статті 8 Конвенції втручання в приватне життя позивача є необґрунтованим»[125].

Вище вже наведено приклад, коли суб'єкт владних повноважень у ході проведення службового розслідування незаконно збирав, зберігав, використовував та поширював конфіденційну інформацію – персональні дані про особу, зокрема стосовно його освіти без її згоди. Не аналізуючи причини та обставини саме такої ситуації у відповідному органі державної влади, тут тільки слід зазначити, що це доволі яскравий приклад надмірного і непропорційного використання владних повноважень не з метою, з якою вони надавалися. У цій справі Верховний Суд, як наслідок, зазначив:

«58. При цьому, під час проведення вказаного службового розслідування була використана інформація, отримана і застосована без належних на це підстав.

59. … наявність з боку відповідача протиправних дій щодо незаконного збирання, зберігання, використання та поширення конфіденційної інформації – персональних даних про особу ОСОБА_1 , зокрема відносно його освіти без його згоди, що можна розцінити, як втручання в особисте життя при проведенні службового розслідування стосовно ОСОБА_3, …»[126].

Як наслідок, можна зробити висновок, що в цій справі, управлінські (адміністративні) процедури у відповідному органі державної влади не були організовані належним чином, щоб не допустити (унеможливити) порушення щодо персональних даних особи.

Прозорість

Виконання управлінських (адміністративних) і технічних процедур щодо обробки персональних даних має бути достатньо чітким та зрозумілим не тільки для суб'єктів, які безпосередньо залучені до таких правовідносин (процесів), але й для ефективного державного і суспільного контролю. Щодо держави, то тут має діяти система інструментів та спеціально уповноважений орган державної влади[127]. Щодо ведення суспільного контролю за обробкою персональних даних, то цей аспект стосується насамперед функціонування органів державної влади та органів місцевого самоврядування. Адже вкрай важливе формування не тільки змістовного контролю за діяльністю публічної влади від імені держави, але й формування належного рівня суспільної довіри до процедур збирання, обробки та використання персональних даних в державних реєстрах, інформаційних системах, базах даних тощо. Водночас такий суспільний контроль має вестися з розумними обмеженнями та створенням відповідного безпечного середовища для самих персональних даних та гарантування забезпечення мети їх збирання та обробки.

---

125. Постанова Верховного Суду у справі № 760/8719/17 від 04 грудня 2019 року: https://reyestr.court.gov.ua/Review/86162369.
126. Постанова Верховного Суду у справі 520/5575/19 від 21 жовтня 2021 року: https://reyestr.court.gov.ua/Review/100471074.
127. Див. Правовий аналіз основних моделей інституалізації державного контролю у сфері персональних даних та доступу до публічної інформації в Україні: https://rm.coe.int/legal-analysis-data-ua/16809ee077.

Як приклад ведення суспільного контролю в цій сфері можна назвати передбачений приписами Закону України «Про Державний реєстр виборців» контроль за функціонуванням відповідного реєстру. Статтею 24 зазначеного закону передбачено, що політична партія, що має свою фракцію у поточному скликанні Верховної Ради України, політична партія, що входить до складу виборчого блоку, який має свою фракцію в поточному скликанні Верховної Ради України, має право брати участь у здійсненні публічного контролю за веденням Реєстру в межах, установлених цією статтею. Під час виборчого процесу виборів Президента України, народних депутатів України, чергових місцевих виборів, процесу всеукраїнського референдуму за письмовим зверненням політичної партії розпорядник Реєстру забезпечує представникові цієї партії, уповноваженому відповідним керівним органом партії, доступ у режимі читання до відомостей Реєстру, передбачених пунктами 1–4 частини першої статті 6 та частиною першою статті 7 цього закону, в установленому розпорядником Реєстру порядку.

Порядок такого контролю та ефективність його механізму були предметом оскарження у справі № 855/17/19. Один із кандидатів на пост Президента України оскаржував дії Центральної виборчої комісії та Служби розпорядника Державного реєстру виборців щодо ненадання йому можливості скористатися своїм правом на отримання електронної копії бази даних Державного реєстру виборців та, відповідно, обмеження його тільки до технічної можливості виключно особисто знайомитися з відомостями Державного реєстру виборців тільки в приміщенні та з використанням спеціального обладнання Служби розпорядника Державного реєстру виборців.

Суд першої інстанції[128], а згодом і суд апеляційної інстанції[129] (в цій категорії справ це остаточне рішення) зробив висновок, що обмеження, визначені Законом України «Про Державний реєстр виборців», а також їх деталізація в підзаконних актах Центральної виборчої комісії достатні та обґрунтовані. Верховний Суд зазначив:

«Аналіз наведених вище норм права дає підстави для висновку, що обов'язок Центральної виборчої комісії щодо надання на вимогу кандидата у Президенти України електронної копії бази даних Реєстру виборців кореспондує інший обов'язок – забезпечення належного захисту цієї бази даних, яка містить персональні дані виборців, що, в свою чергу, відносяться до конфіденційної інформації та захищаються Законом України «Про захист персональних даних»…

… необхідність прийняття додаткових мір щодо захисту відомостей, які містяться у Державному реєстрі виборців, обумовлена стрімким розвитком ІТ-технологій та зростанням ризиків кібератак та несанкціонованого втручання у бази даних, які містять конфіденційну інформацію про персональні дані осіб, зокрема, виборців, за останні декілька років у світі та в Україні»[130].

З такою позицією судів у конкретній справі можна погодитися. Разом з тим інструменти забезпечення контролю за збиранням і обробкою персональних даних, зокрема і в Державному реєстрі виборців потребують системного перегляду та оновлення адже наявні механізми далеко не завжди можуть забезпечити належний рівень суспільної довіри.

128. Рішення Шостого апеляційного адміністративного суду у справі № 855/17/19 від 04 лютого 2019 року: https://reyestr.court.gov.ua/Review/79614875.
129. Постанова Верховного Суду у справі № 855/17/19 від 08 лютого 2019 року: https://reyestr.court.gov.ua/Review/79699192.
130. З тексту Постанови Верховного Суду у справі № 855/17/19 від 08 лютого 2019 року: https://reyestr.court.gov.ua/Review/79699192.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

Захист персональних даних – це комплекс інструментів та механізмів не тільки нормативно-правового характеру (регулювання на рівні законів і підзаконних актів), але й система адміністративно-управлінських заходів, яких має вживати насамперед держава. Тут ідеться про встановлення юридичної відповідальності за порушення у сфері персональних даних. Разом з тим суб'єкт персональних даних також повинен мати змогу ефективно безпосередньо звертатися по захист своїх персональних даних щонайменше через надання йому можливості заборонити збір, обробку та використання його персональних даних. З огляду на це національним законодавством та міжнародними стандартами передбачено низку прав суб'єкта персональних даних щодо їх захисту.

Юридична відповідальність

Кримінальна відповідальність

Кримінальний кодекс України передбачає відповідальність за незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконну зміну такої інформації. Такі дії охоплюються складом злочину, передбаченого статтею 182 Кримінального кодексу України. Це основна стаття, що використовується для кримінально-правового гарантування прав людини у сфері персональних даних.

Судова практика щодо притягнення до відповідальності за порушення законодавства про захист персональних даних відносно вкрай мала. За аналізований проміжок часу (з січня 2016 року до жовтня 2021року) для ретельного аналізу дібрано понад сотня вироків, які набули законної сили.

Найпоширеніші в аспекті статті 182 Кримінального кодексу України справи, де особу притягають до кримінальної відповідальності за незаконне використання персональних даних, поєднане з іншими злочинами, скоєння яких було для засудженого головною метою. Тут, як приклад, можуть бути справи, де йдеться про заволодіння персональними даними і потім їх використання для отримання грошових коштів (безпосередньо в банку чи автоматизованих пристроях (терміналах, банкоматах); через оформлення кредитів (зокрема онлайн), використання електронних та інформаційних систем (веббанкінгу) тощо). Показовим тут можуть бути справи:

- особу засуджено за неодноразове використання персональних даних, отриманих із кількох викрадених мобільних телефонів[131];
- особа, користуючись службовим становищем (працювала в кредитній установі), вела незаконне збирання копій документів (паспортів та карток платника податків), а згодом їх використовувала для оформлення фіктивних кредитних договорів[132];
- особа, використовуючи незаконно зібрані персональні дані, втрутилася в роботу веббанкінгу іншої особи та заволоділа чужими грошовими коштами[133];

131. Див., наприклад, Вирок Луцького міськрайонного суду Волинської області у справі № 161/8390/21 від 13 жовтня 2021 року: https://reyestr.court.gov.ua/Review/100321832.
132. Див., наприклад, Вирок Ржищівського міського суду Київської області у справі № 374/70/21 від 07 жовтня 2021 року: https://reyestr.court.gov.ua/Review/100193020.
133. Див., наприклад, Вирок Ленінського районного суду м.Кіровограда у справі № 405/3899/21 від 29 вересня 2021 року: https://reyestr.court.gov.ua/Review/100076539.

- особа, користуючись службовим становищем незаконно отримувала з інформаційної системи (бази даних) персональні дані осіб, які згодом передавалися (продавалися) третім особам[134];
- особа використовувала незаконно отримані чутливі персональні дані (інформацію про приватне життя) з метою вимагання грошових коштів[135];
- особа несанкціоновано втручалася в роботу комп'ютерних мереж з метою дістати протиправно доступ до електронної пошти та облікових записів у соціальних мережах інших осіб[136];
- особа, користуючись можливістю доступу до комп'ютерної техніки потерпілого, незаконно зібрала персональні дані – інформацію про приватне життя іншої особи[137];
- особа, користуючись службовим становищем, надала доступ до бази даних (картотеки), що мітить персональні дані сторонній особі[138];
- особа на замовлення іншої особи вела незаконне візуальне спостереження за третьою особою та збирала відповідну інформацію, що містить персональні данні[139];
- особа незаконно виготовила та поширила інформацію (авдіовізуальний матеріал – відеоролик), що містить персональні дані та інформацію про приватне життя іншої особи[140].

Порушення законодавства про захист персональних даних суди встановлюють і при скоєнні інших складів злочинів, що не охоплюються приписами статті 182 Кримінального кодексу України. Зазвичай ідеться про злочини, внесені до розділу XVI, «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку»[141]. Властивість цієї категорії справ та, що судді розглядають відповідні матеріали насамперед під кримінально-правовим кутом зору, не вдаючись до аналізу законодавства про захист персональних даних, тільки побіжно згадають про персональні дані, які здобувають, обробляють чи поширюють незаконно. А в окремих випадках навіть зовсім не вдаються до загального аналізу обставин справи крізь призму захисту персональних даних[142].

---

134. Див., наприклад, Вирок Солом'янського районного суду м. Києва у справі № 760/23549/19 від 03 червня 2020 року: https://reyestr.court.gov.ua/Review/89736846.
135. Див., наприклад, Вирок Амур-Нижньодніпровського районного суду м. Дніпропетровська у справі № 199/8396/19 від 10 березня 2020 року: https://reyestr.court.gov.ua/Review/88085379.
136. Див., наприклад, Вирок Рівненського міського суду Рівненської області у справі № 569/12334/19 від 13 вересня 2019 року: https://reyestr.court.gov.ua/Review/84251500.
137. Див., наприклад, Вирок Жовтневого районного суду міста Маріуполя Донецької області у справі № 263/15031/20 від 13 травня 202і року: https://reyestr.court.gov.ua/Review/96871429.
138. Див., наприклад, Вирок Червоноармійського районного суду Житомирської області у справі № 292/777/20 від 23 червня 2020 року: https://reyestr.court.gov.ua/Review/89971342.
139. Див., наприклад, Вирок Луцького міськрайонного суду Волинської області у справі № 161/19355/19 від 17 грудня 2019 року. https://reyestr.court.gov.ua/Review/86405525
140. Див., наприклад, Вирок Миколаївського районного суду Львівської області у справі № 447/105/19 від 11 лютого 2019 року: https://reyestr.court.gov.ua/Review/79798221.
141. Див., наприклад, Вирок Тернопільського міськрайонного суду Тернопільської області у справі № 607/11197/16-к від 10 січня 2017 року: https://reyestr.court.gov.ua/Review/64087077; Вирок Фрунзівського районного суду Одеської області у справі № 517/471/19 від 01 жовтня 2019 року: https://reyestr.court.gov.ua/Review/84659143; Вирок Івано-Франківського міського суду Івано-Франківської області у справі № 344/4482/20 від 17 лютого 2021 року: https://reyestr.court.gov.ua/Review/94942478; Вирок Житомирського районного суду Житомирської області у справі № 278/1394/20 від 01 липня 2021 року: https://reyestr.court.gov.ua/Review/98026985; Вирок Оболонського районного суду м. Києва у справі № 756/9949/21 від 22 жовтня 2021 року: https://reyestr.court.gov.ua/Review/100494459.
142. Див., наприклад, Вирок Дунаєвецького районного суду Хмельницької області у справі № 674/1782/19 від 13 грудня 2019 року: https://reyestr.court.gov.ua/Review/86357578; Вирок Автозаводського районного суду м. Кременчука Полтавської області у справі № 524/8202/20 від 14 січня 2021 року: https://reyestr.court.gov.ua/Review/94131910; Вирок Кам'янець-Подільського міськрайонного суду Хмельницької області у справі № 676/1984/21 від 21 квітня 2021 року: https://reyestr.court.gov.ua/Review/96443215 та ін.

У більшості таких справ суд застосовує звільнення засудженого від відбування покарання, що в кожній конкретній справі, напевно, обґрунтовано та виправдано. Разом з тим узагальнений аналіз дає підстави зробити висновок, що у відповідних приписах Кримінального кодексу України встановлено зависокий рівень відповідальності або ж суди розглядають відповідні провадження гуманніше проти інших категорій справ з інших причин. Можливо, одна з причин – поки відносно невисокий рівень усвідомленості суспільством загроз, що можуть бути цілком реальними в разі порушення законодавства про захист персональних даних. Як підтвердження цієї думки, можна зауважити, що в окремих вироках (у зазначених вище категоріях кримінальних проваджень) судді навіть не вдаються до аналізу законодавства про захист персональних даних або ж і зовсім не згадують про персональні дані, хоч фактично притягають особи до відповідальності за незаконне використання персональних даних[143].

Цікавий приклад кримінального провадження, що стосується персональних даних, – справа № 200/3009/18, у якій ідеться про притягнення до кримінальної відповідальності судді, яка умисно не подала декларацію особи, уповноваженої на виконання функцій держави або місцевого самоврядування, передбачену Законом України «Про запобігання корупції». У цій справі обвинувачена вважає:

«… що в обвинувальному акті зазначено, що вона як суддя мала можливість отримати, проте не отримала електронний цифровий підпис для підпису декларацій, тобто фактично її звинувачують в тому, що вона умисно не отримала цифровий підпис. Однак закону, який би передбачав обов'язок отримувати судді цей підпис для подачі декларацій та закону, який би передбачав кримінальну відповідальність за його неотримання не існує. Взагалі, отримувати чи не отримувати цифровий підпис є її особистим правом, оскільки стосується особистого імені. Обвинувачена зазначила, що коли ОСОБА_4, який був відповідальним за отримання цифрових підписів, пропонував надати копії документів для виготовлення ЕЦП, то вона відмовлялась надавати копію паспорта та ідентифікаційного коду, оскільки вказані документи містять персональні дані, а це її право надавати згоду на обробку персональних даних, та на неї не покладено жодного обов'язку надавати, з будь-якого приводу, копію свого паспорта, копію ідентифікаційного коду, якщо вона цього не бажає. Документи, що видаються від її імені можуть бути підписані лише її оригінальним підписом. Обвинувачена не заперечує, що була ознайомлена з положеннями Закону України «Про запобігання корупції», при цьому вказала, що як тільки вийшов даний закон були проведені збори суддів, де вона говорила, що відмовляється від отримання ЕЦП. Обвинувачена підтвердила, що розписка про ознайомлення, яка була долучена до матеріалів кримінального провадження, дійсно підписувалась нею. Також, обвинувачена зазначила, що з цього приводу зверталася разом зі своїми колегами, які мали таку ж саму позицію, до різних державних органів, зокрема до Уповноваженого Верховної Ради з прав людини. Обвинувачена звертала увагу відповідних органів на те, що Закон України «Про захист персональних даних» є недоробленим, оскільки відмовитися від згоди на обробку персональних даних без негативного наслідку не можливо. На питання суду, чи вважає вона себе такою, що відносилась до категорії осіб, для яких дозвіл не передбачений законом з огляду на ту відповідь, яку їй надіслали листом від Державної служби з питань захисту персональних даних від 06 серпня 2012 року за N 10/34/0-12, не відповіла. Натомість, продовжувала стверджувати про те, що все одно Закон України «Про запобігання корупції» порушує її права. Також зазначила, що дана ситуація стосується не лише її, а й інших осіб, які не підтримують ті технології, які вводяться державою, оскільки мають бути дотримані при цьому альтернативні форми, в тому числі подання декларації…»[144].

---

143. Див., наприклад, Вирок Новозаводського районного суду міста Чернігова у справі № 751/3287/21 від 15 червня 2021 року: https://reyestr.court.gov.ua/Review/97683776.
144. З тексту Вироку Вищого антикорупційного суду у справі № 200/3009/18 від 28 травня 2020 року: https://reyestr.court.gov.ua/Review/89498404.

Попри відповідну позицію та її обґрунтування, обвинуваченому визнано винуватою вироком Вищого антикорупційного суду, відповідне рішення підтвердила Апеляційна палата Вищого антикорупційного суду[145]. Верховний Суд[146] вирок Вищого антикорупційного суду скасував у зв'язку з тим, що Рішенням Конституційного Суду України від 27 жовтня 2020 року № 13-р/2020 статтю 366-1 Кримінального кодексу України визнано неконституційною.

Щодо досудового розслідування, то тут питання збирання, обробки та використання персональних даних опирається насамперед на необхідність отримання відповідної згоди. Разом з тим слід наголосити, що, крім процедур, передбачених Законом України «Про захист персональних даних», вкрай важливе дотримання вимог кримінально-процесуального законодавства щодо збирання доказів і ходу досудового розслідування загалом. Предметом окремого аналізу можуть бути питання щодо надання доступу до речей і документів, надання згоди на проведення негласних слідчих та розшукових дій, збереження майна (що містить персональні дані), на яке накладено арешт та інші. Відповідні питання тільки частково спираються на застосування законодавства про захист персональних даних, тут змістовніший усе ж кримінально-процесуальний аспект. Відповідно, це може бути предметом окремого глибшого дослідження.

Як приклад, варто зазначити, що основний масив відповідних рішень слідчих суддів становлять ухвали про надання тимчасового доступу до речей і документів, які містять охоронювану законом таємницю. Значну більшість таких клопотань слідчі судді задовольняють[147]. При цьому слідчі судді зазвичай не вдаються до детального аналізу законодавства про захист персональних даних. Винятком можуть бути лише неналежно підготовлені клопотання слідчого чи прокурора або ж наявність обставин, які знімають потребу задоволення такого клопотання[148]. Проте такі недоліки клопотань стосуються кримінально-процесуального законодавства.

Водночас до клопотань, які подає сторона захисту, суди ставляться ретельніше і в окремих випадках досить ретельно вивчають необхідність порушення охоронюваної законом інформації. Наприклад, у справі № 757/55253/19-к слідчий суддя відмовив особі (потерпілій у кримінальному провадженні) в задоволенні клопотання про тимчасовий доступ до речей та документів, що перебувають у розпорядженні Олександрівської клінічної лікарні м. Києва, бо відповідні медичні відомості стосуються самої потерпілої і вона може з ними ознайомитися у звичайному порядку[149].

Інший приклад ретельнішого розгляду клопотання сторони захисту – справа № 645/2359/19, у якій суд зазначив:

«Відповідно до ч. ч. 1, 2 ст. 159 Кримінального процесуального кодексу України, тимчасовий доступ до речей і документів полягає у наданні стороні кримінального провадження особою, у володінні якої знаходяться такі речі і документи, можливості ознайомитися з ними, зробити їх копії та вилучити їх (здійснити їх виїмку). Тимчасовий доступ до електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку здійснюється шляхом зняття копії інформації,

145. Ухвала Апеляційної палати Вищого антикорупційного суду у справі № 200/3009/18 від 30 липня 2020 року: https://reyestr.court.gov.ua/Review/90760095.
146. Постанова Верховного Суду у справі № 200/3009/18 від 19 травня 2021 року: https://reyestr.court.gov.ua/Review/97104014.
147. Таких ухвал у Єдиному державному реєстрі судових рішень тисячі в різних категоріях справ, при цьому вони зазвичай однотипні й можуть бути більше предметом дослідження з погляду дотримання кримінально-процесуального законодавства.
148. Див., наприклад, Ухвалу слідчого судді Орджонікідзевського районного суду м. Запоріжжя у справі № 335/9325/20 від 03 лютого 2021 року: https://reyestr.court.gov.ua/Review/95018794; Ухвалу слідчого судді Краматорського міського суду Донецької області у справі № 234/2610/20 від 06 квітня 2020 року: https://reyestr.court.gov.ua/Review/88631165; Ухвалу слідчого судді Білоцерківського міськрайонного суду Київської області у справі № 357/9013/20 від 07 травня 2021 року: https://reyestr.court.gov.ua/Review/96818790 та ін.
149. Ухвала слідчого судді Печерського районного суду м. Києва у справі № 757/55253/19-к від 04 листопада 2019 року: https://reyestr.court.gov.ua/Review/85923862.

що міститься в таких електронних інформаційних системах або їх частинах, мобільних терміналах систем зв'язку, без їх вилучення. Тимчасовий доступ до речей і документів здійснюється на підставі ухвали слідчого судді, суду.

Таким чином, суд зобов'язаний перевіряти наявність об'єктивної необхідності та виправданість такого втручання у права і свободи особи, врахувати докази на підтвердження обставин, викладених у клопотанні, які мають бути надані ініціатором клопотання…

… Надання дозволу на такого роду втручання судова колегія вважає невиправданим у вказаному випадку, оскільки суд розглядає кримінальне провадження в межах висунутого ОСОБА_2 обвинувачення, отже обмеження прав інших осіб, які невстановлені в ході досудового розслідування, шляхом втручання в їх приватне спілкування через надання доступу до їх мобільних номерів суперечать цілям та завданням кримінального судочинства та виходить за межі обвинувачення.

Таким чином, враховуючи викладене, судова колегія доходить висновку про необґрунтованість доводів клопотання представника потерпілого про надання доручення органу досудового розслідування задоволенню не підлягає»[150].

Отже, суд аргументував відмову в задоволенні клопотання неприпустимістю надмірного втручання в приватне життя особи. Разом з тим таке оцінення суд зробив насамперед, виходячи з аналізу всіх обставин справи, вже вжитих кримінально-процесуальних заходів і слідчих дій. При цьому такий підхід набагато частіше застосовується до сторони захисту, що, зокрема, свідчить про доволі значне поширення в кримінальному судочинстві обвинувального характеру провадження, коли суд (інколи навіть усвідомлено) підтримує сторону обвинувачення, а не зберігає неупередженість і об'єктивність.

В ухвалах про обрання запобіжного заходу зазвичай суди не вдаються до детального аналізу і застосування законодавства про захист персональних даних, крім випадків, якщо йдеться про кваліфікацію злочину за відповідною статтею Кримінального кодексу України в частині можливого порушення порядку збирання, обробки чи використання персональних даних. При цьому навіть у таких ситуаціях судді тільки вдаються до відсильного посилання на відповідні приписи Закону України «Про персональні дані», як і у вироках в аналогічних справах, про що вже зазначено вище.

Окремо слід звернути на ситуацією з виконанням ухвал слідчих суддів про надання дозволу на тимчасовий доступ та вилучення (виїмку) речей і документів, які становлять охоронювану законом таємницю. Досить часто володільці відповідної інформації намагаються не надати її з посиланням на необхідність дотримання вимог законодавства про захист персональних даних чи з іншою легітимною метою захисту конфіденційної інформації від розголошення (наприклад, в інтересах слідства). У таких справах володільці інформації часто звертаються до слідчого судді по роз'яснення способу виконання відповідної ухвали. Слідчі судді зазвичай відмовляють у додатковому роз'ясненні й зазначають, що ухвала має бути виконана безпосередньо способом у ній зазначеним[151]. З відповідними заявами про надання роз'яснення інколи звертаються навіть органи досудового розслідування, що не бажають надавати (розкривати) матеріали досудового розслідування перед, наприклад, стороною захисту[152].

---

150. Ухвала колегії суддів Фрунзенського районного суду м. Харкова у справі № 645/2359/19 від 21 жовтня 2021 року: https://reyestr.court.gov.ua/Review/100631568.
151. Див., наприклад, Ухвалу слідчого судді Жовтневого районного суду м. Дніпропетровська у справі № 201/10060/20 від 09 грудня 2020 року: https://reyestr.court.gov.ua/Review/93947659; Ухвалу Слідчого судді Приморського районного суду м. Одеси у справі № 522/8146/19 від 05 лютого 2020 року: https://reyestr.court.gov.ua/Review/87379842; Ухвалу слідчого судді Херсонського міського суду Херсонської області у справі № 766/8719/17 від 11 лютого 2021 року: https://reyestr.court.gov.ua/Review/94820446 та ін.
152. Ухвала Слідчого судді Вищого антикорупційного суду у справі № 991/5942/21 від 11 жовтня 2021 року: https://reyestr.court.gov.ua/Review/100594291.

Досить складне для розв'язання питання ненадання згоди на доступ до персональних даних, насамперед медичного характеру. Суди зазвичай не вдаються до ухвалення окремого рішення про витребовування таких відомостей згідно із законом, а обмежуються наявною інформацією, якщо це критично потрібно для розв'язання справи по суті[153]. Разом з тим доволі поширене розв'язання судом при оціненні доказів питання їх допустимості з огляду на законодавство про захист персональних даних. Найчастіше ці питання постають щодо доступу до медичної інформації про стан здоров'я потерпілих чи підозрюваних (обвинувачених). Зазвичай суд у кожній конкретній ситуації оцінює допустимість використання відповідного доказу з огляду не тільки на законодавство про персональні дані, але й на кримінально-процесуальні особливості досудового розслідування. При цьому суди останньому аспектові, очевидно, приділяють основну увагу. Разом з тим є приклади, коли виконання вимог про захист персональних даних спрощує або навіть і знімає питання проведення спеціальних процесуальних дій. Наприклад, у справі № 337/3509/19 суд, оцінюючи допустимість результатів проведеної експертизи, зазначив:

«Судово-медична експертиза N 577 м від 15.07.2019 року є допустимим доказом, оскільки проведена за ухвалою слідчого судді, як того вимагало діюче на той час процесуальне законодавство. Використання при проведенні цієї експертизи медичної карти N 7884 з КНП «МЛЕ та ШМД» ЗМР стаціонарного хворого ОСОБА_2, яка згідно п. 2) ч. 1. ст. 162 КПК України містить охоронювану законом таємницю, є правомірним, оскільки медична карта були надана в рамках досудового розслідування, на запит слідчого, з одночасним письмовим погодженням самого ОСОБА_2, що є законним, відповідає ч. 2 ст. 93 КПК України, п. 1) ч. 2. ст. 7 ЗУ «Про захист персональних даних», і у зв'язку із згодою суб'єкта персональних даних до яких було отримано доступ, в такому випадку не потребує прийняття слідчим суддею окремого рішення про тимчасовий доступ до речей і документів»[154].

Зазвичай персональні дані, що не були отримані ані з дотриманням кримінально-процесуального, ані законодавства про захист персональних даних, суди до уваги не беруть. Як приклад, у справі № 501/3555/18 суд зазначив:

«Медична карта ОСОБА_1 містить відомості, що стосуються персональних даних про її лікування та стан здоров'я, тому з огляду на положення ч. 2 ст. 11 Закону України «Про інформацію» N 2657-XII від 2 жовтня 1992 року, ст. 7 Закону України «Про захист персональних даних» N 2297-VI від 1 червня 2010 року та рішення Конституційного Суду України від 30 жовтня 1997 року N 5-зп (справа N 18/203-97) могла бути надана для ознайомлення стороні захисту лише за згодою потерпілої або за ухвалою суду.

З матеріалів справи вбачається, що під час ознайомлення обвинуваченої з матеріалами досудового розслідування в порядку ст. 290 КПК України (а. с. 59) ОСОБА_2 з клопотанням про надання її для ознайомлення медичної картки потерпілої не зверталась. Медична картка надана потерпілою, долучена до матеріалів судової справи, тому сторона захисту не обмежена в праві ознайомитись з нею.

За таких обставин клопотання захисника про визнання доказу недопустимим задоволенню не підлягає»[155].

Такий підхід традиційний і трапляється в значній більшості судових рішень в аналогічних ситуаціях.

---

153. Див., наприклад, Вирок Ярмолинецького районного суду Хмельницької області у справі № 689/741/20 від 9 вересня 2021 року: https://reyestr.court.gov.ua/Review/99487654.
154. Див., наприклад, Вирок Хортицького районного суду міста Запоріжжя у справі № 337/3509/19 від 11 травня 2021 року: https://reyestr.court.gov.ua/Review/96803893.
155. Вирок Іллічівського міського суду Одеської області у справі № 501/3555/18 від 19 листопада 2020 року: https://reyestr.court.gov.ua/Review/93231735.

Адміністративна відповідальність

Адміністративна відповідальність за порушення законодавства про захист персональних даних встановлена статтею 18839 Кодексу України про адміністративні правопорушення. Судова практика застосування відповідної статті доволі широка, проте власне притягнення до адміністративної відповідальності настає далеко не в усіх справах.

Значну кількість справ суди закривають, бо нема події та складу адміністративного правопорушення[156] або ж у зв'язку із закінченням строків притягнення до адміністративної відповідальності[157]. Аргументація суддів очевидно в різних справах відрізняється, проте здебільшого проблематичні саме підтвердження належними доказами складу адміністративного правопорушення. Наприклад, у справі № 522/3111/21 суд зазначив:

«В ході судового розгляду встановлено, що ОСОБА_1, перебуваючи на посаді генерального директора ТОВ «ГЕРЦ», надав повне обґрунтоване пояснення стосовно того, що обробка персональних даних, до якої відноситься в тому числі, але не обмежуючись використання і поширення (розповсюдження, реалізація, передача), здійснюється ТОВ «ГЕРЦ» у межах Закону України «Про захист персональних даних», без будь-якого порушення законодавства про захист персональних даних. За таких обставин суд зробив висновок, що твердження про скоєння ОСОБА_1 інкримінованого йому адміністративного правопорушення ґрунтується на припущеннях та недопустимих доказах…

Відсутність достатніх доказів тягне за собою в даному випадку недоведеність події правопорушення і як наслідок відсутність об'єктивної сторони складу інкримінованого йому діяння.

Враховуючи зазначені обставини, аналізуючи в сукупності наявні в матеріалах справи докази, суд приходить до висновку, що в даному випадку відсутні достатні об'єктивні дані, які вказують на вчинення ОСОБА_1 адміністративного правопорушення, передбаченого саме ч. 4 ст. 188-39 КУпАП, на підставі чого справу про адміністративне правопорушення стосовно нього за вчинення адміністративного правопорушення, передбаченого ч. 4 ст. 188-39 КУпАП, слід закрити, у зв'язку з відсутністю в його діях складу адміністративного правопорушення»[158].

У справі № 337/3876/20 позиція суду щодо якості матеріалів (поданих до суду для притягнення до адміністративної відповідальності) була навіть жорсткіша. Зокрема, суд зазначив:

«Ухвалюючи рішення у цій справі, суд також виходить з того, що до протоколу не додано жодного належного та допустимого доказу, визначеного ст.251 КУпАП, на підтвердження факту вчинення ОСОБА_1 зазначеного адміністративного правопорушення.

Незважаючи на те, що за наявними матеріалами події стосуються порушення порядку захисту персональних даних ОСОБА_3 , саме нею ініційовано притягнення ОСОБА_1 до встановленої законом відповідальності, остання як потерпіла чи свідок уповноваженою посадовою особою, яка

156. Див., наприклад, Постанову Печерського районного суду м. Києва у справі № 757/46690/21-п від 12 жовтня 2021 року: https://reyestr.court.gov.ua/Review/100475543; Постанову Подільського районного суду м.Києва у справі № 758/14158/19 від 07 лютого 2020 року: https://reyestr.court.gov.ua/Review/87632133; Постанову Ковпаківського районного суду м. Сум у справі № 592/4220/21 від 01 липня 2021 року: https://reyestr.court.gov.ua/Review/98620189 та ін.
157. Див., наприклад, Постанову Святошинського районного суду м. Києва у справі № 759/19194/17 від 17 січня 2018 року: https://reyestr.court.gov.ua/Review/71703985; Постанову Жовтневого районного суду м. Маріуполя Донецької області у справі № 263/4314/18 від 11 травня 2018 року: https://reyestr.court.gov.ua/Review/73915418; Постанову Городищенського районного суду Черкаської області у справі № 691/1261/17 від 27 листопада 2017 року: https://reyestr.court.gov.ua/Review/70667984; Постанову Комунарського районного суду м. Запоріжжя у справі № 333/4999/16-п від 13.10.2016 року: https://reyestr.court.gov.ua/Review/62006490 та ін.
158. Постанова Приморського районного суду м. Одеси у справі № 522/3111/21 від 28 квітня 2021 року: https://reyestr.court.gov.ua/Review/96670427.

склала протокол про адміністративне правопорушення, не опитана, її пояснення як одні із передбачених ст.251 КУпАП джерел доказів в матеріалах справи відсутні, відомості про неї як потерпілу чи свідка в порушення ст.256 КУпАП в протоколі не зазначені.

Додані до протоколу фотознімки суд вважає неналежними та недопустимими доказами, оскільки вони не містять відомостей про час, місце скоєння адміністративного правопорушення, не вказують на особу, яка його вчинила. Жодних посвідчувальних написів ці фотознімки не містять, ким саме та із застосуванням яких технічних засобів вони вчинені не зазначено. Відомості про застосування будь-яких технічних засобів під час виявлення факту правопорушення та складання протоколу про адміністративне правопорушення в останньому взагалі відсутні.

При цьому, за доданим до матеріалів справи дорученням Уповноваженого ВРУ з прав людини на ім'я ОСОБА_5 остання як регіональний представник має право здійснювати перевірку (за необхідності з виїздом на місце) звернень громадян до Уповноваженого, стану дотримання прав людини, безперешкодно, без попереднього узгодження відвідувати підприємства, установи, організації, отримувати відомості щодо з'ясування обставин подій тощо.

Відомостей про застосування зазначених заходів ОСОБА_5 як уповноваженою посадовою особою з метою встановлення обставин вчинення адміністративного правопорушення, збирання та належного оформлення доказів матеріали справи не містять.

Таким чином, виходячи з вимог ст. 252, 280 КУпАП, всебічно, повно та об'єктивно оцінивши обставини справи та надані докази за своїм внутрішнім переконанням, керуючись законом та правосвідомістю, суд вважає, що факт вчинення ОСОБА_1 адміністративного правопорушення, передбаченого ч.4 ст.188-39 КУпАП, та його винуватість в ньому належними та допустимими доказами не доведені, що в силу принципу презумпції невинуватості трактується судом на його користь»[159].

В окремих випадках суди повертають матеріали суб'єктові їх складення у зв'язку з неналежним підготуванням[160]. Слід наголосити, що апеляційного оскарження судових рішень у справах, де особа не була притягнута до адміністративної відповідальності (з будь-яких із зазначених вище підстав) зазвичай суб'єкт складення протоколу не проводить. З іншого боку, апеляційні скарги осіб притягнутих до відповідальності на підставі 188-39 Кодексу України про адміністративні правопорушення здебільшого не задовольняються[161].

Серед судових рішень, якими притягнуто до адміністративної відповідальності на підставі 18839 Кодексу України про адміністративні правопорушення, чимало справ, що стосуються саме поширення персональних даних суб'єктами владних повноважень в інтернеті (на своїх офіційних вебсайтах чи сторінках у соціальних мережах).

У справі № 456/3297/21 встановлено порушення в частині поширення на офіційній сторінці Стрийської міської ради в соціальній мережі «Фейсбук» персональних даних осіб боржників

---

159. Постанова Хортицького районного суду м. Запоріжжя у справі № 337/3876/20 від 30 жовтня 2020 року: https://reyestr.court.gov.ua/Review/92657926.
160. Див., наприклад, Постанову Долинського районного суду Кіровоградської області у справі № 388/750/21 від 01 червня 2021 року: https://reyestr.court.gov.ua/Review/97308845; Постанову Дружківського міського суду Донецької області у справі № 229/437/20 від 30 січня 2020 року: https://reyestr.court.gov.ua/Review/87425006; Постанову Іллічівського міського суду Одеської області у справі № 501/2458/19 від 29 липня 2019 року. https://reyestr.court.gov.ua/Review/83540276; Постанову Носівського районного суду Чернігівської області у справі № 741/1115/18 від 23 жовтня 2018 року. https://reyestr.court.gov.ua/Review/77422400 та ін.
161. Див., наприклад, Постанову Апеляційного суду Кіровоградської області у справі № 389/300/17 від 22 березня 2017 року: https://reyestr.court.gov.ua/Review/65606253; Постанову Сьомого апеляційного адміністративного суду у справі № 806/536/17 від 09 вересня 2019 року: https://reyestr.court.gov.ua/Review/84133610; Постанову Київського апеляційного суду у справі № 761/23532/20 від 18 грудня 2020 року: https://reyestr.court.gov.ua/Review/94663887 та ін.

перед Комунальним підприємством «Стрийводоканал» за отримані житлово-комунальні послуги з водопостачання та водовідведення, зокрема адрес таких боржників та сум їх заборгованості[162].

У справі № 727/7599/21 до адміністративної відповідальності притягнуто за оприлюднення звернення фізичної особи на офіційному вебсайті Чернівецької міської ради, що спричинило поширення персональних даних на офіційному вебсайті Чернівецької міської ради[163].

У справі № 608/1904/21 йдеться про незаконне оприлюднення на вебсайті Чортківської міської ради рішень виконавчого комітету, які містять персональні дані фізичних осіб (прізвища, ім'я, по батькові, дати народження, адреси проживання, обставини особистого життя тощо)[164].

Прикладів таких рішень чимало[165]. Разом з тим слід звернути увагу на масштаб відповідних правопорушень – вони стосуються зазвичай оприлюднення персональних даних в інтернеті. Попри це, в інших категорія справ про адміністративні правопорушення практично немає згадувань про порушення законодавства про захист персональних даних. Ба більше, суди не розглядають інші категорії справ, із серйознішими порушеннями персональних даних. Це видається щонайменше дивним, з огляду на величезну кількість цивільних справ та кримінальних проваджень. Така ситуація пояснюється, зокрема поки триванням реформування (інституціоналізації) державного контролю у сфері персональних даних.

Дисциплінарна відповідальність

Притягнення до дисциплінарної відповідальності простежувати повноцінно в судовій практиці вкрай важко, бо процедура застосування цього виду юридичної відповідальності може відображатися в судових рішеннях тільки в разі оскарження особою застосованих до неї стягнень. Разом з тим такі приклади також є.

Як приклад, справа № 487/1982/17: медичний працівник оскаржувала притягнення її до дисциплінарної відповідальності за розголошення персональних даних. У цій справі йдеться про «… надання інтерв'ю сторонній особі і розголошення відомостей про пацієнта із зазначенням його прізвища, проведення операції, знеболення сибазоном, вживання твердження, що пацієнт є наркоманом, вживає наркотичні засоби і в нього були ломки»[166]. Тут цікаве застосування різними судами законодавства про захист персональних даних. Адже суд першої інстанції не побачив у діях відповідного медичного працівника (позивачки, яка оскаржувала наказ про накладення дисциплінарного стягнення за «порушення лікарської таємниці, вимог професійної етики, деонтології, […] посадової інструкції») підстав для настання юридичної відповідальності і скасував відповідний наказ головного лікаря. Основою для обґрунтування такої позиції було недоведення факту поширення персональних даних. Суд першої інстанції встановив:

«… представник відповідача так і не вказала суду, якій сторонній особі було надано таке інтерв'ю, ким цей запис було опубліковано, судом особа, якій давалось інтерв'ю не допитувалась,

162. Постанова Стрийського міськрайонного суду Львівської області у справі № 456/3297/21 від 18 серпня 2021 року: https://reyestr.court.gov.ua/Review/99098891.
163. Постанова Шевченківського районного суду м.Чернівців у справі № 727/7599/21 від 27вересня 2021року: https://reyestr.court.gov.ua/Review/100154843.
164. Постанова Чортківського районного суду Тернопільської області у справі № 608/1904/21 від 16 вересня 2021 року: https://reyestr.court.gov.ua/Review/99671794.
165. Див., наприклад, Постанову Шевченківського районного суду м.Києва у справі № 761/23539/20 від 11 вересня 2020 року: https://reyestr.court.gov.ua/Review/91538114.
166. З тексту Постанови Верховного Суду у справі № 487/1982/17 від 20 травня 2019 року: https://reyestr.court.gov.ua/Review/81925629.

і крім того, із переглянутого судом відеозапису встановлено, що ОСОБА_3 під час цього інтерв'ю ніякої інформації відносно пацієнта ОСОБА_5 не розповсюджувала»[167].

Проте рішенням суду апеляційної інстанції рішення суду першої інстанції скасовано та ухвалено нове рішення, яким у задоволенні позову відмовлено:

«Враховуючи те, що в позовній заяві ОСОБА_5 не заперечувала ні сам факт інтерв'ю сторонній особі у зв'язку з подіями 23 лютого 2017 року, які пов'язані з ОСОБА_7, ні поширення під час цього інтерв'ю інформації, яка міститься в довідці від 14 березня 2017 року, а обставини викладені у скаргах ОСОБА_7 і в наказі роботодавця про притягнення до дисциплінарної відповідальності повністю підтверджуються даними відеозапису названого інтерв'ю, то висновок суду про наявність підстав для задоволення позову є помилковим»[168].

Це досить показовий приклад, коли суд робить акцент більше на процесуальних особливостях оцінення обставин справи, а не змісті поняття «персональні дані». Рішеннями апеляційної та касаційної інстанції відповідну позицію відкориговано.

Відшкодування завданої шкоди

Відшкодування шкоди за порушення вимог законодавства про захист персональних даних має бути предметом окремого судового розгляду. У відносно поширених справах щодо оскарження положень кредитних договорів (які містять протиправні зобов'язання щодо надання позичальником безумовної, безвідкличної та безстрокової згоди на обробку персональних даних) суди досить часто зазначають, що порушення відповідними положеннями договорів законодавства про захист персональних даних не може бути підставою для визнання договорів недійсними, натомість способом захисту порушених прав особи може бути відшкодування винною особою завданих збитків та (або) моральної шкоди.

«Посилання на порушення при використанні персональних даних не є обставиною, яка тягне за собою скасування договору або визнання його недійсним. Захист права позивача у цьому разі, у разі наявності такого порушення, може бути реалізоване іншим видом судочинства, зокрема, кримінальним чи адміністративним»[169].

У такій же справі Верховний Суд, підтвердивши таку правову позицію, зазначив: «З урахуванням викладеного, суд першої інстанції, з рішенням якого погодився апеляційний суд, дійшов правильного висновку про те, що в разі поширення персональних даних чи розголошення банківської таємниці з порушенням передбаченого законом порядку способом захисту порушених прав особи може бути відшкодування винною особою завданих збитків та (або) моральної шкоди, а не скасування (чи визнання недійсним) правочину»[170].

Як наслідок, звернення до суду щодо відшкодування моральної шкоди має робитися із зазначенням окремої повноцінної аргументації, належної у відповідній категорій справ, відповідно до цивільно-процесуального законодавства та судової практики.

Також слід зазначити, що відшкодування завданої шкоди – запорука змістовного гарантування державою ефективності та реального захисту прав людини. У справах про шкоду, завдану

167. Рішення Заводського районного суду м. Миколаєва у справі № 487/1982/17 від 26 березня 2018 року: https://reyestr.court.gov.ua/Review/73131097.
168. Постанова Апеляційного суду Миколаївської області у справі № 487/1982/17 від 23 травня 2018 року: https://reyestr.court.gov.ua/Review/74202704.
169. Рішення Жовтневого районного суду Миколаївської області у справі № 477/991/15-ц від 21 липня 2016 року: https://reyestr.court.gov.ua/Review/59327238.
170. Постанова Верховного Суду у справі № 477/991/15-ц від 11 грудня 2018 року. https://reyestr.court.gov.ua/Review/78495991

внаслідок неправомірного поширення персональних даних суди далеко не завжди безумовно застосовують відповідні вид і міру відповідальності щодо винної особи.

Показовою тут може бути справа № 369/5585/15-ц, де суди першої, апеляційної та касаційної інстанцій фактично зайняли позицію, що «…сам по собі факт розповсюдження персональних даних не може бути підтвердженням завдання моральної шкоди, а Законом України «Про захист персональних даних» не передбачено відшкодування моральної шкоди»[171]. Власне, суди[172] встановили факт порушення вимог чинного законодавства щодо таємниці телефонних розмов і розповсюдження персональних даних, попри це вважали необхідним додаткове доведення позивачем заподіяння йому моральної шкоди. Щодо такої позиції судів Верховний Суд України зазначив:

«Оцінюючи завдану моральну шкоду, позивач виходив з кількості прослуховувань його телефонної розмови, що була розміщена у вільному доступі в мережі Інтернет.

Зазначаючи, що факт розповсюдження персональних даних не може бути підтвердженням завдання моральної шкоди, суди не звернули уваги на те, що позивач пов'язував моральну шкоду із спричиненими йому неправомірними діями відповідача душевними стражданнями.

При цьому, встановивши неправомірність дій щодо поширення телефонної розмови та фактично порушення особистого немайнового права позивача, суди не звернули уваги на приписи статті 276 ЦК України щодо обов'язку особи, діями якої порушене особисте немайнове право фізичної особи, вчинити необхідні дії для його поновлення.

Між тим, будь-яких доказів на підтвердження поновлення права позивача щодо таємниці телефонної розмови, зокрема, вжиття заходів з видалення її запису з вільного доступу в мережі Інтернет, матеріали справи не містять.

Відповідно до частини другої статті 276 ЦК України, якщо дії, необхідні для негайного поновлення порушеного особистого немайнового права фізичної особи, не вчиняються, суд може постановити рішення щодо поновлення порушеного права, а також відшкодування моральної шкоди, завданої його порушенням.

Моральна шкода, завдана фізичній або юридичній особі неправомірними рішеннями, діями чи бездіяльністю, відшкодовується особою, яка її завдала, за наявності її вини, крім випадків, встановлених частиною другою цієї статті (частина перша статті 1167 ЦК України).

Відмовляючи у задоволенні заявлених вимог з підстав недоведеності спричинення шкоди, суди фактично поклали на позивача обов'язок довести наявність у нього душевних страждань з приводу порушення його права на таємницю телефонного спілкування, що є неприпустимим з огляду на правову природу такого права, гарантії від порушень якого закріплені Конституцією України.

У даному випадку суди мали б виходити з презумпції спричинення позивачу моральної шкоди відповідачем та обов'язку саме відповідача спростувати таку презумпцію.

Отже, неправильне застосування судами вищенаведених норм матеріального права призвело до неправильного вирішення справи, а це відповідно до статті 3604 ЦПК України є підставою для

171. З тексту Постанови Верховного Суду України у справі № 369/5585/15-ц від 27 вересня 2017 року: https://reyestr.court.gov.ua/Review/70427210.

172. Див.: Рішення Києво-Святошинського районного суду Київської області у справі № 369/5585/15-ц від 08 грудня 2015 року: https://reyestr.court.gov.ua/Review/54667551; Ухвала Апеляційного суду Київської області у справі № 369/5585/15-ц від 09 березня 2016 року: https://reyestr.court.gov.ua/Review/56399149; Ухвала Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ у справі № 369/5585/15-ц від 26 квітня 2017року: https://reyestr.court.gov.ua/Review/66699194.

скасування судових рішень судів першої, апеляційної та касаційної інстанцій в частині вимог про відшкодування моральної шкоди»[173].

Така правова позиція суду касаційної інстанції змістовніше охоплює можливість ефективного судового захисту порушеного права та одночасного звернення з вимогою про відшкодування завданої шкоди. Щоправда, на практиці застосування такої позиції все одно потребує додаткової роботи та обґрунтування від позивачів.

Одночасно варто вказати, що запровадження надійного та ефективного механізму відшкодування шкоди для суб'єктів даних є актуальним та потребує додаткових зусиль як в процесі нормотворчості, так і під час правозастосування.

Право суб'єкта персональних даних заборонити обробку

Судова практика також має приклади хибного сприйняття громадянами права на заборону використання їхніх персональних даних, а в окремих випадках – навіть зловживання відповідним правом. Показовою тут може бути справа № 465/4390/17, у якій позивач (фізична особа) оскаржує дії начальника Управління патрульної поліції у м. Львові щодо надання його (позивача) персональних даних інженерові відділу з паркування Львівського комунального підприємства «Львівавтодор» для складення стосовно нього (позивача) протоколу про адміністративне правопорушення за порушення правил паркування. Суди першої[174], апеляційної[175] та касаційної інстанції дали належну правову оцінку цій ситуації та встановили, що порушень законодавства про захист персональних даних з боку начальника Управління патрульної поліції у м. Львові не було. Зокрема, Верховний Суд у цій справі зазначив:

«38. Зі змісту наведених норм Конституції України, Законів 2657-XII, № 2939-VI та № 2297-VI вбачається що до конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження.

39. Не допускаються 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 захисту прав людини.

40. Приписами підпункту «б» пунктом 5.2 Рекомендації № R(87)15Комітету Міністрів державам-членам, що регулює використання персональних даних у секторі поліції (Схвалено Комітетом Міністрів 17 вересня 1987 на 410-й зустрічі заступників Міністрів) визначено, що передача даних іншим державним органам дозволяється в окремих випадках, якщо ці дані необхідні одержувачу для виконання ним його правомірного завдання, при цьому передбачається, що ціль збирання чи обробки, яка здійснюватиметься одержувачем, не є несумісною з первинною обробкою, а правові зобов'язання передаючого органу, не суперечать цьому.

41. Норми статті 255 КУпАП визначають перелік органів, які мають право складати протоколи про адміністративні правопорушення, зокрема, посадові особи, уповноважені на те виконавчими комітетами.

---

173. Постанова Верховного Суду України у справі № 369/5585/15-ц від 27 вересня 2017 року: https://reyestr.court.gov.ua/Review/70427210.
174. Рішення Франківського районного суду м. Львова у справі № 465/4390/17 від 26.12.2017 року: https://reyestr.court.gov.ua/Review/71439748.
175. Постанова Львівського апеляційного адміністративного суду у справі № 465/4390/17 від 14 травня 2018 року: https://reyestr.court.gov.ua/Review/74098229.

42. Із вказаного переліку вбачається, що законодавець уповноважує, як державні так і не державні органи на вчинення дій щодо складання протоколів про правопорушення…

45. Верховний Суд звертає увагу, що Львівська міська рада звернулася до Управління патрульної поліції у м. Львові із запитом про надання інформації саме для виконання покладених на неї законодавцем дій щодо складання протоколу про адміністративне правопорушення.

46. У відповідь на даний запит Управління патрульної поліції (лист від 22 червня 2016 року № 17083/41/12/01/2016) надало запитувану інформацію, долучивши відповідні витяги із системи «НАІС» МВС України.

47. Отже, у даному випадку Управлінням патрульної поліції у м. Львові надано інформацію органу (Львівській міській раді) для виконання нею її правомірного завдання, відповідно до приписів КУпАП.

48. Таким чином, Верховний Суд погоджується із висновком судів першої та апеляційної інстанцій, що дії начальника Управління патрульної поліції у м.Львові Департаменту патрульної поліції Пузиревського Антона Михайловича щодо передачі конференційної інформації ОСОБА_1 Львівській міській раді вчинені на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України»[176].

Як приклад заперечення проти обробки персональних даних можна навести рішення судів у справі № 127/10831/17, де через свої релігійні переконання низка фізичних осіб відмовилася від умов заяви-приєднання до умов договору постачання природного газу побутовим споживачам і відмовилася від присвоєння їм EIC-коду (Energy Identification Code, персоніфікований EIC-код для кожного суб'єкта ринку природного газу – це елемент системи кодування, рекомендованої Європейською мережею операторів газотранспортних систем). Апеляційний суд Вінницької області позов задовольнив частково і постановив:

«Скасувати присвоєний ОСОБА_6, ОСОБА_7, ОСОБА_3, ОСОБА_5 EIC-код, штрих-код, десятизначний рахунок споживачів, номер запису у реєстрі (УЗНР) та зобов'язати Публічне акціонерне товариство «Вінницягаз», Товариство з обмеженою відповідальністю «Вінницягаз Збут» виключити їх з баз даних.

Вести облік, всю необхідну документацію стосовно ОСОБА_6, ОСОБА_7, ОСОБА_3, ОСОБА_5 як побутових споживачів за прізвищем, ім'ям, по батькові, місцем проживання, без збору та обробки їх персональних даних»[177].

У схожій справі Верховний Суд підтвердив аналогічний підхід, зазначивши:

«З урахуванням наведених норм та встановивши, що позивач за своїми релігійними переконаннями категорично заперечує проти обробки її даних та присвоєння їй будь-яких числових ідентифікаторів, суд першої інстанції дійшов обґрунтованого висновку про наявність підстав для зобов'язання відповідачів видалити з баз даних персонального EIC-коду та інших штрих-кодових ідентифікаторів стосовно ОСОБА_2 , а також ведення обліку і всієї необхідної документації стосовно позивача як побутового споживача за прізвищем, ім'ям, по батькові та місцем фактичного проживання.

Реалізація права ОСОБА_2 зумовлена її релігійними переконаннями та пов'язана з неприпустимістю користуватися будь-якими числовими, буквено-цифровими, штрих-кодовими, QR-кодовими,

176. Постанова Верховного Суду у справі № 465/4390/17 від 13 жовтня 2020 року: https://reyestr.court.gov.ua/Review/92173101.
177. Рішення Апеляційного суду Вінницької області у справі № 127/10831/17 від 25 жовтня 2018 року: https://reyestr.court.gov.ua/Review/77481988.

біометричними ідентифікаторами, і зазначене не заборонено та не обмежене законом, а тому людина в межах реалізації своїх гарантованих прав може відмовитися від присвоєння їй чисел та використання їх.

Установлюючи ті чи інші правила поведінки (у цьому випадку шляхом присвоєння штрих-коду, QR-коду, десятизначного рахунку споживачеві), держава має в першу чергу дбати про потреби людей, утримуючись за можливості від встановлення таких правил, які негативно сприйматимуться тими чи іншими групами суспільства (зокрема, релігійною спільнотою). Встановлення таких правил може бути виправдане тільки наявністю переважаючих суспільних інтересів, які не можуть бути задоволені в інший спосіб, але і в цьому разі має бути дотриманий принцип пропорційності»[178].

Опираючись на потребу захисту релігійних прав конкретних осіб, суд повністю заборонив вести обробку персональних даних при наданні послуг відповідним споживачам, що видається фактично нереалістичним щодо виконання. Ба більше, суди всіх інстанцій, попри посилання на положення Закону України «Про захист персональних даних», практично зовсім не проаналізували особливості його застосування в цій конкретній ситуації, а застосували підхід з використанням можливості «абсолютної заборони» на використання персональних даних.

Інший важливий аспект – це необхідність доведення факту незаконного використання персональних даних фізичною особою, що інколи може бути вкрай непростим завданням. Особливо якщо йдеться про електронні системи (реєстри, бази даних, спеціальне програмне забезпечення тощо), які технічно та технологічно контролюють потенційний порушник та/або третя особа. У таких справах йдеться про цивільне провадження, що вимагає від позивача доведення тих обставини, на які він посилається як на підставу своїх вимог або заперечень (частина перша статті 81 Цивільного процесуального кодексу України). Суди зазвичай саме на цій підставі відмовляють у задоволенні позовних вимог[179]. З огляду на це, реалізація права суб'єкта на заперечення проти обробки його персональних даних доволі ускладнена.

Суди зазвичай займають позицію суб'єктів персональних даних у разі наявності спору з суб'єктами владних повноважень (володільцями чи розпорядниками персональних даних) щодо надання доступу до інформації про самого суб'єкта звернення. Таку позицію суди займають навіть у разі, коли змістовної інформації щодо особи фактично нема (на думку органу влади), проте особі відмовили в наданні інформації про це[180].

У судовій практиці також досить часто трапляються випадки, коли, посилаючись на гарантії, передбачені законодавством про захист персональних даних, особи намагаються визнати договори (цивільно-правові чи господарські) недійсними. Вище вже проаналізовано приклади таких ситуацій у справах про укладення договорів споживчого кредитування.

Тут можна додатково навести приклад дещо масштабнішої справи, де позивач намагався з посиланням на захист персональних даних зупинити дію низки договірних правовідносин, а також заборонити здійснювати повноваження Національному банкові України та іншим органам державної влади. У справі № 760/27582/17 суд першої інстанції з урахуванням аргументації позивача про необхідність захисту персональних даних задовольнив заяву про забезпечення позову і заборонив «… виконувати умови, вимоги та будь-які інші положення будь-яких договорів, угод,

178. Постанова Верховного Суду у справі № 579/806/19 від 21 квітня 2021 року: https://reyestr.court.gov.ua/Review/96501519.
179. Див. наприклад, Рішення Печерського районного суду міста Києва у справі № 183/6565/17-ц від 05 вересня 2018 року: https://reyestr.court.gov.ua/Review/78375041#.
180. Див., наприклад, Постанову Деснянського районного суду м. Києва у справі № 754/6262/16-а від 05 грудня 2017 року: https://reyestr.court.gov.ua/Review/70970356.

контрактів, довіреностей та будь-яких інших правочинів, укладених з Національним банком України та/або ПАТ КБ «ПРИВАТБАНК» та/або Міністерством фінансів України, що прямо та/або опосередковано стосуються та/або будь-яким чином впливають та/або впливатимуть на права та/або законні інтереси ОСОБА_1, в тому числі та не обмежуючись заборонити виконувати будь-які повноваження та користуватися будь-якими правами, що прямо чи опосередковано зазначені та/або випливають з будь-яких договорів, угод, контрактів, довіреностей та будь-яких інших правочинів, укладених з Національним банком України…»[181]. Згодом відповідну Ухвалу скасував суд апеляційної інстанції[182] і таке рішення підтвердила касаційна інстанція, зокрема з мотивацією, що « …місцевий суд не врахував, що відповідно до вимог ЦПК України заходи забезпечення позову повинні застосовуватись лише в разі необхідності та бути співмірними із заявленими вимогами, оскільки безпідставне забезпечення позову може призвести до порушення прав і законних інтересів інших осіб»[183].

Вкрай важливе є забезпечення можливості досудового врегулювання спору щодо незаконного на думку хоча б однієї зі сторін поводження з персональними даними. Як показовий приклад, тут можна навести справу № 757/40209/20-ц, у якій ідеться про вимогу позивача (фізичної особи) до фінансової установи вжити заходів для припинення дії кредитних договорів, які він не укладав, а уклали інші, невідомі йому особи з використанням його персональних даних (без його відома) через спеціальні електронні інструменти в інтернеті. Власне, відповідач не тільки не вжив відповідних заходів для перевірки висловлених позивачем доводів, а й, навпаки, зі слів позивача, вживав активних дій для забезпечення виконання позивачем відповідних кредитних договорів. Суд першої інстанції дійшов висновку:

«Ураховуючи те, що позивач не мав наміру укладати з відповідачами кредитні договори, не подавав заявок на онлайн кредити, не мав волевиявлення на оформлення кредитних договорів та не отримував грошових коштів від цих фінансових установ, наявні підстави для висновку про наявність факту незаконної обробки відповідачами персональних даних позивача»[184].

Апеляційний суд залишив рішення суду першої інстанції без змін. В цьому аспекті слід звернути увагу, що встановлення судом факту незаконної чи невірогідної обробки персональних даних – підстава для їх видалення. Разом з тим відповідне рішення міг ухвалити відповідач і на етапі «адміністративного» оскарження, тобто за результатами розгляду відповідних заяв і скарг позивача на досудовому етапі.

181. З тексту Ухвали Солом'янського районного суду м. Києва у справі № 760/27582/17 від 15 грудня 2017 року: https://reyestr.court.gov.ua/Review/71023966.
182. Постанова Апеляційного суду м. Києва у справі № 760/27582/17 від 28 серпня 2018 року. https://reyestr.court.gov.ua/Review/76160701.
183. Постанова Верховного Суду у справі № 760/27582/17 від 29 травня 2019 року: https://reyestr.court.gov.ua/Review/82419826.
184. Рішення Печерського районного суду м. Києва у справі № 757/40209/20-ц від 21 січня 2021 року: https://reyestr.court.gov.ua/Review/94605296.

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

Провівши загальний аналіз судової практики, можна виокремити такі основні тези, тенденції та напрямки:

Приписи Закону України «Про захист персональних даних» у багатьох моментах потребують уточнення та конкретизації, бо обумовлюють різне тлумачення їх змісту судами. При цьому проблемні не стільки прогалини в регулюванні (тут суди вдаються до застосування за аналогією приписів інших законів, що регулюють інформаційні правовідносини), скільки колізійні моменти суперечливого регулювання одних правовідносин (процедур) різними нормами (наприклад, змішування в різних справах правових режимів публічної інформації та персональних даних). Зважаючи на це, перегляду потребує не тільки Закон України «Про захист персональних даних», але й низка суміжних законів, що регулюють споріднені правовідносини.

Міжнародні стандарти щодо захисту персональних даних суди застосовують доволі часто, проте, на жаль, інколи таке застосування більше церемоніальне, наприклад, через просте цитування міжнародних договорів чи практики Європейського суду з прав людини. При цьому зазвичай суди покликаються на загальні акти (наприклад, Конвенцію про захист прав людини та основоположних свобод), не надаючи уваги конкретнішим актам (наприклад, Конвенції про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних). Очевидно, що це потребує додаткових заходів для розвитку відповідних знань, вмінь і навичок у суддів.

Застосування законодавства про захист персональних даних з кожним роком стає глибшим та цілеспрямованішим, суди узгоджують свою практику з правовими позиціями вищих інстанцій, що, безумовно, сприяє єдності судової практики. У цьому аспекті слід відзначити роботу Верховного Суду, який у багатьох сферах, переглядаючи рішення судів апеляційної, а інколи й першої інстанцій, формував правові позиції, що, загалом відповідають міжнародним стандартам захисту персональних даних.

Аргументація судових рішень далеко не завжди належна та ґрунтовна. У цій категорії справ це особливо важливо, бо йдеться про визначення меж обмеження втручання держави в приватне життя особи. Це вимагає не тільки доволі ретельного вивчення всіх обставин справи, але й надання їм належної оцінки, що обов'язково має бути відображена в тексті судового рішення. Суди обґрунтовують власну позицію переважно цитуванням текстів законів, а не їх безпосереднім застосуванням. За таких обставин інколи навіть важко зрозуміти логіку, на основі якої суд дійшов висновку, що відображений у резолютивній частині рішення.

У діяльності органів державної влади досі спостерігається не зовсім коректне розуміння змісту і значення деяких приписів законодавства про захист персональних даних. Наприклад, досі вкрай поширена «абсолютизація» одержання згоди на обробку персональних даних від їх суб'єкта. Це часто спричиняє неможливість реалізації інших прав людини, наприклад щодо отримання соціального захисту (субсидій, пільг, виплат тощо). Проблемне те, що такі ж помилки щодо розуміння базових понять у сфері персональних даних повторюють і суди. За таких обставин варто скоригувати законодавство хоча б у найкритичніших блоках нормативного регулювання.

В адміністративних провадженнях щодо надання громадянам публічних (зокрема адміністративних послуг) є кілька блоків проблем, які опосередковано унеможливлюють здійснення органами публічної влади ефективного управління. У таких справах виникають колізії між, наприклад, законодавством про функціонування публічних реєстрів (інформаційних систем, баз даних

тощо), правом на захист персональних даних і правом на свободу віросповідання (реалізації релігійних переконань). Наприклад, у справі про паспорт у формі книжечки Верховний Суд однозначно вказав, що розв'язання таких проблем судами без внесення відповідних змін до законів неможливе.

Доволі часто трапляються зловживання правом на захист персональних даних у ситуаціях, де це не обґрунтовано. Існують цілі блоки (напрямки) справ, в яких позивачі намагаються визнати недійсними цивільно-правові договори (наприклад, кредитні договори з невигідними для позичальника умовами), маніпулюючи змістом і способом захисту персональних даних, зокрема в частині оскарження надання/ненадання згоди на обробку персональних даних. Аналогічні приклади є і зі зловживанням у частині «захисту» персональних даних при оскарженні ухвал слідчих суддів про надання тимчасового доступу до речей і документів. Ці та низку інших моментів має врахувати законодавець при внесенні змін до відповідних законів.

При розгляді кримінальних проваджень у справах, що стосуються персональних даних, суди переважно акцентують увагу на кримінально-правових особливостях кваліфікації злочинів, інколи не вдаючись до ретельного з'ясування змісту законодавчих вимог саме щодо обробки персональних даних. У більшості проваджень до кримінальної відповідальності за незаконне збирання, обробку чи використання персональних даних притягають одночасно з іншими складами кримінальних правопорушень. Відповідно, обґрунтування суду щодо захисту персональних даних інколи «губиться» серед інших обставин справи. В окремих випадках кваліфікація відповідних злочинів не зробиться окремо зовсім, а порушення обробки персональних даних визначається як спосіб скоєння іншого злочину. Очевидно, що це потребує додаткових заходів для розвитку відповідних знань, вмінь і навичок у суддів.

У справах про адміністративні правопорушення кількість випадків притягнення до адміністративної відповідальності відносно невелика. Є дуже велика кількість справ, де суди закривають провадження, бо нема події та складу адміністративного правопорушення, або ж у зв'язку із закінченням строків притягнення до адміністративної відповідальності, або повертають матеріали суб'єктові складення відповідного протоколу для їх (матеріалів) належного оформлення. Інший важливий тут момент – це те, що більшість направлених до суду протоколів стосуються відносно дрібних порушень (наприклад, оприлюднення на вебсайті органу документів, що містять персональні дані), тоді як дійсно серйозних порушень вкрай мало. Це свідчить про актуалізацію потреби реформування державного контролю за дотриманням законодавства про захист персональних даних.

Ці та інші виявлені та окреслені в цьому аналізі тенденції демонструють доволі високий рівень обізнаності суддів із засадами законодавства про захист персональних даних. Разом з тим окремі аспекти потребують детальнішого регулювання на рівні законодавства, та відповідно конкретнішого розуміння, сприйняття і застосування суддями в нормозастосовчій практиці.

SUMMARY

This Analysis represents the first attempt to conduct a systemic research and analysis of judicial practice in the field of personal data protection. It offers a general overview of the principal aspects and key trends in how Ukrainian courts of general jurisdiction apply the Law of Ukraine *On Personal Data Protection*.

The research focuses on the analysis of court decisions at different levels in civil, criminal, economic, and administrative cases as well as misdemeanor cases. The scale of the research made choosing the analysis methodology and consolidating the findings more difficult, however, it helped demonstrate the comprehensiveness of the application of the personal data protection legislation in different fields of law.

For the purposes of the research, the experts examined nearly 10,000 court decisions. More than 500 of those were picked for more in-depth examination, some of which are directly referenced in the text of the Analysis. All the decisions were selected from the Integrated State Register of Court Decisions using various criteria and search methods.

With that said, the chosen scope of the research informed the particular structure of the Analysis where the material is structured based on the principles applicable in the field of personal data protection.

Building on the previous research conducted with the support from the Council of Europe,[185] the authors of the Analysis have catalogued the principles of personal data protection including lawfulness, purpose limitation, proportionality, data accuracy, and accountability.

It was also taken into account that the elements of the personal data protection legislation (such as the grounds for processing of personal data and the rights of personal data subjects) are, in fact, a logical extension of those principles, build upon and detail them, and should be interpreted in the light of those principles[186].

Another reason to highlight and dissect the principles of personal data protection more in depth is their underpinning importance for the application of the law in general and judicial practice in particular. Less than perfect legal regulation, collisions and lacunas, as well as the need to *'go beyond'* the law to ensure protection of human rights may only be effectively addressed through legal principles.

In view of the above, the Analysis provides information and direction to judges which should ensure more in-depth and correct application of the personal data protection legislation.

The Analysis also seeks to have a positive impact on the enforcement of the constitutional right to privacy by increasing the legal awareness of individuals about the possibilities of judicial protection of personal data.

Based on the findings of the research, the following main trends and aspects were identified in the analysis of judicial practice:

185. See *Handbook on European Data Protection Law*. URL: https://rm.coe.int/16805966a8

186. Захист персональних даних: правове регулювання та практичні аспекти. Науково-практичний посібник/ М. Бем та І Городиський/ Рада Європи, 2021 [*Personal Data Protection. Legal Regulation and Practical Aspects. A Theoretical and Practical Manual* / By Markiyan Bem and Ivan Horodysky / Council of Europe, 2021]. - P. 44. URL: https://rm.coe.int/handbook-pers-data-protect-2021-web/1680a37a69

The provisions laid down by the Law of Ukraine *On Personal Data Protection* need to be clarified and elaborated, as well as brought into line with complementary laws that govern complementary legal relations. This is confirmed by how differently courts tend to interpret them and the fact that the same legal relations (procedures) are regulated by different conflicting provisions (for instance, mixing up the legal status of public information and personal data across different cases[187]).

Also, some collisions, such as between the legislation on the operation of public registers (information systems, databases, etc.), the right to personal data protection, and the right to freedom of religion (free exercise of religious beliefs) were addressed[188] while also acknowledging that the legal problem could not be solved without making amendments to the legislation. It is worth mentioning that the Supreme Court has been making efforts to ensure uniform application of legal provisions by courts by reviewing decisions of trial and appellate courts and formulating legal opinions that had a positive impact on consistency and uniformity of judicial practice. There have been many instances where courts applied the same approach and reasoning as the Supreme Court did in the case # 750/6287/17[189]. This is a clear example of how the Supreme Court's reasoning can be a reference point and a basis for structuring judicial practice in particular fields.

The international standards of personal data protection are quite widely applied in judicial practice. Sometimes, however, when providing the reasoning for their decisions, judges apply the international standards of personal data protection fairly nominally[190] (namely referring to international instruments that are irrelevant to Ukraine or merely quoting the ECtHR case law without proper analysis of the subject matter). That said, to support their reasoning, normally, courts fairly often choose to quote the texts of laws[191] instead of applying them directly. This makes it difficult to understand the court's logic underlying the findings reflected in the operative part of the decision.

Therefore, it is crucial that the reasoning and rationale of court decisions are brought to a higher level to ensure that they are clearly reflected when substantive provisions of the personal data protection legislation are applied, with reference to any relevant international standards.

Similarly, when hearing criminal cases involving personal data, courts examine relevant materials mainly from the criminal law perspective without engaging in analysis of the personal data protection legislation, only making slight references to personal data that were illegally collected, processed, or distributed[192]. It would thus be advisable to work on enhancing the knowledge and skills of judges in terms of the reasoning of court judgments in criminal cases with regard to personal data protection.

---

187. See, for instance, the Judgment of Frunze District Court of Kharkiv in the case # 645/545/17 of 29 September, 2017. URL: https://reyestr.court.gov.ua/Review/69339299; The Ruling of Kharkiv Oblast Appellate Court in the case # 645/545/17 of 12 April, 2018. https://reyestr.court.gov.ua/Review/73528431; Pursuant to the Ruling of the Supreme Court in the case # 645/545/17 of 12 April, 2020. URL: https://reyestr.court.gov.ua/Review/91134733#
188. See, for instance, the Ruling of the 6th Appellate Administrative Court in the case # 580/1751/19 of 12 December, 2019. https://reyestr.court.gov.ua/Review/86425640; the Judgment of the Supreme Court in the case # 806/3265/17 of 26 March, 2018. https://reyestr.court.gov.ua/Review/73139306
189. See, for instance, the Judgment of Lviv District Administrative Court in the case # 380/11843/20 of 17 February, 2021. https://reyestr.court.gov.ua/Review/94966560; the Judgment of Kharkiv District Administrative Court in the case # 520/8073/21 of 14 July, 2021. https://reyestr.court.gov.ua/Review/98335992; the Judgment of Donetsk District Administrative Court in the case # 200/12018/21 of 18 October, 2021. https://reyestr.court.gov.ua/Review/100400945 та ін.
190. See, for instance, the Judgment of Shevchenko District Court of Kyiv in the case # 761/44774/17 of 23 January, 2019. https://reyestr.court.gov.ua/Review/79881631; the Ruling of the Supreme Court in the case # 760/8719/17 of 04 December, 2019. https://reyestr.court.gov.ua/Review/86162369
191. See, for instance, the Judgment of Kyiv Economic Court in the case # 910/15262/19 of 17 December, 2019. URL: https://reyestr.court.gov.ua/Review/86568737; The Ruling of the Supreme Court in the case # 579/806/19 of 21 April, 2021. URL: https://reyestr.court.gov.ua/Review/96501519
192. See, for instance, the Verdict of Dunaivtsi District Court of Khmelnytsky Oblast in the case # 674/1782/19 of 13 December, 2019. https://reyestr.court.gov.ua/Review/86357578; the Verdict of Avtozavodsky District Court of Kremenchuk, Poltava Oblast, in the case # 524/8202/20 of 14 January, 2021. https://reyestr.court.gov.ua/Review/94131910; the Verdict of Kamyanets-Podilsky City/District Cort of Khmelnytsky Oblast in the case # 676/1984/21 of 21 April, 2021. https://reyestr.court.gov.ua/Review/96443215 etc.

Of great relevance is the issue of misapprehension of the provisions of the personal data protection legislation by individuals who take their cases to court as well as public authorities[193], including courts. Misapprehension and misinterpretation of the scope and notion of the *'consent to the processing of personal data'* (seeing it as *'absolute consent'*) make realization of other human rights, such as the right to social security including subsidies, benefits, payments etc., substantially more difficult if not impossible.

In addition to misapprehension of the personal data protection legislation, cases of deliberate abuse of the right to personal data protection are not uncommon which merits particular attention from the legislators. For instance, claimants may try to seek to invalidate civil-law contracts[194] (such as disadvantageous loan agreements) by manipulating the purpose and methods of personal data protection, particularly by appealing decisions to grant/not grant consent to personal data protection. There have also been similar instances of abuse of the right to personal data protection when appealing orders[195] of investigating judges granting temporary access to items and documents.

The need to reform the government's controls over compliance with the personal data protection legislation is vividly illustrated by judicial practice in misdemeanor cases. The actual number of misdemeanor charges is relatively small and those mainly involve minor misdemeanors (such as online publishing of documents that contain personal data). On the contrary, courts very often dismiss cases for lack of evidence or elements of a misdemeanor, or due to the expiration of the statute of limitations period for misdemeanors, or send cases back to the reporting officers requesting corrections to the reports.

The trends identified and outlined in the Analysis show the fairly high awareness of judges about the principles underlying the personal data protection legislation. With that said, some aspects need to be legislated in more detail and, accordingly, understood more specifically, accepted, and applied by judges in their law-enforcement practice.

193. See, for instance, the Judgment of Sumy District Administrative Court in the case # 480/3526/19 of 05 November, 2019. https://reyestr.court.gov.ua/Review/85396099; the Ruling of Dubno City/District court of Rivne Oblast in the case # 559/451/14-a of 26 February, 2014. https://reyestr.court.gov.ua/Review/37336087; the Ruling of Ratne District Court of Volyn Oblast in the case # 166/1494/15-a of 14 December, 2015. https://reyestr.court.gov.ua/Review/54446035; the Ruling of Vinnytsia City Court of Vinnytsia Oblast in the case # 127/14353/15-a of 27 August, 2015. https://reyestr.court.gov.ua/Review/49397907; the Ruling of Znamyanka City/District Court of Kirovohrad Oblast in the case # 389/2267/17 of 22 November, 2017. https://reyestr.court.gov.ua/Review/70722428; the Ruling of Volodymyr-Volynsky City Court of Volyn Oblast in the case # 154/364/17 of 27 February, 2017. https://reyestr.court.gov.ua/Review/64983331; the Judgment of Desna District Court of Chernihiv in the case # 750/5535/17 of 04 October, 2017. https://reyestr.court.gov.ua/Review/69305331 etc.
194. See, for instance, the Judgment of Monastyryshche District Court of Cherkasy Oblast in the case # 702/279/21 of 31 May, 2021. https://reyestr.court.gov.ua/Review/97261860; the Judgment of Novozavodsky District Court of Chernihiv in the case # 748/1374/20 of 01 October, 2020. https://reyestr.court.gov.ua/Review/92062236
195. See, for instance, the Order of the Investigating Judge of Pechersk District Court of Kyiv in the case # 757/55253/19-к of 04 November, 2019. https://reyestr.court.gov.ua/Review/85923862; The Order of the Judicial Panel of Frunze District Court of Kharkiv in the case # 645/2359/19 of 21 October, 2021. https://reyestr.court.gov.ua/Review/100631568

Володимир ВЕНГЕР – кандидат юридичних наук, доцент кафедри загальнотеоретичного правознавства та публічного права, виконавчий директор Центру дослідження верховенства права Національного університету «Києво-Могилянська академія». З 2017 року залучений до низки проєктів Ради Європи та Європейської комісії за демократію через право (Венеційська комісія) у сфері верховенства права, захисту прав людини, конституційних засад діяльності органів публічної влади та функціонування демократичних інститутів. В рамках Спільного проєкту Європейського Союзу та Ради Європи «Європейський Союз та Рада Європи працюють разом задля посилення операційної спроможності Омбудсмана у захисті прав людини» готував спеціальний правовий аналіз «Основні моделі інституалізації державного контролю у сфері персональних даних та доступу до публічної інформації в Україні».

Андрій КОШМАН – юрист із більш ніж десятирічним досвідом роботи в сфері публічної адміністрації, в тому числі у органах законодавчої, виконавчої, судової влади. Наразі працює юридичним радником (національним експертом) проектів Ради Європи, Європейського союзу, Програми розвитку ООН в Україні, а також займається науковою та дослідницькою діяльністю в Центрі дослідження верховенства права Національного університету «Києво-Могилянська академія».

Олександр Шевчук – кандидат юридичних наук. У 2019–2020 роках обіймав посаду національного експерта з електронного правосуддя за напрямком удосконалення захисту персональних даних у рамках проекту ЄС «Право-Justice». Наразі є національним консультантом у сфері захисту персональних даних у рамках спільного проекту ЄС та Ради Європи з посилення спроможностей Омбудсмана для захисту прав людини. У 2019–2021 роках брав участь у підготовці реформи системи захисту персональних даних в Україні. Олександр Шевчук є одним з авторів проекту Закону «Про захист персональних даних» (реєстраційний №5628 від 7 червня 2021 р.).

UKR

Рада Європи є провідною організацією із захисту прав людини на континенті. Вона нараховує 47 держав-членів, включно з усіма державами – членами Європейського Союзу. Усі держави – члени Ради Європи приєдналися до Європейської конвенції з прав людини – договору, спрямованого на захист прав людини, демократії та верховенства права. Європейський суд з прав людини здійснює нагляд за виконанням Конвенції у державах-членах.

www.coe.int

Держави – учасниці Європейського Союзу вирішили поєднати свої ноу-хау, ресурси та долі. Разом вони збудували зону стабільності, демократії та сталого розвитку, зберігаючи при цьому культурне розмаїття, толерантність та громадянські свободи. Європейський Союз прагне поділитися своїми досягненнями та цінностями з країнами та народами за його межами.

www.europa.eu

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE