ПРЯМУЄМО РАЗОМ

МІЖНАРОДНИЙ ФОНД ВІДРОДЖЕННЯ

УКРАЇНСЬКА ГЕЛЬСІНСЬКА СПІЛКА З ПРАВ ЛЮДИНИ

АНАЛІЗ ПРОЄКТУ

Закону України «Про захист персональних даних»

#5628

Європейський Союз складається з 28 держав-членів та їхніх народів. Це унікальне політичне та економічне партнерство, засноване на цінностях поваги до людської гідності, свободи, рівності, верховенства права і прав людини. Понад п'ятдесят років знадобилось для створення зони миру, демократії, стабільності і процвітання на нашому континенті. Водночас нам вдалось зберегти культурне розмаїття, толерантність і свободу особистості. ЄС налаштований поділитись своїми цінностями та досягненнями з країнами-сусідами ЄС, їхніми народами, та з народами з-поза їхніх меж.

Міжнародний фонд «Відродження» – одна з найбільших благодійних фундацій в Україні, що з 1990-го року допомагає розвивати в Україні відкрите суспільство на основі демократичних цінностей. За час своєї діяльності Фонд підтримав близько 20 тисяч проектів, до реалізації яких долучилися понад 60 тисяч активістів та організацій України на суму понад 200 мільйонів доларів США.

Сайт: www.irf.ua
Facebook: www.fb.com/irf.ukraine

ПРЯМУЄМО РАЗОМ

МІЖНАРОДНИЙ ФОНД ВІДРОДЖЕННЯ

УКРАЇНСЬКА ГЕЛЬСІНСЬКА СПІЛКА З ПРАВ ЛЮДИНИ

Матеріал підготовлено за підтримки Європейського Союзу та Міжнародного Фонду «Відродження» в рамках спільної ініціативи «EU4USociety». Матеріал відображає позицію авторів і не обов'язково відображає позицію Міжнародного фонду «Відродження» та Європейського Союзу».

АНАЛІЗ ПРОЄКТУ ЗАКОНУ УКРАЇНИ “ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ” #5628

Зміст

ОГЛЯД ЧИННОГО ЗАКОНОДАВСТВА ЩОДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В УКРАЇНІ

1-го червня 2010-го року Верховною Радою України був прийнятий законопроєкт “Про захист персональних даних” №2297-VI. Законопроєкт запроваджував, серед іншого, поняття “суб’єкт персональних даних”, “володілець персональних даних”, “розпорядник персональних даних”, “картотека”, “згода суб’єкта персональних даних”. Під суб’єктом персональних даних в законі розуміється фізична особа, персональні дані якої обробляються, під володільцем персональних даних — фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, під розпорядником персональних даних — фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця. [1, ст. 1]

Закон України “Про захист персональних даних” 2010-го року критикувався правозахисниками як до [5], так після набрання ним чинності [6]. Перша редакція закону передбачала для володільців баз персональних даних необхідність реєструвати ці бази у спеціально уповноваженому державному органі; використання персональних даних в історичних, статистичних чи наукових цілях, відповідно до закону, могло здійснюватися лише в знеособленому вигляді. У подальшому до закону були внесені зміни: ці норми були виключені. Норма про обов’язкову реєстрацію баз персональних даних устигла навести чимало клопоту, адже під неї підпадало найширше коло суб’єктів, які зрештою “заспамили” Державну службу України з питань захисту персональних даних заявками на реєстрацію баз даних. У 2014-му році ця служба була ліквідована.

Чинна нині редакція закону 2297-VI закріплює для суб’єкта персональних даних право на доступ до своїх

персональних даних, право знати умови надання доступу до його персональних даних, пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних, відкликати згоду на обробку персональних даних, право дізнатися впродовж 30-ти днів, чи обробляються його персональні дані, та зміст таких даних. [1, ст. 8]

Закон передбачає 6 підстав для обробки персональних даних: згода суб'єкта персональних даних на таку обробку; дозвіл на обробку, наданий володільцю відповідно до закону для здійснення його повноважень; укладення та виконання правочину чи для здійснення заходів, що передують укладенню правочину; захист життєво важливих інтересів суб'єкта персональних даних; необхідність виконання законного обов'язку володільця персональних даних; необхідність захисту законних інтересів володільця або третьої особи, якій передаються персональні дані. [1, ст. 11]

Контрольна функція покладається на Уповноваженого Верховної Ради України з прав людини. Зокрема, Уповноважений наділений повноваженням розглядати скарги та пропозиції щодо захисту персональних даних, приймати на їх підставі рішення, проводити планові та позапланові перевірки володільців або розпорядників персональних даних, видавати обов'язкові до виконання приписи, отримувати інформацію від розпорядників персональних даних, складати протоколи про притягнення до адміністративної відповідальності. Такий механізм контролю не можна назвати дієвим: офіс Уповноваженого, окрім обов'язків із захисту персональних даних, має безліч інших функцій, зокрема контроль за дотриманням вимог законів Про доступ до публічної інформації та Про звернення громадян — Офіс Омбудсмана розглядає скарги на порушення строків розгляду звернень та запитів, ненадання відповідей; складає протоколи про адміністративні правопорушення у зв'язку з невиконанням норм цих двох законів. Усе це вимагає значних ресурсів, і при обмеженому штаті Офісу Уповноваженого призво-

дить до того, що механізм захисту права на приватність належним чином не реалізований.

Закон критикують за брак визначеності, деталізації норм і процедур, відсутність ефективного механізму захисту права на приватність. Хоча закон і закріплює деякі права суб'єкта персональних даних, він не пояснює, як саме ці права можна реалізувати, і які санкції передбачені за порушення цих прав.

Закон також не відповідає оновленій у 2018-му році Конвенції Ради Європи 108, зокрема, щодо вимоги, щоб персональні дані оброблялися на підставі вільної, конкретизованої, поінформованої й однозначної згоди. [4, ст. 5 ч. 2] У законі немає винятків для обробки інформації в наукових та архівних цілях (які також передбачені Конвенцією 108).

Усталеною європейською практикою є поділ персональних даних на дані загального характеру та чутливі (sensitive) персональні дані — дані про расове або етнічне походження, релігійні переконання, здоров'я, сексуальне життя, генетику, біометричні дані, дані про кримінальні переслідування тощо. До таких персональних даних вимоги щодо обробки та зберігання є більш суворими — такими, що зокрема гарантуватимуть, що обробка персональних даних не призводитиме до дискримінації.

Нарешті, у законі Про захист персональних даних відсутнє визначення, що таке "захист персональних даних", визначення персональних даних неконкретизоване — відсутній хоч який перелік персональних даних.

ЗАКОНОДАВСТВО ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ У ЄВРОПЕЙСЬКОМУ СОЮЗІ ТА СПОЛУЧЕНИХ ШТАТАХ

General Data Protection Regulation (Загальний регламент про захист даних, далі GDPR) Європейського Союзу, який набув чинності 24-го травня 2016-го року, — замінив Data Protection Directive 1995-го року. Він застосовується на території країн — членів ЄС безпосередньо. Регламент упровадив підхід "захист даних за призначенням і за замовчуванням" (data protection by design and by default), згідно з яким контролер (тобто той, хто визначає цілі обробки даних) повинен упроваджувати технічні та організаційні заходи, які б забезпечували захист даних.

GDPR встановлює вимоги щодо отримання згоди на обробку даних (зокрема, текст згоди має бути сформульований зрозумілою мовою, має конкретно вказуватися ціль обробки); право на інформацію про обробку; право на доступ до даних; право на виправлення (right to rectification); право на обмеження обробки; право на заперечення проти обробки (right to object); право на захист від "автоматизованого прийняття рішень"; право знати про витоки даних (data breaches)

Право на забуття (right to be forgotten), представлене в проєкті GDPR, було замінене більш м'яким правом на стирання (right to erasure), яке дозволяє суб'єкту даних вимагати від контролера видалення своїх даних за певних обставин.

Контролери, які широкомасштабно обробляють чутливі дані, а також державні органи, — зобов'язані призначати посадову особу із захисту даних (data protection officer).

За невиконання вимог GDPR контролери та оператори можуть бути оштрафовані на суму до €20 млн або до 4% річного обороту.

У Сполучених Штатах Америки не існує федерального кодифікованого акта, який би регламентував захист персональних даних.

Прийнятий у 1974-му році US Privacy Act був покликаний захищати дані громадян від порушень із боку держави. Він встановлював для громадян право знати інформацію, якою володіють державні установи, а також отримувати копію цих даних; право на виправлення помилок. Державні установи мають обробляти дані згідно з принципом мінімізації даних.

У 1996-му році було ухвалено Health Insurance Portability and Accountability Act (HIPAA), який захищає медичні дані. HIPAA дозволяє обробляти медичну інформацію медустановам, якщо вона стосується лікування, оплати або заходів із охорони здоров'я. Для обробки даних у рекламних цілях вимагається "явна згода". Також HIPAA регламентує правила поводження з даними (необхідність запобігати "недоречному і непотрібному" доступу до даних тощо).

Існує також закон, який захищає дані дітей (COPPA) та закон, що, зокрема, регламентує обробку даних у фінансовій і банківській сферах (GLBA).

Приватність в інтернеті не регулюється, однак Федеральна торгова комісія (FTC) наділена повноваженнями протидіяти "нечесним практикам" із боку компаній. У 2011-му році FTC оштрафувала Facebook за оманливе сповіщення своїх користувачів про те, що їхні дані в соцмережі не розповсюджуються іншим. [7]

Чимось схожим на європейський акт є California Consumer Privacy Act (CCPA) від 2018-го року. Персональні дані за CCPA — це "інформація, що ідентифікує, стосується, або може розумно бути пов'язана, прямо чи непрямо, з окремим користувачем чи домогосподарством".

CCPA дає каліфорнійцям право знати про обробку даних, які їхні дані обробляються та як саме вони обробляються; право вимагати не продавати їхні дані (right to opt out); право на видалення (з багатьма винятками). CCPA забороняє дискримінувати споживачів за здійснення цих прав.

На відміну від GDPR, CCPA не передбачає права на стирання чи на забуття, а сфера його дії розповсюджується лише на крупний бізнес (із річним доходом понад $25 млн або той, який отримує більше половини виручки за рахунок продажу персональних даних) і не стосується, наприклад, державних структур та неурядових організацій. Також CCPA дозволяє вебсайтам збирати дані користувачів без окремої згоди.

Штрафи, передбачені CCPA — до $2 500 за кожне неумисне та до $7 500 за кожне умисне порушення.

У деяких штатах прийняті або розробляються подібні до CCPA акти з більш або менш суворими вимогами до контролерів.

ЗАКОНОПРОЄКТ #5628

Проєкт Закону України “Про захист персональних даних” №5628 було зареєстровано у Верховній Раді 7-го червня 2021-го року. Цей проєкт є значно об’ємнішим за чинний закон про захист, містить більше визначень, більш детально визначає процедури тощо. Багато норм перегукуються або й по суті копіюють такі ж норми у GDPR Європейського Союзу.

Замість зв’язки “суб’єкт-володілець-розпорядник” новий проєкт пропонує терміни “суб’єкт-оператор-контролер”, що відповідає європейській та загальновизнаній практиці. Крім цього, у законопроєкті визначено терміни “одержувач” — будь-яка фізична чи юридична особа, суб’єкт владних повноважень чи будь-який інший орган, якому надаються (розкриваються) персональні дані; “третя особа” — фізична або юридична особа, за винятком суб’єкта персональних даних, контролера, оператора, а також інших осіб, які уповноважені обробляти персональні дані під безпосереднім керівництвом такого контролера або оператора.

Як і чинний нині закон, проєкт №5628 передбачає 6 законних підстав для обробки персональних даних: згода суб’єкта (причому, на відміну від діючого закону, згода надається “для однієї або кількох точно визначених цілей”); укладення правочину; необхідність виконання юридичного обов’язку контролера персональних даних; необхідність виконання завдань в суспільних інтересах або повноважень, покладених на контролера законом; необхідність обробки персональних даних для цілей легітимного інтересу контролера або третьої особи, крім випадків, коли такі інтереси не переважають інтереси або основоположні права та свободи суб’єкта персональних даних, які вимагають захисту персональних даних, особливо якщо суб’єктом персональних даних є дитина.

Автори проєкту вирішили деталізувати поняття згоди на обробку персональних даних. У статті 6 перелічуються можливі способи надання згоди. Згоду можна надавати, зокрема, "шляхом обрання відповідних технічних налаштувань в інтерфейсі веб-сайта, операційній системі, програмному забезпеченні, чи мобільному додатку", а також конклюдентно — "через іншу ствердну дію чи поведінку, яка однозначно вказує на те, що суб'єкт персональних даних в конкретному випадку згоден на подальшу обробку його персональних даних". Причому заводські налаштування інтерфейсу, зокрема попередньо проставлена позначка про згоду, — не можуть вважатися наданням згоди.

Згода не вважається добровільною, якщо суб'єкт перебуває у залежному чи підпорядкованому становищі відносно контролера, якщо в суб'єкта немає можливості відмовити в наданні згоди або відкликати раніше надану, а також якщо в нього відсутні альтернативні шляхи доступу до товарів чи послуг без надання згоди, а також якщо згода "не передбачає окремого дозволу суб'єкта персональних даних на окремі види обробки персональних даних, незважаючи на те, що такий дозвіл є необхідним за індивідуальних обставин".

Частина 4 статті 6 забороняє відмовляти суб'єкту персональних даних у наданні товарів, робіт чи послуг на підставі відмови суб'єкта від надання згоди. Така заборона є досить ультимативною, і в ситуаціях, коли надання певних товарів чи послуг безпосередньо пов'язане з обробкою персональних даних (наприклад, переліт пасажирським рейсом, виготовлення документів), може спричиняти непорозуміння. Частину 4 варто сформулювати менш категорично, установивши конкретні винятки із загальної заборони.

ОБРОБКА ЧУТЛИВОЇ ІНФОРМАЦІЇ

Законопроєкт забороняє обробку персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в професійних спілках, а також генетичних та біометричних даних, даних, що стосуються здоров'я, статевого життя або сексуальної орієнтації, психометричних даних. Однак, перелічується 11 випадків, коли ця заборона може не застосовуватись, зокрема: коли суб'єкт надає явну згоду на обробку таких даних; обробка необхідна для здійснення прав та виконання обов'язків контролера або суб'єкта персональних даних у сфері трудових правовідносин або соціального захисту у випадках, передбачених законом, для захисту життєво важливих інтересів суб'єкта, для здійснення судом його повноважень та інші. [2, ст. 7]

Згадана інформація може оброблятися, якщо вона є "необхідною в цілях значного суспільного інтересу у випадках, передбачених законом, за умови, що такий закон є пропорційним відносно цілі, яка переслідується, враховує принцип поваги до суті права на захист персональних даних та передбачає належні та відповідні засоби захисту основоположних прав та інтересів суб'єкта персональних даних" [2, ст. 7 ч. 2 п. 7]. Водночас, іще одна підстава для обробки таких персональних даних в законопроєкті виглядає так: якщо обробка "необхідна в цілях суспільного інтересу в сфері громадського здоров'я, такого як захист від серйозних транскордонних загроз для здоров'я або забезпечення високих стандартів якості та безпеки послуг з охорони здоров'я та медичних продуктів або медичного устаткування у випадках, передбачених законом, який передбачає належні і відповідні засоби захисту основоположних прав та свобод суб'єкта персональних даних, зокрема, професійної таємниці". Хоча міркування, якими керувалися автори законопроєкту, є доволі зрозумілими, все ж виникає сумнів у необхідності окремо виділяти "суспільний інтерес у сфері

громадського здоров'я" [2, ст. 7 ч. 2 п. 9]. По суті, цей випадок незастосування заборони охоплюється випадком із пункту 7 про значний суспільний інтерес.

Крім цього, положення про заборону обробки перелічених чутливих даних не застосовується, якщо обробка "необхідна в цілях попередження, розслідування, виявлення правопорушень або виконання кримінальних покарань або покарань за адміністративні правопорушення, у випадках визначених законом, який має передбачати належні гарантії захисту прав та інтересів суб'єкта персональних даних".

Невже дані про етнічне походження, політичні переконання чи сексуальну орієнтацію можуть бути необхідними для проведення розслідувань правоохоронними органами або для виконання покарань співробітникам пенітенціарної системи? Обробка біометричних даних (відбитків пальців, скажімо) може дійсно бути корисною для пошуку злочинців, але прирівнювання її за рівнем необхідності до обробки даних про політичні переконання виглядає сумнівним.

Збирання та зберігання інформації стосовно приватного життя особи, а також її розповсюдження охоплюються сферою застосування пункту 1 статті 8 Європейської конвенції з прав людини. ЄСПЛ наголошував не необхідності, зокрема, належного контролю за збором інформації правоохоронними органами. Так, у справі Заїченко проти України визнано порушення статті 8, зокрема, через опитування міліцією сусідів заявника про стан його психічного здоров'я.

Обробка біометричних даних суб'єктами владних повноважень у законопроєкті вважається правомірною, якщо здійснюється для цілей, зокрема, "економічного добробуту". [2, ст. 9 ч. 2 п. 1] Поняття "економічний добробут" уживається в проєкті кілька разів, а "економічні та фінансові інтереси" згадуються у статті 4. Слід зазначи-

ти, що автори проєкти прагнуть інтегрувати в нього так званий трискладовий тест, який застосовується Європейським судом для визначення прийнятності обмежень конкретних прав, гарантованих Європейською конвенцією (у цьому випадку йдеться про право на приватність, гарантоване статтею 8 ЄКПЛ). Втручання у здійснення права визнається допустимим, якщо воно здійснюється відповідно до закону, є пропорційним до згаданої в статті 8 мети втручання та необхідним у демократичному суспільстві. Проте, Європейською конвенцією визначаються виключні переліки легітимних цілей (наприклад, для обмеження свобод, передбачених статтею 10, є 12 легітимних цілей).

У п. 5 ч. 1 ст. 4 законопроєкту Про захист персональних даних, у якому йдеться про принцип зберігання даних, зазначено: "дані повинні зберігатись у формі, що дозволяє ідентифікацію суб'єкта персональних даних не довше, ніж це необхідно для цілей, в яких вони обробляються, крім випадків, встановлених законом, за умови дотримання сукупності наступних критеріїв: випадки мають бути встановлені законом; становити необхідні та пропорційні заходи у демократичному суспільстві для забезпечення захисту конкретних цінностей, зокрема забезпечення громадської безпеки, важливих суспільних, економічних або фінансових інтересів); забезпечувати дотримання прав і свобод суб'єкта персональних даних". Якщо порівняти це з формулюванням, викладеним у ч. 2 ст. 8 Європейської конвенції, можна помітити деякі розбіжності. У конвенції не згадуються "цінності", а в українському законопроєкті вони є, причому прикметник "конкретний" відносно цінностей вживається разом із прислівником "зокрема": незрозуміло, як це може не викликати логічну суперечність, адже якщо йдеться про захист "конкретних цінностей", вони мають бути визначені чітким вичерпним переліком, а прислівник "зокрема" вказує на те, що, крім перелічених, існують іще якісь цінності, заради захисту яких може порушуватися загальне правило про недопустимість зберігання даних

довше, ніж потрібно для цілей їхньої обробки. У Конвенції є "інтерес економічного добробуту країни", але не "економічні та фінансові інтереси".

Такий викривлений, порівняно з нормами ЄКПЛ, перелік легітимних цілей, який, до того ж, не можна однозначно трактувати як вичерпний, не сприятиме визначеності та може призвести до порушень права на приватність за відсутності легітимної мети, передбаченої Конвенцією, і, відповідно, скаргам до ЄСПЛ проти України.

ЗЙОМКА В ПУБЛІЧНИХ МІСЦЯХ

Стаття 11 законопроєкту говорить: “У разі здійснення аудіозапису, відеозйомки, кінозйомки, фотозйомки або будь-якої іншої фіксації зображення або голосу суб’єкта персональних даних, незалежно від технології що використовувалася, відкрито на вулиці або на заходах публічного характеру (публічних зборах, конференціях тощо), контролер зобов’язаний завчасно вжити достатніх заходів для повідомлення суб’єктів персональних даних про здійснення аудіозапису, відеозйомки, кінозйомки, фотозйомки або будь-якої іншої фіксації зображення або голосу суб’єкта персональних даних у спосіб, який надає можливість суб’єкту персональних даних заперечити проти обробки його персональних даних”.

Таке формулювання викликає чимало питань, якщо спробувати проєктувати його на реальне життя. Якщо вуличний фотограф буде щоразу попереджати кожен об’єкт своєї зйомки про те, що він фіксує його зображення, — це фактично знищує елемент спонтанності, без якого деякі світлини просто втрачають сенс. Якщо відеооператор має на меті зняти натовп людей на вулиці, як саме має виглядати “завчасне вжиття заходів про повідомлення суб’єктів персональних даних про здійснення відеозйомки” з наданням їм можливості заперечити проти цієї зйомки?

Європейський суд з прав людини у справі Friedl v. Austria визнав, що здійснення поліцією фотофіксації під час публічного заходу не було порушенням права на приватність заявника. Відповідно, межі здійснення права на приватність звужуються

ЖУРНАЛІСТСЬКА ТА ТВОРЧА ДІЯЛЬНІСТЬ

У статті 14 написано, що "контролер, який здійснює обробку персональних даних з метою наукового або історичного дослідження, може обмежити права суб'єкта персональних даних". Таке формулювання не вбачається доречним, оскільки можливістю обмежувати права в окремих випадках наділена виключно держава (щодо права на приватність у Європейській конвенції це сформульовано як можливість "втручатися у здійснення права", а не обмежувати, хоча по суті йдеться про одне й теж), а поняття "контролер" у законопроєкті може охоплювати як державні органи, так і значно ширше коло індивідів.

Стаття 15 передбачає, що ряд вимог законопроєкту щодо обробки даних не застосовуються, якщо обробка здійснюється "для цілей журналістської та творчої діяльності". Однак, що таке "журналістська діяльність" та які її цілі, ця стаття відповіді не дає. У частині 3 лише зазначається, що "для цілей цієї статті поняття журналістська діяльність підлягає тлумаченню з урахуванням практики Європейського суду з прав людини". Прагнення законодавця спиратися на практику Європейського суду тут не можна не вітати, але така невинна маршрутизація в бік Страсбурга може створити багато проблем у найближчому після імплементації законопроєкту майбутньому. Адже виходить, що кожен журналіст має знатися на практиці ЄСПЛ у цих питаннях, хоча варто зауважити, що далеко не всі судді в судах першої інстанції здатні цим похизуватися. Виходить, що журналістам доведеться звертатися за послугами кваліфікованих адвокатів, які розтлумачуватимуть їм закон та релевантну практику ЄСПЛ, що спричинить додатковий тягар на й без того ледь здатну себе прогодувати без сторонньої підтримки українську журналістику. І навіть це не дозволить журналістам ефективно захищатися в судах із уже названої причини. Щодо тлумачення поняття "творча діяльність" стаття 15 не говорить узагалі нічого.

Практика ЄСПЛ згадується і в іншій статті законопроєкту, у якій контролера зобов'язують враховувати практику ЄСПЛ при виконанні принципів обробки персональних даних, передбачених у законопроєкті. Очевидно, що ця норма працювати не буде, тому що кожен контролер (під визначення контролера в розумінні цього законопроєкту підпадає дуже широке коло суб'єктів) не в змозі володіти практикою ЄСПЛ, і безглуздо покладати на нього такий обов'язок. Щоб убезпечити себе від претензій з боку регулятора, контролери почнуть формально використовувати назви або фрагменти рішень Європейського суду — наприклад, у згодах на обробку. Практика ЄСПЛ за таких умов перетвориться на карго-культ (щось подібне вже є в судовій системі, коли суди подекуди готові посилатися на рішення ЄСПЛ ледь не на підставі лише наявності в ньому фрази, подібної до фрази в їхньому рішенні). Не має також упевненості, що дієслово "виконувати" доречно вживати щодо принципів. Можливо, доцільніше вжити більш традиційне "дотримуватися" або по-іншому перекласти слово "implement", яке вживається у GDPR. [3, ст. 25 ч. 1]

Щодо позиції самого Європейського суду щодо балансу між правом на приватність та професійною діяльністю журналістів, суд низкою послідовних рішень вивів розуміння, що десята стаття Конвенції гарантує, крім іншого, право збирати інформацію. У рішенні "Dammann v Switzerland" суд зазначив, що збір інформації був "ключовим підготовчим кроком до журналістики" і невід'ємною, захищеною частиною свободи преси.

Межі здійснення права на приватність звужуються по мірі того, як особа починає займатися публічною діяльністю. ЄСПЛ визнає, що журналісти можуть критикувати політиків та державних службовців, навіть у доволі різкій формі (справа Лінгенс проти Австрії).

Цікавою є також окрема думка судів Шайо і Вучініча у справі "'Молодіжна ініціатива з прав людини' проти

Сербії", у якій вони зазначають, що "у світі інтернету різниця між журналістами і іншими представниками громадськості швидко зникає. Без прозорості, якій повинні служити і яку повинні використовувати всі громадяни, не може бути здорової демократії" (справа стосувалася відмови неурядовій організації в отриманні статистичної інформації про прослуховування).

У справі Угорської Гельсінської спілки проти Угорщини ЄСПЛ зазначив, що хоча імена державних адвокатів і є персональними даними, їхня професійна діяльність не може вважатися такою, що носить приватний характер, і тому відомості про неї можуть бути розголошені.

ПРАВА СУБ'ЄКТА ПЕРСОНАЛЬНИХ ДАНИХ

Перелік інформації, яку контролер зобов'язаний повідомити суб'єкту персональних даних, наведений у статті 18, навіть більший, ніж у ст. 13 GDPR. Окрім того, що було перенесено в український законопроєкт із європейського регламенту, він також вимагає від контролера повідомляти "мету, цілі та способи обробки" (GDPR вимагає лише "purposes"); форму, зміст та порядок надання або відкликання згоди на обробку персональних даних; дії або сукупність дій, які будуть здійснюватися з персональними даними; здійснення обробки персональних даних для цілей прямого маркетингу і право відмовитися від неї.

Законопроєкт про захист відтворює норми GDPR про право суб'єкта на доступ до інформації про себе. Проєкт передбачає, що контролер завжди має надавати суб'єкту копію його персональних даних безоплатно, хоча GDPR дозволяє контролеру брати за це "розумну плату, що ґрунтується на адміністративних витратах". Проте, через брак коми в українському проєкті речення "суб'єкт персональних даних має право отримати копію своїх персональних даних, які обробляються контролером безоплатно" [2, ч. 2 ст. 19] по суті надає суб'єкту право отримати копію лише тих своїх персональних даних, за обробку яких контролер не отримує грошей, тобто дані "обробляються контролером безплатно".

Законопроєкт №5628, подібно GDPR, передбачає право на виправлення (right to rectification), право на забуття (right to be forgotten). Останнє сформульовано як право на "повне знищення контролером персональних даних без надмірної затримки".

Згідно з частиною другою статті 21, контролер зобов'язаний знищити персональні дані у строк не більше тридцяти днів, якщо, зокрема: відсутня необхідність подальшої обробки персональних даних для цілей, для яких вони збирались або оброблялись; суб'єкт персональних даних відкликав згоду або заперечує проти обробки. Крім того, контролер зо-

бов'язаний "вжити всіх достатніх заходів" для повідомлення інших контролерів, яким він передавав персональні дані, про вимогу знищення цих даних, крім випадків, коли таке повідомлення становить для контролера надмірний тягар.

Це доволі сувора вимога до контролера, яка потенційно створюватиме для нього серйозне навантаження.

Крім цього, законопроєкт вимагає від іноземних контролерів, які обробляють персональні дані громадян України, а також пропонують послуги суб'єктам персональних даних в Україні, призначати представника в Україні. Це означає, що не лише великі міжнародні компанії, але навіть іноземні інтернет-магазини будуть змушені призначити в Україні свого представника, якщо замовлення в них здійснить громадянин України. Таку вимогу просто неможливо буде виконати, тому це може призвести не лише до надмірних витрат для компаній, які працюють в Україні, але й до того, що санкції за її невиконання будуть застосовуватися лише до деяких "порушників", що створюватиме нерівність перед законом і загалом не сприятиме приходу іноземного бізнесу в Україну.

Законопроєкт вимагає від контролерів та операторів здійснювати реєстрацію операцій із обробки персональних даних, встановлюючи винятки для "суб'єктів мікропідприємництва, підприємств, організацій і установ незалежно від форми власності та організаційно-правової форми з чисельністю працівників менше ніж 10 осіб" [2, ст. 34]. Варто зазначити, що європейський регламент не вимагає здійснювати реєстрацію від підприємств чи організацій із чисельністю працівників менше 250-ти (але вони все ж повинні здійснювати реєстрацію, якщо обробка персональних даних може порушувати права та основоположні свободи суб'єктів персональних даних, якщо обробка є систематичною, або якщо обробляються спеціальні категорії "чутливих даних"; ці винятки відтворює і український проєкт).

ПЕРСОНАЛЬНІ ДАНІ, ЯКІ ОБРОБЛЯЄ РОБОТОДАВЕЦЬ

Законопроєкт містить окремий розділ, присвячений питанням обробки персональних даних роботодавцем.

По-перше, у проєкті закону вживається термін "кандидат на працевлаштування", визначення якого не наведено ані в самому проєкті, ані в профільному чи іншому законодавстві. У статті 51 наводиться перелік "цілей трудових відносин": "Для цілей цього Закону під цілями трудових відносин розуміються відносини між роботодавцем та працівником та/або кандидатом на працевлаштування, які стосуються працевлаштування, виконання трудового договору, включаючи виконання обов'язків, передбачених законодавством, установчими документами, колективним договором, а також планування та ефективне управління органом державної влади та органом місцевого самоврядування, підприємством, установою або організацією та розірвання трудових відносин. До цілей трудових відносин також належать відносини, які мають місце після припинення трудових відносин". Таке визначення виглядає сумнівним із багатьох причин.

1) **Незрозуміло,** чому для визначення цього поняття обрали саме слово "ціль", адже ціллю у загальновизнаному значенні прийнято вважати те, до чого прагнуть, кінцеву мету. Із наведеного визначення випливає, що ціллю трудових правовідносин є самі трудові правовідносини, що доволі дивно.

2) **"Планування** та ефективне управління органом державної влади та органом місцевого самоврядування", — самі ці слова звучали б доречно на черговому з'їзді комуністичної партії, але із сучасним законом, який претен-

дує на статус такого, що імплементує європейські норми, — не в'яжуться зовсім. Взагалі незрозуміло, чого тут стосується слово "планування" (ніби як п'ятирічних держпланів уже давно немає, але "планування" просто лишається за старою звичкою). Якщо щодо органу державної влади слово "управління" ще якось застосувати можливо (але краще не варто), то хто взагалі має "управляти" органом місцевого самоврядування? Відповідно до Закону України "Про місцеве самоврядування", місцеве самоврядування в Україні — це гарантоване державою право та реальна здатність територіальної громади — жителів села чи добровільного об'єднання у сільську громаду жителів кількох сіл, селища, міста — самостійно або під відповідальність органів та посадових осіб місцевого самоврядування вирішувати питання місцевого значення в межах Конституції і законів України. Хочеться вірити, що ми живемо в державі, де немає нікого, хто мав би повноваження управляти жителями села чи міста, або їх добровільним об'єднанням. Причому в цій конструкції йдеться лише про "ефективне управління" — відповідно, на неефективне управління вона не поширюється.

3) **До цілей** (тобто до мети) трудових відносин відноситься розірвання трудових відносин та "відносини, які мають місце після припинення трудових відносин". Особливо цікавим є останнє формулювання, адже після припинення трудових відносин у будь-якого індивіда зазвичай протягом життя виникає багато інших відносин (відносини з продавцем у магазині, із касиром у банку, із членами родини), і всі вони охоплюються поняттям "цілі трудових відносин" за визначенням законопроєкту.

Частина 5 статті 51 визначає умови, за яких роботодавець може обробляти персональні дані в цілях, які не передбачені частиною четвертою цієї статті — проте четверта частина взагалі не містить ніяких цілей.

У частині 6 згаданої статті йдеться про те, що під час обробки персональних даних роботодавець повинен "враховувати можливий вплив на основоположні права та обов'язки суб'єктів, передбачених частиною другою цієї статті". Цікаво було б уявити документ, який би визначав чиїсь "основоположні обов'язки".

Частина 2 статті 52 зазначає, у яких випадках роботодавець може збирати персональні дані без згоди суб'єктів персональних даних від інших осіб чи джерел. Згода не вимагається, якщо "персональні дані збираються роботодавцем від органу державної влади для виконання ним своїх обов'язків, передбачених законодавством". Саме формулювання є невдалим, адже з нього майже нічого не зрозуміло, крім того, що автори проєкту хочуть із якоїсь причини зробити виняток із заборони обробки персональних даних без згоди суб'єкта цих даних для державних органів. В усякому разі — це сумнівне і потенційно небезпечне прагнення — адже чому державний орган має отримувати індульгенцію там, де її не передбачено ні для кого іншого?

Стаття 55, яка передбачає для працівника право отримати від роботодавця інформацію про обробку його персональних даних; подавати роботодавцю запит на отримання інформації щодо обробки його персональних даних; отримати дані про його оцінку роботодавцем, оскаржувати достовірність та/або повноту обставин, які було взято до уваги під час формування оцінки; на захист від прийняття рішень щодо його персональних даних на підставі автоматичної обробки.

ПЕРЕДАЧА ДАНИХ ЗА КОРДОН

Законопроєкт регламентує передавання персональних даних міжнародним організаціям та іноземним державам, цьому питанню присвячено розділ VI.

Такими, що забезпечують належний захист даних, вважаються держави та організації, на які поширюється дія Конвенції 108+ та GDPR. Щоб будь-які інші держави чи організації потрапили до цього "клубу", їх повинен внести до відповідного списку контролюючий орган. Виходить, що Сполучені Штати Америки або ООН мають бути спершу проаналізовані контролюючим органом за наведеними в законопроєкті критеріями, перш ніж туди можна буде вільно передавати персональні дані. Контролюючий орган також буде вести та оприлюднювати перелік держав та міжнародних організацій, які не забезпечують належний захист даних.

Не дуже зрозуміло, для чого потрібні ці реєстри, враховуючи, що передавати дані до держав чи організацій з останнього переліку все одно можна за певних обставин (надання належних гарантій, виконання правочину та інші). Можна було б залишити один із таких списків, і складати його лише щодо держав. Буде ніяково, якщо поважні міжнародні інституції (наприклад, ВОЗ або Червоний Хрест) не увійдуть до переліку "тих, що забезпечують належний захист даних", навіть якщо контролюючий орган просто забуде їх туди додати. Та й взагалі — те, що поки неіснуючий орган з невідомою структурою і повноваженнями буде піддавати оцінці спроможність ООН захищати персональні дані, виглядає не дуже добре. У Європі подібний перелік (адекватних юрисдикцій) складає Єврокомісія.

ПРАВА КОНТРОЛЮЮЧОГО ОРГАНУ

Широта прав контролюючого органу, визначених законопроєктом Про захист персональних даних, які надані йому ніби з метою захисту суб'єктів персональних даних, потенційно може призвести до зловживань із боку самого контролюючого органу. По суті, на контролюючий орган не розповсюджуються деякі гарантії забезпечення захисту персональних даних суб'єктів — тобто персональні дані можуть бути в деяких випадках захищені від усіх, крім контролюючого органу. Під приводом захисту персональних даних держава в особі контролюючого органу сама може стати найбільшим порушником права на приватність.

Наприклад, викликає занепокоєння стаття 36, у якій описується взаємодія контролера та контролюючого органу. У статті зазначається, що контролер, оператор чи їхній представник "зобов'язані забезпечувати доступ до приміщень, засобів, інформаційно телекомунікаційних систем, матеріалів і документів, у тому числі на засадах, визначених законодавчими актами щодо захисту інформації з обмеженим доступом". Виходить, що контролюючий орган матиме змогу навідуватися до приміщень, отримувати доступ до документів та інше — по суті будь-якої фізичної та юридичної особи, яка здійснює обробку чи визначає цілі обробки будь-якої інформації, що стосується фізичної особи, яку ідентифіковано або може бути ідентифіковано (окрім інформації для особистих та побутових потреб). Якщо скласти ланцюжок із цієї норми, визначень "контролера", "оператора" та "персональних даних", — виходить саме така конструкція. Із такими повноваженнями контролюючий орган, про який ідеться в законопроєкті, має бути однією з найпотужніших структур у державі, оскільки на його вимогу повинні відчинятися двері будь-якого бізнесу. І що означає "на засадах, визначених законодавчими актами щодо захисту інформації з обмеженим доступом"? Завуальований спосіб сказати про те, що контролюючий орган на його вимогу

має отримувати доступ і до конфіденційної інформації (яка відноситься до інформації з обмеженим доступом відповідно до ЗУ "Про інформацію" [10, ст. 21])?

Далі — ще більше.

Частина п'ята статті 64 говорить: "Постачальник електронних комунікаційних мереж та/або послуг зобов'язаний надати дані про місцезнаходження споживача та/або кінцевого користувача контролюючому органу на його вимогу з метою доведення дотримання вимог цього Закону". Щоб захистити персональні дані абонентів, держава буде збирати дані про їхнє розташування. Тут згадується орвелівське "свобода — це рабство". І хоча десятий розділ законопроєкту містить певні гарантії та вимоги щодо обробки даних правоохоронними органами, це ніяк не може виправдати такої "straightforward" заяви про те, що держава може вимагати в контролерів персональні дані, щоб нібито їх захистити. До того ж, незрозуміло, чи буде вважатися контролюючий орган правоохоронним за визначенням.

Стаття 65 розвиває тему про доступ до даних про місцезнаходження ще далі. У частині першій зазначено, що "Постачальник електронних комунікаційних мереж та/або послуг з метою захисту життєво важливих інтересів фізичної особи зобов'язаний надати уповноваженим органам або особам дані, необхідні для встановлення останнього місця знаходження мобільного кінцевого (термінального) обладнання" за умови, якщо надання таких даних є необхідним для "попередження смерті, дорожньо-транспортної пригоди або спричинення серйозної шкоди особі", "встановлення місця знаходження особи, яка визнана судом недієздатною, оголошена в розшук, хворіє на хворобу, яка може призвести до вчинення дій, що являють собою безпосередню небезпеку для неї чи оточуючих", а також для "встановлення місця знаходження малолітньої або неповнолітньої особи, яку за заявою батьків або опікунів чи піклувальників ого-

лошено в розшук". У частині 6 згаданої статті написано: "постачальник електронних комунікаційних мереж та/або послуг у відповідь на обґрунтований запит зобов'язаний надати дані настільки швидко, як тільки це технічно можливо. Відповідальність за дотримання законності при наданні даних несе постачальник електронних комунікаційних мереж та/або послуг".

У статті 65 слово "суд" уживається лише один раз — щодо особи, яка визнана судом недієздатною. Про те, що такі дані, як дані про місцезнаходження, мають розголошуватися виключно на підставі вмотивованого рішення суду — ані слова. Хоча в будь-якій правовій державі саме суд має надавати санкцію на витребування в операторів чи провайдерів персональних даних їхніх абонентів, адже суд є тим органом, який здатен забезпечити об'єктивний розгляд питання про необхідність втручання у конкретному випадку як у справи приватної компанії, так і у здійснення права на приватність її клієнтів. За відсутності незалежного органу контролю за діяльністю правоохоронних органів — вони не матимуть перешкод на шляху перетворення на правопорушні органи.

У статтях 66 і 67 ідеться про те, що абонент може подати запит до постачальника електронних комунікацій про відстеження "небажаних" або "зловмисних" викликів та отримати контактні дані того, хто їх здійснює, але немає визначень чи хоча б орієнтовних критеріїв віднесення викликів до "небажаних" чи "зловмисних". Узагалі видається сумнівним, що провайдер або оператор повинен по суті здійснювати стеження за своїм абонентом та розголошувати його дані на підставі скарги від іншого абонента, причому про кожну відмову в розголошенні він має обов'язок сповіщати контролюючий орган. Звичайно, провайдеру чи оператору здебільшого простіше просто "поділитися" даними, щоб уникнути зайвого клопоту. Але суттєво також те, що на постачальника електронних комунікацій тут покладається функція "судді", який має визначити, чи можна обмежувати право на приватність

одного абонента на користь захисту прав іншого. Якщо додати до цього те, що будь-які критерії, за якими провайдер міг би розрізняти "небажані" та "зловмисні" виклики, відсутні, — така норма закону майже гарантовано стане інструментом зловживань. Можна навіть уявити, як поліцейські в якості цивільних осіб будуть подавати оператору скарги на чиїсь "небажані виклики", щоб встановити його особу в обхід судової процедури.

САНКЦІЇ

Законопроєкт пропонує встановити відповідальність за порушення законодавства про захист персональних даних.

Стаття 72 у частині 1 встановлює відповідальність за порушення хоча б однієї з 26-ти статтей законопроєкту, які в ній наводяться. Якщо це порушення не призвело до порушення прав суб'єктів персональних даних, на контролерів та операторів пропонується накладати штраф у розмірі:

- **для фізичних осіб** — від 10 000 до 30 000 гривень;
- **для юридичних осіб** — від 0,05% до 0,1% загального річного обороту такої юридичної особи але не менше ніж 30 000 гривень за кожне окреме порушення.

Інші частини статті 72 встановлюють іще більш жорсткі штрафні санкції — аж до 300 000 ₴ для фізичних осіб та до 5% річного обороту для юридичних осіб.

Такі суворі санкції важко назвати співмірними порушенням, за які їх накладатимуть. Такі високі штрафи нелегко знайти навіть у Кримінальному кодексі, який передбачає відповідальність за діяння, які вважаються в суспільстві найбільш небезпечними. Наприклад, такі злочини проти приватності як порушення недоторканності житла та порушення таємниці листування караються штрафом до ста неоподатковуваних мінімумів доходів громадян (1700 ₴), хоч за них також передбачена відповідальність у виді обмеження та позбавлення волі на певний строк. [11, ст. 162-163]

Санкції можуть накладатися за порушення надзвичайно великої множини норм закону, які перелічуються в диспозиції лише посиланнями на номери статей або частин статей. Це робить дуже складним розуміння того,

за які саме діяння передбачена відповідальність: контролерам і операторам потрібно співставити відповідні статті із санкціями, передбаченими за їхнє порушення.

Варто звернути увагу і на те, що санкції можуть накладатися за порушення, наприклад, норм статті 4 законопроєкту, у якій перелічуються принципи; статті 11, яка регламентує зйомку в публічних місцях (відтак, журналіст або фотограф може отримати штраф до 30 000 ₴ за зйомку без згоди навіть якщо вона не призвела до порушення нічиїх прав); статті 20 щодо права на виправлення неточних даних (контролер може отримати штраф за зволікання з виправленням неточностей у персональних даних суб'єкта).

За відмову постачальника електронних комунікаційних мереж надати контролюючому органу дані про місцезнаходження своїх клієнтів передбачено штраф 100-300 тисяч гривень для фізичних осіб та 3-5% річного обороту для юридичних осіб.

У ч. 4 статті 65 зазначено: "порушення інших положень цього Закону, не зазначених у частинах першій — третій цієї статті, — тягне за собою збільшення розміру штрафу передбаченого частинами першою — третьою цієї статті Закону на тридцять відсотків". Тобто законодавець пропонує карати за порушення буквально будь-якої норми закону, причому зрозуміти, за які діяння можна отримати найсуворіше покарання — найскладніше, тому що потрібно методом виключення викреслювати норми, перелічені у трьох попередніх частинах статті 65. Незрозуміло також, збільшення якого саме штрафу мається на увазі (адже в кожній із трьох частин статті розміри штрафу різні).

Відповідальність стосується контролерів та операторів — відповідальність для контролюючого органу не передбачена.

Варто також зауважити, що структура українського законодавства передбачає, що юридична відповідальність за порушення регламентується окремими кодексами, тому санкції за порушення законодавства про захист персональних даних доцільно реалізувати шляхом доповнення Кодексу України про адміністративні правопорушення чи Кримінального кодексу України відповідними статтями.

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ ЩОДО ПОЛІПШЕННЯ ЗАКОНОПРОЄКТУ

Законопроєкт №5628 прагне привести законодавство України про захист персональних даних у відповідність до актів Ради Європи та Європейського Союзу, запроваджує нові підходи до обробки та зберігання даних, вводить поняття "чутливих даних" тощо.

Варто відзначити позитивні риси проєкту, такі як деталізація визначень та процедур, орієнтація на підходи Європейського суду з прав людини, запровадження принципу "захист персональних даних за проєктуванням і за замовчуванням". Права суб'єктів персональних даних та обов'язки контролера й оператора визначені доволі конкретно, добре регламентовано дії контролера у випадку витоків даних (data breach), деталізовано ознаки згоди, питання цілей обробки даних.

Водночас, законопроєкт містить низку недоліків, зокрема структурних.

Перш за все, у проєкті відсутній розділ чи хоча б окрема стаття, яка б регламентувала діяльність контролюючого органу. Водночас серйозне занепокоєння викликають деякі зобов'язання перед цим органом із боку контролерів та операторів (наприклад, надавати доступ до своїх приміщень на вимогу, надавати персональні дані про місцезнаходження абонентів). За відсутності реально діючого контролюючого органу всі широкі гарантії, які надає законопроєкт, просто не будуть працювати на практиці. Водночас, якщо чітко не визначити його компетенцію та повноваження, є серйозний ризик, що цей орган сам перетвориться на найбільшого порушника права на приватність. Із законопроєкту незрозуміло, який порядок обробки контролюючим органом персональних даних, які він отримуватиме для здійснення своїх функцій. Зрештою, про його функції також майже нічого не відомо.

Необхідно або присвятити частину законопроєкту регламентації роботи контролюючого органу, або паралельно підготувати окремий законопроєкт про цей орган.

У проєкті також немає детальної процедури передачі персональних даних між державними органами, що є важливим з огляду на обсяг персональних даних, якими володіють окремі державні структури.

Санкції, передбачені проєктом, є занадто жорсткими, а підстави для їх накладення — надто широкими та розмитими. Потрібно чітко визначити диспозицію, а розміри штрафів доцільно суттєво зменшити. Доцільно також відтермінувати набуття чинності закону в частині накладення санкцій.

До кінця незрозуміло, які вимоги законопроєкту стосуватимуться журналістської та творчої діяльності, немає визначень цих діяльностей. Норми про зйомку в публічних місцях є такими, що можуть стримувати діяльність журналістів, фотографів, операторів, художників тощо, і, відтак, призводити до обмеження свободи вираження. Абстрактне посилання на практику ЄСПЛ у визначенні журналістської діяльності доцільно замінити більш конкретизованими визначеннями.

У проєкті бракує визначеності деяких термінів (наприклад, немає визначень понять "автоматизована обробка персональних даних", "кандидат на працевлаштування"), окремі терміни вживаються по різному ("автоматизований" і "автоматичний", "місцезнаходження", "місце знаходження" та "розташування" тощо). Деякі принципи та норми базуються на спотворених положеннях Європейської конвенції з прав людини.

Хоча відносини щодо обробки персональних даних працівника роботодавцем описані загалом непогано, деякі визначення є незрозумілими та такими, що заплутують. Цей розділ потребує доопрацювання.

Також доопрацювання потребує й розділ про передачу даних до іноземних держав чи міжнародних організацій.

Сумнівною є ультимативна заборона відмовляти в наданні послуги чи товару у випадку відмови в обробці персональних даних, а також вимога до іноземних компаній призначати своїх представників в Україні.

Ураховуючи всі наведені недоліки, законопроєкт не можна приймати в такому вигляді.

Насамкінець хочеться зауважити, що, розробляючи такий вагомий законопроєкт, варто ретельно оцінювати ризики, пов'язані з обмеженням свободи слова та стримуванням економічної активності. У багатьох нормах законопроєкт №5628 по суті копіює GDPR Європейського Союзу, причому чимало норм в українському проєкті є навіть жорсткішими за європейські, незважаючи на те, що європейський регламент вважається найбільш вимогливим щодо поводження з даними. Законопроєкт, до того ж, сам по собі є доволі об'ємним і складним. І якщо ретельно вивчити і імплементувати його положення є доцільним для великих компаній чи державних структур, для малого бізнесу це може стати непосильним тягарем, що погіршить конкуренцію на ринку і просто економічну ситуацію в країні.

У Сполучених Штатах Америки, наприклад, відсутній федеральний закон, який би регламентував питання обробки персональних даних загалом. "Аналог GDPR" існує в штаті Каліфорнія та деяких інших штатах, але там дія цих законодавчих актів розповсюджуються лише на великий бізнес і загалом вони є суттєво менш вимогливими за європейські норми (наприклад, не передбачено права на стирання, штрафи за порушення є значно меншими).

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Закон України "Про захист персональних даних" 2297-VI
2. Проєкт Закону України "Про захист персональних даних" 5628 від 07.06.2021
3. General Data Protection Regulation (EU) 2016/679
4. Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Consolidated text (CM/Inf(2018)15-final) — https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf
5. УГСПЛ: Президент оформив наступ на свободу інформації законодавчо / Право на приватність — http://privacy.khpg.org/1277476182
6. Коментар до Закону України «Про захист персональних даних», Ігор Усенко / Право на приватність — http://privacy.khpg.org/1604922604
7. Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises — https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep
8. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data — https://rm.coe.int/16808ac918
9. California Consumer Privacy Act of 2018 — https://iapp.org/resources/article/comparing-privacy-laws-gdpr-v-ccpa
10. Закон України "Про інформацію" (редакція від 16.07.2020)
11. Кримінальний кодекс України (редакція від 08.08.2021)