Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Страсбург , 19 січня 2012 DGI/DP/expertiseUKR(2012)

АНАЛІЗ ЗАКОНУ УКРАЇНИ ПРО ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

Марі Жорж
Незалежний експерт з питань захисту даних,
колишній радник Голови CNIL,
(Національна комісія з інформаційних
технологій та свобод)
Франція

та

Грем Саттон
Незалежний експерт з питань захисту даних,
Колишній радник зі стратегічних питань,
Управління конституційних справ,
Велика Британія

ЗМІСТ

*****

МАРІ ЖОРЖ

Звіт про оцінку існуючої української законодавчої бази в галузі захисту даних

I. Вступ та пояснювальна записка

1. Метою викладеного нижче аналізу є представити основні спостереження та перші рекомендації щодо української законодавчої бази в галузі права громадян на захист даних у зв'язку з Конвенцією Ради Європи про захист осіб стосовно автономізованої обробки персональних даних (далі – "Конвенція №108") та Додатковим Протоколом до неї, а також з урахуванням європейської Директиви 95/46/ЕС (далі – "Директива ЄС"), яка розробляє принципи вищезазначених документів Ради Європи для цілей гармонізації.

2. Через те, що як Конвенція №108, так і законодавча база ЄС з питань захисту даних на даний час є предметом перегляду (з метою забезпечення кращого захисту прав фізичних осіб перед різноманітними викликами, до яких призводить поява нових технологій), і я взяла на себе сміливість, у разі необхідності, вносити пропозиції відповідно до основних ідей поточної дискусії. Проте в цих рекомендаціях також береться до уваги той факт, що Україна перебуває в такому періоді, кола вона набуває перший досвід у цій галузі.

3. Українська законодавча база, щодо якої я отримала запит на оцінку, складається із:

- Закону України "Про захист персональних даних" 2010 року (далі – "Закон", останній переклад англійською мовою отриманий 19 грудня 2011 р.) та відповідних документів, передбачених в цьому законі, які вже ухвалені:
- Закону України "Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних" від 1 червня 2011 р. (переклад англійською мовою отриманий 22 листопада 2011 р.),
- Постанови Кабінету Міністрів "Про затвердження Положення про Державний реєстр баз персональних даних та порядок його ведення" від 25 травня 2011 року (далі – "Постанова", переклад англійською мовою отриманий 22 листопада 2011 р.),
- Указу Президента України "Про положення про Державну службу України з питань захисту персональних даних" від 6 квітня 2011 р. **(**далі - "Указ про **ДСУЗПД",** іноді згадується в Законі як "Уповноважений орган з питань захисту даних", переклад англійською мовою отриманий 22 листопада 2011 р.).

Необхідно нагадати, що право на захист даних було вперше впроваджено в Україні в якості основного права в зв'язку з правом на приватне життя, у статті 32 Конституції України 1996 року (офіційний переклад англійською мовою на http://www.rada.gov.ua/const/conengl.htm)[1]

[1] **Стаття 32.**

- Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України.
- Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

4. На загальному рівні законодавча система відповідає обсягу європейського законодавства:

Вона охоплює як державний, так і приватний сектор в одному всеосяжному документі, як у майже всіх європейських державах.
Вона охоплює як ручну, так і автоматизовану обробку даних, як і Директива ЄС, і це, напевно, стане обов'язковою вимогою після перегляду Конвенції №108.
Вона визначає принципи, які ведуть до:

- зобов'язань, які повинні дотримуватися тими, хто створює / опрацьовує та обробляє персональні дані, у тому числі у зв'язку з передачею персональних даних в зарубіжні країни,
- особистих прав громадян, чиї дані обробляються попередньо згаданими особами,
- особливих випадків звільнення від зобов'язань у зв'язку з іншими правами людини,
- особливих винятків у межах особливих потреб у галузі державної безпеки, необхідних у демократичному суспільстві.

Вона впроваджує низку механізмів, що сприяють та забезпечують дотримання закону, серед яких заснування централізованого державного органу, відповідального, зокрема, за контроль дотримання законодавства із захисту даних, а також призначення внутрішніх спеціалістів з питань збереження приватності у складі організацій, що збирають та обробляють персональні дані (що, як передбачається, буде внесене як вимога до переглянутих європейських документів).
Вона визначає засоби правового захисту та санкції в разі порушення закону.
Тим не менше, деякі аспекти структури документу ускладнюють прочитання закону, а тому й можливість його інтерпретації. Більше того, дуже багато положень викликають питання або проблеми з точки зору захисту, який забезпечується для громадян, його технологічних аспектів, а також практичного застосування цих правил (виходячи з досвіду інших країн).
Ці недоліки, тією чи іншою мірою, впливають на практично всі складові частини документу, його предмет, сферу застосування, визначення, принципи, виключення й обмеження, а також положення про Державну службу України з питань захисту персональних даних, яка аж ніяк не має можливості діяти незалежно та неупереджено, хоча й має повноваження, зокрема, щодо подання позовів та контролю забезпечення прав людини на місці в державному та приватному секторах.

- Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею.
- Кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації.

Внаслідок цього я хотіла б представити свої основні зауваження / рекомендації відповідно до логічного підходу як Конвенції №108, так і Директиви ЄС наступним чином:

- Мета закону та зв'язок із конституційними правами людини, зокрема, щодо захисту персональних даних
- Структура закону
- Визначення термінів
- Чинне законодавство та сфера дії Закону
- Принципи, яких повинен дотримуватися персонал, яких працює з обробкою даних
- Права громадян
- Механізми впровадження та забезпечення дотримання закону

Утім, хоча цей звіт був написаний, перш ніж відбувся будь-який обмін думками з компетентними українськими спеціалістами, які брали участь у підготовці та прийнятті цих документів, у мене виникає питання, чи я правильно зрозуміла деякі положення, адже через переклад або відмінності загальних правових та організаційних концепцій, що мені відомі. Тому я прошу вибачення, якщо я включила сюди певні невірні твердження.

2. Детальна оцінка

Мета Закону

5. Назва Закону говорить про те, що у ньому йдеться про "захист персональних даних". Цей вираз, що з'явився у цій сфері з німецької мови в 1971 р., на даний час використовується на міжнародному рівні, і тому я також буду його використовувати. Тим не менше, він дещо заплутує, адже здається, що мова йде тільки про питання безпеки даних, у той час як ані Конституція України, ні Конвенція №108 чи Директива ЄС не використовують цей термін. Європейський тексти визначають мету / предмет, використовуючи набагато ширше та чіткіше формулювання: "забезпечення захисту основних прав громадян, зокрема, на їх особисте життя, у зв'язку з обробкою персональних даних".

6. У наявній статті 1 Закону (Сфера дії Закону) говориться, що Закон "регулює відносини, пов'язані із захистом персональних даних під час їх обробки", що не роз'яснює сферу дії.

7. У статті 3 робиться посилання на Конституцію, але не уточнюється, що посилання стосується, зокрема, її положень у сфері прав людини (другий розділ) та положень стосовно недоторканності приватного життя та персональних даних (стаття 32).

8. Можна було б подумати, що йдеться саме про ці основні права, якщо читати текст до статті 22.2 про парламентський контроль прав людини щодо персональних даних, який буде здійснювати Уповноважений з прав людини у Парламенті.

9. Ясність з цього питання із самого початку тексту Закону дуже допомогла б зрозуміти мету Закону, особливо всім особам з огляду на їх нові права. Це було б також доречно у якості загальних критеріїв для роз'яснення принципів та при їх застосуванні у конкретних випадках тими, хто проводить обробку персональних даних, Уповноваженим державним органом з питань захисту персональних даних та з метою забезпечення обізнаності всіх сторін, у тому числі на міжнародному рівні.

Структура Закону

10. Для ясності та зручності прочитання / розуміння тексту громадянами у зв'язку з їх обов'язками (коли вони мають намір опрацьовувати / обробляти персональні дані) і їх правами (коли вони є суб'єктами обробки даних іншими особами), було б корисно організувати виклад положень Закону за цими двома основними аспектами. Це можна було б зробити за рахунок перегрупування, зокрема, всіх положень, які пов'язані з обов'язками, у окремий розділ / главу та об'єднання всього, що стосується прав суб'єктів, що володіють даними, в іншому розділі / главі.

11. Здається, що нинішній підхід і структура Закону були в основному орієнтовані на особливості та внутрішнє бачення ІТ, що спричинене підходом діючої Конвенції №108 (1981 р.), але цей підхід був розвинений у Директиві ЄС чотирнадцять років потому, набувши більш узагальненого баченні та будучи адаптований як до технічних інновацій, так і до необхідності вірного застосування всіх правових принципів. Передбачається, що перегляд Конвенції приведе у відповідність її технічні концепції.

12. Технічний підхід українського Закону 2011 р. зосереджений виключно на структурованих базах даних і обробці та використанні даних для баз даних або із баз даних, а отже включає в себе скоріше внутрішнє технічне, юридичне та фінансове бачення різних зацікавлених сторін тими, хто відповідає за управління базами даних. Такий підхід призводить до плутанини. Як приклад, наведу легітимність розкриття особистих даних, що відносяться до інших осіб, третій особі (що в тексті згадується як "право доступу" третьої сторони) і розкриття даних суб'єкту даних як відповідь на його / її фундаментальне право знати, які його / її дані зберігаються / обробляються (що за загальною міжнародною концепцією називається його / її "правом доступу"), що розглядається в межах положень послідовно статей 16 "Порядок доступу до персональних даних", 17 "Відстрочення або відмова у доступі до персональних даних", 18 "Оскарження рішення про відстрочення або відмову в доступі до персональних даних", 19 "Оплата доступу до персональних даних", 20 "Зміни і доповнення до персональних даних".

13. Тому я рекомендувала би в процесі майбутніх змін Закону додержуватися логічнішого порядку, що міститься у Конвенції №108, і в директиви ЄС:

- Мета закону: переглянути статтю 3, уточнивши, що цей закон спрямований на забезпечення прав громадян на захист при обробці персональних даних,
- Визначення (переглянути статтю 2, див. нижче),
- Сфера дії закону (переглянути поточну статтю 1, див. нижче) та відповідне законодавство,
- Зміст і правила щодо процедури впровадження та функціонування обробки персональних даних в окремому розділі / главі – як зобов'язання, які повинні застосовуватися володільцями процесу обробки даних та самими операторами з обробки (переглянути та реорганізувати наступні поточні статті: стаття 6 Загальні вимоги, 7 Особливі вимоги до обробки "чутливих" даних, 10 Використання персональних даних, 11 Підстави виникнення "права" на використання персональних даних, 12 Збирання персональних даних, 13 Зберігання персональних даних, 14 Поширення персональних даних, 15 Знищення персональних даних, 16-19 Порядок доступу до персональних даних третіх осіб і суб'єкта даних, за винятком положень про право доступу суб'єкта даних, 21 Повідомлення про дії з персональними даними, за винятком положень, пов'язаних з вимогою суб'єкта даних, стаття 24 Забезпечення захисту персональних даних

(вимоги безпеки), стаття 29 Передача даних іноземним державам (так зване "Міжнародне співробітництво"), стаття 9 Реєстрація баз персональних даних);
- Права суб'єктів даних в окремому розділі / главі (переглянути статтю 8, інші відповідні положення, таких як ті, що містяться в статті 12 (Збір даних), 16-19 Доступ до даних, 21 Повідомлення суб'єкта даних про передачу даних третім особам,
- Обмеження застосування принципів (переглянути поточну статтю 25);
- Механізми застосування та впровадження, згруповані в окремому розділі / главі (переглянути та реорганізувати поточні статті 22, 23 Уповноважений державний орган з питань захисту персональних даних (УДОЗПД), статтю 24.5 Внутрішній структурний підрозділ або відповідальна особа, статтю 27 Застосування положень закону (доповнення іншими законами, професійний кодекс поведінки), статтю 25 Фінансування діяльності із захисту персональних даних),
- Відповідальність за порушення Закону (ст. 28),
- Прикінцеві положення (ст. 30).

Визначення

14. Загальні зауваження щодо технічних понять. Як було сказано раніше, бачення бази даних при автоматизації даних, орієнтоване на ІТ, занадто обмежене і не дозволяє з легкістю описати всі операції із захисту даних (напр., збір даних, зберігання, застосування певного програмного забезпечення для розрахунків на основі даних, розкриття даних іншим, ін.) із законною метою, що є основним принципом підходу до "захисту даних". Це наступним чином впливає на наступні визначення:

15. Використання поняття бази даних необхідно обмежити, як і в директиві ЄС, до файлів у ручному режимі, таке визначення було б принаймні технічно нейтральним.

16. Визначення обробки персональних даних не повинне обмежуватися конкретними операціями. Тобто, перелік операцій, викладений на самому початку визначення, повинен бути ілюстративним (замінити "які пов'язані з" на "такі як")

17. Визначення персональних даних як таке має свою цінність, але проблема в тому, що дуже часто поняття "про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована" обмежено тлумачиться як особа, яка може бути визначена володільцем. На практиці це призводить до широких непродуктивних дискусій, протягом яких суб'єкт даних залишається безправним. Тому було б розумно дещо більше уточнити, що таке визначення може бути прямо чи опосередковано надане володільцем або іншими особами.

18. Три юридичні зауваження з приводу визначення володільця, розпорядника, суб'єкта даних і третіх осіб.

1) Акцент на "праві власності" на базу даних при наданні повноважень володільцю при визначенні розпорядника та третіх сторін (і в інших положеннях Закону та пов'язаних з ним текстах) є недоречним, оскільки персональні дані, будучи предметом особистого права людини, навряд чи можуть підлягати праву власності в руках інших осіб.

2) Володілець, суб'єкт даних і третя особа визначаються з урахуванням вірного застосування закону. А як щодо володільців або третіх осіб, які не мають

повноважень відповідно до закону бути такими суб'єктами? Необхідно, щоб закон охоплював і їх, в іншому випадку до них неможливо буде застосувати санкції, і суб'єкт даних не матиме прав.

3) Стосовно визначення розпорядника, мене занепокоїло те, що я прочитала, що розпорядник має "право" обробляти дані (проблема перекладу)? Було б більш доречно кваліфікувати розпорядника як такого, що "діє від імені володільця", як прописано в директиві ЄС і як це передбачається відобразити в оновленому варіанті Конвенції №108.

19. Ці коментарі можуть викликати питання щодо корисності статті 4, яка перераховує суб'єктів відносин, пов'язаних з персональними даними.

20. Що стосується визначення згоди суб'єкта даних, я б наголосила на трьох складових, які варто взяти до уваги для забезпечення дотримання європейського підходу, який націлений на те, щоб уникнути формальної згоди в численних ситуаціях, коли людина не може вільно давати згоду (напр., найняті працівники), підхід полягає в обмеженні згоди як юридичної підстави для обробки даних до ситуацій, до ситуацій, коли людина "вільна" і "поінформована" щодо обробки "конкретних" даних:

1) Характеристика "вільна" на даний час відсутнє у визначенні.

2) Відповідно визначення, інформація, що надається суб'єкту даних стосується тільки цілі обробки даних, але цього ніколи не буває достатньо (хто володілець, хто одержувачі, чи відбувається розкриття якоїсь інформації третім особам? чи передаються якісь дані в третю країну та ін.). Через те, що все залежить від конкретної ситуації, поняття "конкретної і поінформованої згоди" може бути відповідним узагальненим розв'язанням проблеми на рівні визначення.

3) Визначення прописує, що згода має бути надана в письмовій формі (на папері). Це може працювати в багатьох ситуаціях, але це занадто обмежуючий підхід на практиці (наприклад, надання згоди он-лайн). Може бути достатньо сказати, що згода має бути "явно вираженою", щоб уникнути застосування мовчазної згоди та пристосувати її застосування для всіх конкретних ситуацій.

21. Можливість надати визначення отримувачів: таке визначення не входить до наявної Конвенції №108, але передбачається в межах директиви ЄС на додаток до визначення третьої особи. Воно включає в себе внутрішні спеціальні служби володільця, які обробляють дані в зв'язку з їх конкретними завданнями (і, фактично, несуть обов'язки, як це передбачено в статті 10.3), а також третіх осіб. Це подвійне поняття має особливе значення у зв'язку з легітимністю (і відповідальністю) різних суб'єктів доступу або отримання даних, обов'язком реєстрації (прозорість для всіх) та зобов'язанням інформувати суб'єкта даних. Див. Директиву ЄС і поточний відкритий проект модернізації Конвенції №108.

Сфера дії Закону: обробка персональних даних виключена із Закону

22. Стаття 1 передбачає три винятки. Те, наскільки вони легітимні, потребує роз'яснень.

23. У Європі виключення зі сфери дії законів про захист даних виправдані забезпеченням, зокрема, права людини та основоположних свобод, які можуть вступати в конфлікт з "захистом даних", але за певних умов, права на особисте життя та свободу вираження. Я рекомендую взяти їх до уваги при перегляді Закону, керуючись наступними зауваженнями.

24. Кожна людина в демократичному суспільстві має право на приватне життя. Тому будь-яка особа може обробляти будь-які дані із суто особистими цілями без будь-яких перешкод, таких як необхідність застосування цього Закону. Побутова діяльність також є складовою частиною такої діяльності. У цьому сенсі посилання в поточному визначенні також і на "непрофесійні потреби" є неточним, оскільки існують інші види діяльності, які не є професійними, і не є особистими.

25. Звичайно, обмеження цього виключення повинне включати те, що фізична особа вживатиме відповідні заходи, щоб гарантувати безпеку персональних даних, що використовуються. Ті особи, які пропонують цифрові послуги клієнтам, у сфері такої діяльності (напр., послуги поштової скриньки он-лайн, архіви), коли вони обробляють персональні дані, пов'язані з іншими, для застосування в своїй особистій діяльності, пов'язаній з особистим життям, підпадають під цей Закон і повинні забезпечити своїм клієнтам заходи безпеки.

26. Кожна особа також має право на свободу вираження думок. Деякі виключення у сфері "захисту даних" необхідні, адже конфлікт між недоторканністю приватного життя і свободою вираження поглядів в демократичному суспільстві може розглядатися тільки в судовому порядку (тобто, коли на карту ставиться честь або репутація людини). Тому, коли Закон передбачає виняток щодо обробки даних "журналістами", це абсолютно вірно (зокрема, щодо захисту джерел при підготовці редакційного матеріалу), але це має свої межі, особливо за умови вживання заходів безпеки, і, як правило, в межах закону встановлюються гарантії для громадян як компенсація відмови у праві доступу (захист джерел), як то право на відповідь, коли інформація про них, що опублікована журналістом, не відповідає дійсності. Ці умови чітко не визначені в статті 1.

27. Як згадувалося раніше, кожна людина має право на свободу вираження. Тому це виключення повинно бути ширшим, що тут не спостерігається.

28. Третій передбачений виняток на користь "працівників творчих професій" не є адекватним з наступних причин:

1) тільки частина творчої діяльності належить до галузі свободи вираження поглядів – частина, що стосується мистецьких і літературних цілей, і

2) особи, які не є творчими працівниками, також повинні мати свободу вираження думок.

Застосовне право

29. Ні Конвенція №108, ні Закон не містять жодних положень з питання застосовного права. Проте, у певному контексті, за умов зростання транснаціональних обсягів обробки даних, на національному рівні кожному важливо знати, до обробки яких даних застосовується українське законодавство. Для цілей гармонізації Директива ЄС встановлює критерії, які можуть братися до уваги, проте не забуваймо, що ці критерії наразі виправляються в процесі перегляду системи законодавства із захисту даних. Теоретично необхідно брати до уваги три основні критерії або їх поєднання:

- громадянство суб'єкта даних, хоча, загалом, цього недостатньо, адже необхідно передбачити захист суб'єкта даних незалежно від її/його національності, якщо її/його дані обробляються на території Україні,
- місце здійснення обробки даних,

- місце розташування володільця процесу обробки даних в Україні або за її межами, де застосовується міжнародне публічне право (тобто, в посольствах), і якщо володільці здійснюють обробку даних на її території. Цей останній критерій є чинним відповідно до правил Всесвітньої торгової організації (див. статтю XIV Генеральної Тарифної Угоди GATTS 1994 р.).

Принципи, обов'язки володільця (і розпорядника), основні коментарі

30. Згідно Конвенції №108 такі принципи / обов'язки володільців (і розпорядників) включають в себе три групи принципів

- Основні принципи ("якість даних" у статті 5 Закону), незалежно від характеру обробки дані, зокрема відповідь на ризики при переведенні даних у цифровий формат. Ці ризики пов'язані з легкістю використання таких даних для будь-яких цілей, їх зберігання протягом тривалого часу, змінювання, копіювання, розкриття за низького рівня витрат),
- Підсиленні принципи у зв'язку з даними, обробка яких здатна призвести до можливої дискримінації (стаття 6 "Особливі категорії даних")
- Принцип безпеки (стаття 7)

31. Основні Загальні принципи українського Закону розглядаються в статті 6. Для ясності, я вважаю, можна розділити загальні принципи, пов'язані з принципами статті 5 Конвенції №108 (справедливий і законний збір і обробка, визначені та законні цілі, пропорційність інформаційного змісту і тривалість утримання у зв'язку з цілями), та питання щодо правової основи для законних цілей обробки даних (згода, закон).

32. Більше того, я замислилася щодо того, чи є доцільною концептуальна правова система для цілей обробки даних, що стає законною тільки на основі згоди суб'єкта даних або якщо це сформульовано в законі або в інших нормативних актах.

33. Ця система знайшла своє відображення у статті 32 Конституції, але так, як вона сформульована в Законі, вона здається недієспроможною. Замість цього цей Закон міг би сформулювати загальні критерії правової бази законних цілей, що дозволить уникнути прийняття норм з будь-якого питання в контексті величезного зростання обсягів обробки різних даних.

34. Проте нормативний підхід необхідно зберегти в сфері обробки даних, що здійснюється в державному секторі для цілей прозорості та забезпечення демократичного процесу прийняття рішень щодо обробки таких даних. Його можна також використовувати для обробки інших даних, коли виникають конкретні проблеми.

35. Конвенція №108 на даний час нічого не говорить із цього питання, але ілюстрацію такого диференційованого підходу можна знайти в статтях Директиви ЄС, зокрема 7 (перелік правових підстав / критеріїв законних цілей обробки даних), 18 про реєстрацію обробки даних, а також у статті 20 щодо попередньою вивчення проекту обробки даних у випадках, що представляють конкретні ризики для основних прав і свобод, як показано у статті 53). Подальші законодавчі потреби також викладені в додатковій директиві ЄС, пов'язаній з конфіденційністю та електронною комунікацією, де легітимність конкретних цілей визначається разом з умовами.

36. Деяких принципів Конвенції №108 і Директиви ЄС бракує: обробка повинна бути "справедливою", а також дані, що обробляються, повинні бути не тільки відповідними (і не надмірними), але й "адекватними" меті.

37. Стаття 6.9 Закону щодо використання даних в історичних, статистичних чи наукових цілях у зв'язку з принципом використання даних, які не є несумісними з метою обробки даних, і принципу обмеженого утримання, може виявитися нереалістичною ("може здійснюватися лише в знеособленому вигляді"). Існують певні соціальні чи громадські потреби у демократичному суспільстві, такі, як дослідження епідеміології на основі медичних карток, або зберігання історичних архівів для майбутніх досліджень. Ці заходи мають мету, "сумісну" з первинними цілями, для яких дані були зібрані та пізніше оброблені, та повинні обов'язково ґрунтуватися на "ідентифікації" суб'єкта даних, прямо чи опосередковано, на рівні первинних даних (і, звичайно, не на рівні результату дослідження, окрім як у галузі досліджень дуже старих архівів). Тому їх необхідно дозволити, звичайно, передбачивши особливі гарантії (див. статтю 6 Директиви ЄС та документи на національному рівні, тобто закони про архіви та медичні епідеміологічні дослідження).

38. Посилений режим для спеціальних категорій даних, що зазвичай звуться "чутливими даними", передбачений у статті 7 українського Закону. Список "чутливих" даних відповідає переліку у Конвенції №108, визначеному для підсилення захисту від можливої дискримінації. Проблема в тому, що перераховані винятки щодо заборони на обробку таких даних, будучи виправданими, не супроводжуються принципом "особливих гарантій" (тобто в медичному секторі гарантією є, на додаток до усіх інших вимог Закону, те, що дані, з якими працює персонал, охороняються обов'язком щодо лікарської таємниці).

39. Дивлячись на останні технологічні розробки, можна було б передбачити можливість додати до списку чутливих даних, поряд із відповідними виключеннями та гарантіями, біометричні дані та генетичні дані з метою збереження, зокрема, гідності та презумпції невинності людини. У сфері "обробки чутливих даних" можна також розглянути відеоспостереження з метою забезпечити свободу пересування. Ці можливості на даний час розглядаються в ЄС і в Раді Європи.

Обов'язки, передбачені в українському Законі

40. Статті від 9 до 21 (зобов'язання щодо реєстрації обробки даних і пов'язана з цим Постанова, що стосуються використання, збирання, зберігання, доступу, розкриття, стирання персональних даних) і стаття 24 (від 1 до 4 щодо обов'язку забезпечити безпеку обробки даних).

41. Для більш чіткого прочитання тексту положення щодо таких докладних зобов'язань (після виключення тих, які стосуються прав суб'єктів даних, як зазначено на початку цього звіту) можна переформулювати / перегрупувати в окремий розділ / главу з попередньою статтею 6 про загальні принципи, статтею 7 про чутливі дані, 24 про безпеку, статтею 9 про реєстрацію обробки даних, яка є процесуальною нормою, що йтиме після переглянутої статті 6 або наприкінці.

42. З метою переписування цих статей у вигляді простішого тексту на основі більш загального та логічного бачення обробки даних у зв'язку з її метою, як зазначено на початку цього звіту, а також щоб не додавати складності, беручи до уваги цей звіт разом з іншими звітами експертів з того ж питання, я не буду тут

детально викладати свої коментарі, тому що вони дуже наближені до тих, що наразі висловлюються іншими європейськими експертами, зокрема до коментарів Євроюсту, які я отримала 12 грудня 2011 року.

Правила, що стосуються передачі даних до зарубіжних країн

43. Беручи до уваги Директиву ЄС (статті 26 і 27) та Додатковий протокол до Конвенції №108 (стаття 2), а також положення, закріплені в статті 29 Закону "Про міжнародне співробітництво", виникають декілька запитань.

44. Зокрема, щодо статті 29.3, неясно, 1) що таке "*належний захист*" даних, переданих до іншої країни, 2) хто дає "*відповідний дозвіл*", 3) відповідно до якої процедури "*в порядку, встановленому законодавством*".

45. Принцип, викладений в останньому реченні статті 29.3 вітається, адже він поширює на передачу даних основний "принцип мети", що означає, що ніхто за межами України не зможе використовувати персональні дані, передані з іншою метою, ніж та мета, для якої ці дані були зібрані (в Україні). Але, звичайно, цього принципу недостатньо для забезпечення повного захисту, що повертає нас до вищезазначеного питання про те, що таке "належний захист".

46. Я не знаю, чи у відповідному законі, який не прийнятий, планується розв'язати ці проблеми.

Стаття 9 про реєстрацію бази персональних даних Державним органом із питань захисту даних, а також про Постанову, прийняту Кабінетом Міністрів України з цього питання 25 травня 2011 року.

47. Прозорість у демократичному суспільстві у сферах діяльності, які представляють певні ризики, є вкрай важливим принципом, який діє як превентивний захід та спосіб роботи з інформацією та управління для всіх. Конвенція №108 у статті 8 визначає, що будь-яка людина повинна мати можливість з'ясувати, чи здійснюється обробка його / її персональних даних, але у національному законодавстві необхідно точно визначити, як це робитиметься. У Директиві ЄС централізований реєстр, сформований наглядовим органом із захисту даних та працюючий на основі "повідомлення" (заяви) з боку розпорядників обробки даних, розглядається у статтях з 18 по 21.

48. Для тих цілей, щоб кожний мав достатню інформацію, аби перевірити законність обробки, реєстр, сформований в ЄС, є набагато більш інформативним, ніж той, що представлений Постановою. Останній, здається, включає в себе, загалом, тільки назву та розташування володільців і розпорядників, а також призначення бази даних. Це відповідає статті 8.a Конвенції. Але для того щоб контролювати, як застосовуються ці принципи на основі Директиви ЄС (стаття 19), необхідно додати декілька елементів, наприклад, залучені категорії суб'єктів даних, категорії даних, які обробляються, різні категорії одержувачів даних, можливу передачу даних в зарубіжні країни. Вимога щодо інформування суб'єктів даних на даний час розглядається в ЄС, і це може привести, при застосуванні "справедливої обробки персональних даних", до появи додаткової інформації, такої як обов'язковий чи факультативний характер надання даних, термін зберігання даних і засоби реалізації прав.

49. Постанова, здається, не уточнює, коли таке повідомлення повинне бути надане. З урахуванням того, що таке повідомлення має забезпечити прозорість, повідомлення повинне бути надане до проведення обробки даних.

50. Термін у 10 днів (стаття 11 Постанови), що надається УДООПД на те, щоб перевірити повноту та достовірність заявки, її внесення до реєстру, а також для проведення сертифікації реєстрації, здається дуже коротким, особливо за набрання чинності положень, на які будуть подавати безліч заявок у зв'язку з поточною обробкою даних.

51. Не вся обробка даних на практиці становить ризик, тому можна пошукати деякі "менш забюрократизовані" рішення щодо повідомлення про проведення обробки даних та їх опублікування, так як в це на даний час робиться в ЄС, але, враховуючи те, що Україна отримує перший досвід у сфері "захисту даних", я дотримуюся думки, що такий центральний реєстр може бути дуже доречним.

52. У цьому сенсі я хотіла би зрозуміти, що мається на увазі під повноваженнями Органу із захисту даних перевіряти "надійність" застосування обробки даних перед видачею сертифіката. Чи означає це, що він повинен перевірити відповідність кожного процесу обробки даних закону? Якщо це так, особливо протягом початкового періоду, це може виявитися важкою роботою, та, звичайно, її неможливо буде виконати протягом "10 днів". У будь-якому випадку, було б корисно, якби Державний орган усе ж мав право проводити таку перевірку цілеспрямовано, там, де виникають значні проблеми.

53. Крім того, повідомлення про обробку даних дають Органу із захисту даних повну документацію щодо різного роду поточної обробки даних, а також щодо еволюції його діяльності. Тому цей Орган матиме можливість оцінити, де можуть бути доцільними подальші рекомендації та нормативні тексти, тобто за секторами, цілями або конкретною технологією.

54. Доступ громадськості до Реєстру. Статті 14 і 15 Постанови, здається, адекватно організовують доступ до Реєстру для будь-кого, навіть електронним шляхом, що практично забезпечує прозорість обробки даних.

Права суб'єкта даних (стаття 8, відповідні положення статті 12 про збір даних, 16,17,18,19 про доступ до даних, статті 21 про повідомлення суб'єкта даних щодо передачі даних третій особі)

55. Перші два права, закріплені у статті 8 Закону, пов'язані з правом всіх на прозорість обробки даних. У цьому контексті буде логічно взяти до уваги мої попередні коментарі щодо змісту Реєстру, який є конкретним способом реалізації цього загального права.

56. Стаття 12 про збір даних забезпечує обов'язок володільця повідомити суб'єкта даних, що його / її дані включені в базу даних протягом 10 днів з моменту такої дії (стаття 12.2). Це положення викликає низку проблем.

57. Цей обов'язок інформування не застосовується, коли дані збираються з "відкритих джерел". Ця концепція "відкритих джерел" не є визнаною концепцією в Європейському Союзі, тому у всьому світі здійснюється лобіювання з боку маркетингової галузі іще з 70-х років з метою зробити такі джерела відкритими для "вільного" використання. Кожний державний реєстр персональних даних,

доступний громадськості, що в основному служить в демократичних країнах для прозорості / контролю (тобто, реєстр народжених, виборчі списки, реєстри об'єднань, підприємств), створений та доступний для конкретних цілей, а не для "вільного" використання таких реєстрів. ЄС відмовився прийняти цю концепцію / підхід у процесі в розробки та прийняття європейської Директиви, а також угоди про "Безпечну гавань" з США в контексті визнання рівня достатності для передачі комерційних даних у США.

58. Обов'язок інформування, пов'язаний зі збором даних (і подальшою обробкою або передачею третім особам, якщо такі мають місце), передбачений в директиві ЄС (стаття 10) під час збору даних, коли дані стосовно особи збираються, а не принципово пізніше, коли дані вводяться в базу даних (стаття 12.2 Закону), або після того, як дані були передані третій стороні, як це робить можливим стаття 21 Закону. Цей принцип важливий у контексті принципу "справедливої" обробки даних, незалежно від правової підстави, що забезпечує законність її мети (згода або інші підстави). Це важливе право бути поінформованим у момент збору інформації не передбачене в Законі.

59. Третє, четверте і шосте право, передбачені у статті 8 Закону, стосуються права суб'єкта даних отримати підтвердження того, що він / вона є субєктом даних, його / її права на отримання доступу / копії своїх даних та його / її право на виправлення або видалення невірних або незаконних даних.

60. Стаття 12 Закону додає право суб'єкту даних на доступ до своїх даних, право знати джерела цих даних. Це передбачено в Директиві ЄС у статті 13 та є абсолютно правильним. Для ясності при читанні тексту це право повинне бути, як і в Директиві, пересунуте ближче до положень про право на доступ, що на даний час передбачені у статті 8 Закону.

61. Відповідно до Конвенції (стаття 8, пп. b, c), Закон передбачає, що відповідь на запит суб'єкта даних щодо передачі даних має бути надана в межах розумних термінів, що обмежені строком 30 днів, і цей термін представляється розумним.

62. *Як фізична особа реалізовуватиме своє право на доступ і виправлення чи видалення інформації*? Безпосередньо звертатиметься до володільця? Або через компетентні органи (орган) із питань захисту даних, як, очевидно, пропонується в статті 8.8? Це не зрозуміло при прочитанні статті 8, здається, що це звернення спрямовується "безпосередньо" до володільця при подальшому прочитанні статті 16.6, яка стосується цього питання. У статті 8 слід уточнити, що спочатку запит надсилається безпосередньо володільцю. Звичайно, якщо суб'єкти даних не задоволені відповіддю, вони повинні мати право направити це питання до Органу захисту даних або до суду за своїм вибором, як це представляється можливим на підставі статей 8.8 і 8.9.

63. Стаття 18 стосується випадку відмови суб'єкту даних у доступі до його / її даних і передбачає звернення до суду, як це передбачено в Конституції. Якщо єдина можливість – діяти через суд, на практиці вона виявиться непрацездатною через тривалість судових процедур, і я рекомендую взяти до уваги більш гнучкий підхід, який я запропонувала вище у цьому звіті.

64. Такий подвійний підхід ще більш рекомендований у разі обмеження права доступу на підставі інтересів громадської національної безпеки й оборони (тобто,

секретною службою). У такій ситуації втручання Органу із питань захисту даних є однією з основних можливостей захистити особу та перевірити законність і достовірність даних в якості компенсації обмеження його / її права.

65. *За який рахунок може реалізуватися право на доступ*? Відповідь міститься не в статті 8, а в статті 19 про оплату доступу, яка передбачає, що "доступ" суб'єкта даних (і передача даних суб'єкту даних?) здійснюються безкоштовно. Було б більше сенсу прямо це передбачити в статті 8.

66. П'яте право, передбачене у статті 8 Закону, пов'язане із правом заперечення проти обробки даних за наявності підстав. Це право, яке прямо не передбачене в Конвенції №108 дуже вітається. Воно передбачене в Директиві ЄС (стаття 14), але без обмеження на обробку даних у державному секторі, як це має місце в українському Законі.

67. Наполегливо рекомендується розширити право на заперечення проти обробки даних на приватний сектор. І в окремому випадку, пов'язаному з маркетинговими цілями (не важливо, з якими конкретно цілями маркетингу: комерційними, стратегічними чи благодійними, і так далі), це право повинне надаватися без пояснення мотивації суб'єктом даних (див. статтю 14, b Директиви ЄС).

68. Крім того, рекомендується взяти до уваги відповідне підсилене право щодо обробки даних для маркетингових цілей із застосуванням телекомунікаційних та електронних засобів (наприклад, шляхом автоматичних дзвінків, повідомлень електронної пошти, смс), як це визначено в додатковій директиві ЄС з питань конфіденційності електронної інформації, яка передбачає в цьому разі згоду суб'єкта даних.

69. Я хотіла би також підняти питання щодо можливості розгляду питання розширення інструментів захисту суб'єкта даних стосовно можливого рішення щодо його / неї на основі профілювання (див. статтю 15 Директиви ЄС) і в зв'язку з цим права знати логіку процесу обробки даних (стаття 12 Директиви ЄС). Такі гарантії стали предметом останньої рекомендації, прийнятої Радою Європи, та очікується, що загальні положення з цього питання будуть внесені до модернізованої Конвенції №108.

Обмеження у застосуванні принципів і прав (стаття 25)

70. У Конвенції №108 положення, щодо яких законом можуть бути встановлені відступи / обмеження, поділяються на основні принципи (стаття 6 про якість даних), положення про чутливі дані (стаття 7) та про права суб'єкта даних (стаття 8)

71. У статті 25 Закону ці відступи / обмеження стосуються положень

- статті 8 про права фізичних осіб,
- статті 11 про правові підстави використання персональних даних
- статті 17 про відстрочення або відмову суб'єкту даних у доступі до його / її даних.

Але можливості інших виняткі / обмежень також передбачаються в інших статтях Закону (у зв'язку зі статтями 6 і 7 Конвенції):

- статті 6.6 про правові підстави обробки персональних даних,
- статті 14.2 про правові підстави розголошення даних

в обох випадках в "інтересах національної безпеки, економічного добробуту та прав людини";
- у статті 7.7. про виняток із заборони на обробку конфіденційних даних для цілей діяльності контррозвідки, боротьби з тероризмом.

72. Моє перше зауваження стосується переліку інтересів, задля яких Законом передбачені винятки / обмеження. Закон (як і українська Конституція у статті 32) передбачає обмеження в інтересах "економічного добробуту" (статті 6.6, 14.2, 25), що не передбачено в Конвенції №108 (стаття 9).

73. Моє друге зауваження стосується інтенсивності застосування відступів / обмежень, яке в Конвенції №108 обмежене (стаття 9, а в Директиві ЄС – стаття 13) на основі критерію, що це є "необхідним заходом у демократичному суспільстві в інтересах...". Такий критерій означає, що відступ обмежений тим, що є "необхідним та пропорційним" для захисту інтересів.

74. Таке формулювання включене до положень Закону, в той же час вказівки на загальні винятки у зв'язку з тим чи іншим інтересом не передбачають такого обмеження.

Механізми застосування та забезпечення дотримання Закону

75. З аналізу Закону та пов'язаних із ним текстів слідує, що український Закон встановлює багаторівневий підхід, коли від рівня володільця до суду та парламенту передбачено шість видів спеціалізованих органів, які мають загальний обов'язок / компетенцію щодо застосування цього Закону та його впровадження.

76. Хоча такий багаторівневий підхід наразі більше вітається та переважно передбачений в директиві ЄС, мої основні зауваження за різними компонентами цієї структури наступні.

Конкретна внутрішня структура або відповідальна особа володільця

77. Стаття 24.5 передбачає, що будь-яка організація (державна та приватна), яка обробляє дані, має обов'язок "визначити структурний підрозділ або відповідальну особу, яка організовує роботу, пов'язану із захистом персональних даних при їх обробці". Принципово, з огляду на підзвітність, такий підхід дуже вітається. Він не є обов'язковим у Директиві ЄС, але цілком може стати обов'язковим у майбутній переглянутій законодавчій базі ЄС, також деякі положення на цю тему цілком можуть бути введені до модернізованої Конвенції №108.

78. Питання щодо таких внутрішніх структурних функцій, по-перше, пов'язані з їх повноваженнями втручатися незалежно від інших служб. Такий статус (і його захист) не визначений конкретно у тексті.

79. Питання виникає і щодо їх місії. Чи їх мета обмежується забезпеченням безпеки даних (та процесу їх обробки), як це прописано в статті 24, в якій, здається, йдеться лише про безпеку? Чи їх місія ширша, оскільки вираз "відповідальна особа, яка організовує роботу" може передбачати, наприклад, і охоплення того, коли, як і який зміст інформації надається суб'єкту даних, а також роботу із зверненнями суб'єктів даних і так далі?

Професійні асоціації, які можуть розробляти корпоративні кодекси поведінки для забезпечення ефективного захисту (стаття 27.2 Закону)

80. Цей "інструмент", який також передбачений в директиві ЄС (стаття 27), є розширенням звичайної місії такої професійної структури, яка полягає в тому, щоб сприяти розробці своїми членами регуляторних актів, що регулюють діяльність їхнього сектора. Такий підхід за професійними кодексами поведінки може бути дуже ефективним у країнах, де професійні об'єднання є активними у багатьох конкретних та методологічних специфічних сферах свого сектору, що може бути дуже доречним в питаннях захисту даних, тому що практика та процес обробки персональних даних дуже часто є єдиними у межах сектору, але відрізняються від інших секторів. Але цей підхід виявляється ефективним не у всіх країнах ЄС, і до цього часу на рівні ЄС було розроблено дуже небагато професійних кодексів поведінки. Саме тому рекомендації сектору, прийняті контролюючими органами з питань захисту даних, можуть бути корисними після консультацій із зацікавленою стороною, а в разі необхідності (якщо рекомендації не впроваджуються) стає необхідною пропозиція щодо внесення додаткових положень до закону.

81. У будь-якому разі для правової ясності необхідно, щоб певний зовнішній незалежний державний орган контролював те, що такі професійні кодекси не суперечать Закону і додають до нього дещо цінне. Такий "контроль", покладений у Директиві ЄС про захист даних на незалежний наглядовий орган на національному рівні (а на рівні ЄС – на європейську групу таких національних органів влади та на Європейську Комісію), не передбачений в українському законі.

Уповноважений державний орган із питань захисту персональних даних (статті 4, 8.2.8 і 23 та відповідний наказ про положення про Державну службу України із питань захисту персональних даних від 6 квітня 2011 р.)

82. Цей орган несе велику відповідальність щодо динамічного застосування закону на національному та міжнародному рівнях:

- Подає законодавчі пропозицій щодо розвитку політики через міністра юстиції, зокрема, щодо удосконалення Закону, на затвердження урядом,
- Виступає володільцем "Реєстру персональних баз даних",
- Контролює застосування закону, видає накази у разі порушення закону,
- Працює з претензіями та скаргами суб'єктів даних і юридичних осіб,
- Проводить дослідження,
- Виконує освітні функції,
- (Організовує і контролює фінансування роботи інших організацій у сфері своєї компетенції)
- Співпрацює із зарубіжними колегами і бере участь у діяльності міжнародних організацій у сфері захисту даних.

83. Такі горизонтальні місії та повноваження органу із захисту даних є дуже своєчасними (див. також мої коментарі щодо реєстрації та застосування професійних кодексів поведінки) і в основному стимульовані Директивою ЄС, додатковим протоколом до Конвенції №108 і національним законодавством країн ЄС за винятком фінансування заходів інших органів щодо захисту даних. Однак головна проблема у порівнянні з європейською законодавчою базою полягає в тому, що цей орган очевидно є компонентом виконавчої гілки влади (стаття 23.1 Закону, стаття 1 Положення). Саме до цієї сфери належить компетенція міністра юстиції, який, зокрема:

- Пропонує Президенту кандидатів на призначення главою органу через прем'єр-міністра,

- Погоджує разом з главою структуру органу та його річний план роботи, зокрема те, що пов'язане з розслідуваннями та дослідженнями.

84. За таких умов цей орган не діє незалежно, що є абсолютно необхідним, особливо тому, що обробка даних вестиметься як в приватному, так і в державному секторі, зокрема стосовно спецслужб.

85. Ця вимога щодо незалежної роботи добре прописана в статті 1 додаткового протоколу Конвенції №108 і в статті 28.1 Директиви ЄС.

86. Складові незалежності, які повинні бути передбачені в законодавстві, як це встановлено в Паризькій угоді Організації Об'єднаних Націй про органи із захисту прав людини 1991 року, зазвичай включають принаймні наступне

- Механізм призначення (чи за моделі однієї особи, чи за колегіальної моделі), що забезпечує компетентність і незалежність. Це може включати в себе на практиці, наприклад, публічне звернення до кандидата та журі, роль парламенту як у низці європейських країн;
- Несумісність з виконанням державних функцій
- Фіксований період дії мандату;
- Суворе визначення випадків зняття з посади,
- Організаційну та бюджетну автономію (свободу щодо набору персоналу, відсутність контролю за фінансами апріорі, фінансовий контроль компетентним органом з роботи з державними організаціями за результатами діяльності). Сума бюджету такого органу повинна бути достатньо для його ефективної роботи. (Зверніть увагу, що обробка персональних даних розвивається величезними темпами, постійно відбувається технічна еволюція, а також розвиваються міжнародні зв'язки);
- Відкритий звіт про діяльність, включаючи рекомендації.

87. Ще одна проблема, пов'язана зі сферою повноважень органу, - втручання до обробки даних, які заявлені до реєстрації, як я коментувала вище.

88. Третя проблема пов'язана з дією адміністративних наказів у разі порушень (Якщо я вірно розуміла, орган має таке повноваження). Чи може таке рішення бути оскаржене в суді? Як це зазвичай передбачене для адміністративного рішення, а також в Директиві ЄС (стаття 28.3) та у додатковому протоколі Ради Європи (стаття 1.4).

89. Нарешті, такий державний орган повинен працювати прозоро. Зокрема, його річний звіт повинен публікуватися (стаття 28.5). На даний час передбачено, що він передається тільки міністру юстиції. Чи він також передається і представляється Уповноваженому у парламенті з прав людини? У деяких європейських країнах річний звіт представляється главі держави і парламенту.

"Інші органи державної влади та місцевого самоврядування, повноваження яких охоплюють питання захисту персональних даних", передбачені в статтях 4 та інших статтях, зокрема 8.2

90. Я так розумію, що окрім центрального Державного органу з питань захисту даних інші національні органи влади можуть також мати компетенцію щодо захисту даних, наприклад органи банківського нагляду, як уже передбачено в Законі. І що, згідно з конституцією, національне законодавство може передавати конкретні обов'язки національних органів органам місцевого самоврядування.

91. Ці інституційні механізми піднімають наступні питання.

1) Хоча з деяких питань захисту даних може здатися ефективним консультуватися зі спеціалізованими контролюючими органами, що мають компетенцію у певних секторах, очевидно, що надання повноважень із захисту даних різним секторним органам пов'язане з багатьма ризиками для впровадження послідовної політики. Саме тому в європейських країнах, які експериментували з такими підходами, від такої тенденції відмовилися. Тільки в федеративних державах, де існує чіткий поділ сфер компетенції, встановлений подвійний рівень органів з питань захисту даних, який в будь-якому разі потребує координації.
2) Втручання органів місцевого самоврядування до захисту даних викликає питання щодо незалежності та координації.
92. Хоча у великій країні (де більш ніж 45 мільйонів жителів), безумовно, логічно шукати варіанти місцевих компетентних органів ближче до громадян і володільців, я рекомендую взяти до уваги варіант національного незалежного органу, компетентного з усіх питань захисту даних, що має місцеві представництва з певних питань.

Суд: засоби захисту прав суб'єктів даних і санкції за порушення Закону
93. Стаття 32 Конституції передбачає виплату компенсації за матеріальний і моральний збиток, але тільки в результаті надання недостовірної інформації.

"Стаття 32 Конституції: "кожному гарантується судовий захист права виправити невірну інформацію про себе або себе та членів своєї сім'ї, і право вимагати, щоб будь-який тип інформації буде знята, а також право відшкодування матеріальної та моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації"
94. Але такі збитки можуть також виникати, якщо дані є достовірними, наприклад, коли дані використовуються для інших цілей, ніж ті, про які повідомили суб'єкта даних, або в разі навмисного або ненавмисного порушення правил безпеки. Та загалом у всіх випадках, коли відбувається порушення положень закону.

95. Стаття 8.7 Закону передбачає, що особи мають право на "на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи". А стаття 8.9 Закону передбачає право кожної людини на "застосування заходів правового захисту у разі порушення закону".

96. Ми розуміємо це так, але це потрібно уточнити, що ці права передбачають можливість подавати претензії як державним органам, відповідальним за захист даних, так і до суду, зокрема, для отримання засобів захисту.

Адміністративна та кримінальна відповідальність
97. Закон про внесення змін (від 2 червня 2011 року) щодо відповідальності за порушення законодавства про захист персональних даних прийнятий на виконання статті 28 Закону та передбачає санкції шляхом посилання на додаткові статті у Кодексі про адміністративні правопорушення та Кримінальному кодексі.

98. Адміністративні стягнення або "amercements (штрафи?)" – статті 188-39 і 188-40 Кодексу про адміністративні правопорушення впроваджуються для низки порушень вимог: повідомлення суб'єкта даних, повідомлення про бази даних Державному органу з питань захисту даних, недотримання норм захисту даних, що призвело до неправомірного доступу до баз даних, невиконання законних вимог, встановлених Державним органом з питань захисту даних. Повторення таких дій призводить до зростання штрафів.

99. Дивно, чому адміністративні покарання обмежені таким невеликим переліком порушень Закону та Положення.

100. Кримінальне покарання, передбачене додатковою статтею 182 Кримінального кодексу, пов'язане з операціями з незаконної обробки персональних даних або незаконною зміною персональних даних. Також передбачені виключення для "випадків, передбачених іншими статтями Кодексу".

101. Хоча, здавалося б, цим охоплені всі види порушень Закону, не знаючи, що це за "випадки", нам не представляється можливим оцінити це положення.

102. Стаття 182 також передбачає посилене покарання у випадку повторних дій та у разі нанесення істотної шкоди правам, що охороняються законом. Це положення є доцільним.

Парламентський уповноважений з прав людини

103. Стаття 22.2 Закону визначає, що контрольні повноваження парламенту реалізуються через парламентського уповноваженого з прав людини.

104. У мене не було можливості більше дізнатися про обсяги контрольних повноважень та практику діяльності парламенту та парламентського уповноваженого з прав людини, зокрема, за новими законами, які застосовуються потенційно у всіх видах діяльності та передбачають втручання спеціалізованого державного органу.

105. Утім, очевидно, що парламент повинен бути добре обізнаний про сферу ІТ та її звязок із правами людини, а також з багатьма видами соціальної діяльності, що трансформуються або виникають у зв'язку з використанням ІТ. Така еволюція вимагає розвитку економічної, технічної і законодавчої політики. Таму я б порекомендувала передбачити тісні прямі інституційні відносини між Державним органом з питань захисту даних і парламентом в цілому і на рівні різних зацікавлених парламентських комісій. Я б порекомендувала, зокрема, щоб будь-яка думка Управління із питань захисту даних щодо законопроектів та його річна доповідь публікувалися та представлялися на розгляд парламенту.

ГРЕХЕМ САТТОН

Експертний висновок до Закону України «Про захист персональних даних»

ВСТУП

1. Цей документ містить спостереження стосовно сумісності Закону України «Про захист персональних даних» (Закону) та спорідненого законодавства з Конвенцією Ради Європи від 1981 року про захист осіб у зв'язку з автоматизованою обробкою персональних даних (Конвенція) та Додатковим Протоколом до цієї Конвенції (Додатковий Протокол). Споріднене законодавство:
    - Закон України «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних»;
    - Постанова про затвердження Положення про Державний реєстр баз персональних даних та порядок його ведення;
    - Положення про Державну службу України з питань захисту персональних даних.

    У своїх спостереженнях стосовно відповідних положень Закону я паралельно розглядаю споріднене законодавство.

2. В роботі над спостереженнями я працював з Законом у перекладі на англійську мову, який був мені надісланий 19 грудня 2011 року, та спорідненого законодавства в перекладі на англійську мову, який був мені надісланий 22 листопада 2011 року. Що до технічних аспектів захисту даних, в перекладі не завжди є можливість передати точне значення оригіналу. Тому в деяких моментах це може означати, що спостереження, наведені в цьому документі, не відображають належним чином текст закону в оригіналі.

3. Працюючи над спостереженнями, я також брав до уваги Директиву ЄС від 1995 року про захист осіб у зв'язку з автоматизованою обробкою персональних даних та про вільний рух таких даних (Директива 95/46/ЕС) (Директива). Утім, у тих випадках, коли Конвенція та Директива містять аналогічне положення, я посилаюся лише на Конвенцію. Я посилаюся на Директиву лише тоді, коли нею доповнюються положення Конвенції. Я здебільшого надаю коментарі лише до тих положень законодавства, які, на мою думку, викликають запитання у зв'язку з сумісністю цього законодавства з зазначеними міжнародними інструментами. Водночас, я також надаю зауваження до деяких положень, які, на мій погляд, можна було б доопрацювати навіть за відсутності до них запитань стосовно сумісності.

4. В цьому документі наведені лише мої власні спостереження, і їх не слід сприймати такими, що представляють погляди Ради Європи або будь-якої іншої особи.

ЗАГАЛЬНІ ПОЛОЖЕННЯ

5. Перед тим, як приступати до коментарів стосовно окремих положень Закону, я вважаю, що маю зазначити два загальних моменти. По-перше, я не думаю, що Закон буде легко виконувати. Частково це може пояснюватися тим, що я

працював з перекладом, а не з оригіналом тексту. Зокрема, мені було важко зрозуміти деякі мовні звороти у тексті. Однак, я також вважаю, що і структура Закону збиває з пантелику. Деякі теми розглядаються в різних статтях в різних місцях у Законі. Як приклад - питання розголошення третім особам. Також у деяких випадках в Законі з'являються непослідовні положення. У своїх деталізованих спостереженнях, наприклад, я звертаю увагу на збіг та вочевидь взаємну несумісність понять "*обробка*" та *використання*". Інший приклад – непослідовність положення, яким передбачаються обмеження.

6. Другий момент не передбачається жорстко рамками мого технічного завдання, але я вважаю його суттєвим і сподіваюся, що мені пробачать такий відступ. Захист даних передбачає встановлення балансу між потребою захистити персональну інформацію особи та потребою з боку організацій використовувати таку інформацію в законних цілях. Країни, які вперше прописують у законі захист даних, мають тенденцію припускатися помилок, схиляючись у бік захисту осіб. Хоча в теорії це й добре для таких осіб, але якщо не встановити такий баланс належним чином, це може призвести до серйозних наслідків для тих, кому потрібно обробляти персональну інформацію з метою надання послуг, від яких залежать сучасні технічно розвинені суспільства, та якими користуються окремі особи. Теперішній Закон містить низку положень, які є дуже суворими, та які, на мою думку, можуть створювати серйозні перешкоди на шляху намагання володільців даних здійснювати свою законну діяльність. Ось, наприклад, цілком зрозумілий приклад, коли на згоду особи покладаються, як чи не на єдину підставу для обробки персональних даних. Ця складність ще посилюється тим фактом, що згода має завжди надаватися у письмовій формі. Інший приклад – відсутність у Законі положення статті 5.b Конвенції, яким дозволяється подальша обробка персональних даних у цілях, які не є несумісними з первинною метою, для якої і збиралися дані. Це вельми корисне положення додає гнучкості цьому комплексному напрямкові закону. Плюс до інших міркувань, якщо законом про захист даних будуть запроваджені такі моменти, які володільці можуть розглядати як обмеження, що унеможливлюють їх діяльність, існує реальна небезпека того, що закон може ігноруватися, а отже, не буде і захисту осіб, як такого.

ПОГЛИБЛЕНІ СПОСТЕРЕЖЕННЯ

Стаття 1: Сфера дії Закону

7. У першому пункті цієї статті стверджується: "*Цей Закон регулює відносини, пов'язані із захистом персональних даних під час їх обробки.* " Я не розумію цього речення. Зокрема, я не розумію значення слова "*відносини*" (яке частенько використовується в Законі). При цьому я розумію цей параграф як загальне положення, зміст якого полягає в тому, що мета цього Закону – розглянути порядок захисту даних. Як на мене, він не сприймається таким, що визначає сферу застосування Закону. Тут я маю на увазі, що він не встановлює, на яку саме обробку персональних даних поширюється дія цього Закону. За цим необхідно звернутися до статті 5.

8. Хоча у статті 1 не уточнюється, на яку обробку поширюється дія цього Закону, у ній наводиться певна діяльність у зв'язку з обробкою, на яку не поширюється дія Закону. У другому параграфі цієї статті передбачається обмеження на три категорії обробки на Закон в цілому.

9. Перше обмеження охоплює обробку "*фізичною особою - виключно для непрофесійних особистих чи побутових потреб*." Мета цього положення наводить на думку про відповідність обмеженню, наведеному у статті 3.2 Директиви з питань обробки "*фізичною особою у ході суто особистої чи побутової діяльності.*" Відповідність Закону Директиві в цьому відношенні знаходиться під питанням, оскільки "непрофесійні" та "особисті" мають не однакове значення. Особа може обробляти персональні дані в цілях, що не мають нічого спільного з професійною діяльністю, але при цьому це буде стосуватися діяльності, яка не буде суто особистою.

10. Друге та третє обмеження поширюються на обробку у зв'язку з професійною діяльністю – відповідно "*журналістами"* та "*професійними творчими працівниками*". Цими обмеженнями, вірогідно, мали на меті відобразити статтю 9 Директиви. Однак, належним чином це зробити не вдалося.

11. Одна з проблем полягає в тому, що обмеження в Законі надаються певним категоріям осіб, тоді як обмеження в Директиві поширюються на певні категорії діяльності. Згідно з Директивою, обмеження стосуються будь-якої особи (безвідносно до того, чи є ця особа фахівцем у даній галузі, чи ні), яка обробляє персональні дані в цілях журналістики або художнього чи літературного вираження. Згідно з Законом, обмеження поширюються лише на фахівців. Це розрізнення має значення у зв'язку з тим, що обмеження в Директиві мають на меті пошук балансу між приватністю та свободою вираження. Закон не досягає такого балансу, якщо говорити про «непрофесіоналів». Крім того, посилання на "працівників" у другому обмеженні створює ще навіть вужчу категорію осіб, які з такого обмеження отримують користь, оскільки з нього виключені професійні творчі працівники, які працюють на себе, і не є працівниками.

12. Положення цього Закону також суперечать Директиві в такому відношенні:
    - Вони передбачають обмеження до Закону в цілому, а не до визначених положень, як це відбувається в Директиві;
    - Посилання на "*професійних творчих працівників*" спірно охоплює ширшу діяльність, аніж термін "*в цілях художнього або літературного вираження*" – а саме такий термін застосовується в Директиві;
    - Обмеження, передбачені в Законі, є абсолютними та всупереч вимогам Директиви виходять за рамки обставин, за яких виникає конфлікт між приватністю та свободою вираження.

Стаття 2: Визначення термінів

13. "*Володілець бази даних*": це визначення встановлює осіб, які відповідають за обробку персональних даних. Однак, воно обмежує таких осіб тими, яким "*...за законом або за згодою суб'єкта персональних даних надано право на обробку цих даних...*". Далі зазначається, що особи, яким не надано таке право, не вважаються володільцями в цілях Закону. Це означає, що вони не зобов'язуються тими положеннями Закону, в яких висуваються вимоги до володільців, або які впливають на них іншим чином. Аналогічний момент виникає у статті 4.

14. "*Згода суб'єкта даних*": це визначення не містить вимогу стосовно того, що згода має бути «поінформованою». Це - один з критеріїв чинності згоди, який ми знаходимо у відповідному визначенні у статті 2(h) Директиви. До того ж, визначення в Законі вимагає, щоб згода на обробку персональних даних завжди оформлялася письмово. Це обтяжлива умова, і завжди виконувати її на практиці може виявитися складно.

15. "*Обробка персональних даних*": це визначення в широкому сенсі відповідає відповідному визначенню у статті 2(b) Директиви шляхом надання переліку дій з персональними даними, з яких складається обробка. Однак, цей перелік не такий всеосяжний, як у Директиві. Також, на відміну від визначення, наведеного в Директиві, яке містить відкритий перелік у такому значенні, що будь-яка не згадана дія також вважається «обробкою», перелік у визначенні Закону є закритим. Це означає, що обробка складається лише з даних конкретно визначених дій, в силу чого будь-які не згадані у визначенні дії, що здійснюються з персональними даними, Законом не охоплюються.

16. "*Розпорядник"*: це визначення передбачає, що розпорядникові право обробляти персональні дані може бути надане або володільцем, або він може мати «*право*» обробляти персональні дані "*відповідно до закону"*. У другому випадку незрозуміло, чим же відрізняється розпорядник від володільця, оскільки у визначенні володільця також сказано, що володілець може отримати право обробляти персональні дані "*відповідно до закону"*.

17. Далі виникає проблема відносин між володільцями та розпорядниками за Законом. В силу Директиви розпорядник має право діяти лише за інструкціями володільця, з яким він уклав договір, і (окрім випадків наявності домовленостей щодо безпеки) відповідальність за дотримання закону покладається на володільця, а не на розпорядника. Проте, декілька статей Закону передбачають, що розпорядники або діють незалежно від володільців, або розпорядникам надається такий же статус, як і володільцям. Наприклад, у другому підпункті другого пункту статті 15 Закону передбачається, що розпорядник може мати правовідносини з суб'єктом даних незалежно від володільця. Дозвіл на таку незалежну дію ще більше розмиває відмінності між володільцями та розпорядниками.

<u>Стаття 4:</u> Суб'єкти відносин, пов'язаних із персональними даними

18. Я не розумію ані вислову "*Суб'єкти відносин, пов'язаних із персональними даними*" у заголовку до цієї статті, ані вислову "*відносин, пов'язаних із персональними даними*" у першому пункті статті 4.

19. Перелік "*суб'єктів, пов'язаних з персональними даним*", наведений у першому пункті статті 4, дуже широкий; він охоплює суб'єктів даних, орган нагляду, а також володільців, розпорядників, третіх осіб, яким можна повідомляти персональні дані. Не розумію, навіщо в Законі охоплювати всіх цих різнорідних суб'єктів права єдиною фразою.

20. У другому пункті статті 4 наведений перелік суб'єктів, які мають право бути володільцем або розпорядником. У ньому сказано, що володільцем чи розпорядником бази персональних даних можуть бути суб'єкти права, які обробляють персональні дані "*відповідно до закону*". Як уже зазначалося відносно використання аналогічної термінології у визначенні терміну «володілець», вживання таких слів звужує сферу застосування Закону. Суб'єкти права, які обробляють персональні дані іншим чином, аніж "*відповідно до закону*", не можуть бути володільцями і, відповідно, не зобов'язані положеннями Закону, дія яких поширюється на володільців.

<u>Стаття 5: Об'єкти захисту</u>

21. Стаття 5 містить важливе положення, оскільки воно фактично визначає діапазон обробки даних, на який поширюється дія Закону.

22. Заголовок до статті звучить так: "Об'єкти захисту". Припускаю, що закладене у цих словах значення мало на меті визначення категорій персональних даних, яким Закон забезпечує відповідний захист. У першому пункті статті 5 зазначається: "*Об'єктами захисту є персональні дані, які обробляються в базах персональних даних*." Я так розумію, це означає, що Закон забезпечує захист персональних даних, *«які обробляються в базах персональних даних»*. Стаття 2 визначає «базу персональних даних» як " *…іменовану сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних.*" (Я бачив альтернативний переклад Закону, в якому була примітка, і в ній сказано, що термін "*картотека*" відноситься до порядку обробки персональних даних в ручному режимі. В перекладі, з яким я маю справу, такої примітки немає, але я так розумію, ці слова означають дані, з якими працюють в ручному режимі.) Разом ці положення складають враження, що дія Закону поширюється лише на персональні дані, які обробляються або в електронній формі, або у формі картотек. В результаті, складається враження, що обробка персональних даних, яка не належить до цих способів, не підлягає захисту, передбаченому в цьому Законі.

23. Що до обробки персональних даних в електронній формі, це означає, що Закон суперечить Конвенції або Директиві, дія яких поширюється на автоматизовану обробку персональних даних, а не лише на персональні дані, які зберігаються в базах даних. Що стосується обліку в формі картотек, це не суперечить Конвенції, оскільки в ній немає прямого посилання на те, що її дія поширюється саме на картотеку, що дозволяє сторонам до Конвенції застосовувати правила до таких картотек за власним бажанням. Дія Директиви поширюється на обробку персональних даних, які зберігаються у певних ретельно визначених системах зберігання документів. Хоча Закон і не дає визначення терміну «картотека», сфера його застосування, ймовірно, узгоджується з Директивою в даному аспекті.

24. Другий пункт статті 5 зазначає, що персональні дані вважаються "*інформацією з обмеженим доступом* ". Я розумію це, як наявність обмежень доступу до персональних даних третіх осіб, як-от наприклад, що персональні дані не дозволяється вільно оприлюднювати або повідомляти третім особам; та що для такого оприлюднення або повідомлення повинні виконуватися правила, встановлені Законом. Це, звісно, нормальний статус для персональних даних в рамках законів про захист даних навіть за умови відсутності положення такого роду.

25. Пункт 3 статті 5 передбачає відступ від пункту 2 статті 5, передбачаючи, що Законом може не дозволятися віднесення персональних даних певних категорій громадян до «*інформації з обмеженим доступом»*. У пункті 4 статті 5 міститься таке уточнення стосовно осіб, які претендують обійняти чи обіймають певні державні посади, хоча й передбачається положення про те, що певна персональна інформація підпадає під категорію інформації з обмеженим доступом.

26. Мене непокоять два моменти стосовно цих відступів. По-перше, моє прочитання відповідних положень припускає, що дія відступів полягає не лише в тому, щоб забезпечити вільне надання інформації про даних осіб. Радше, дія полягає в тому, що інформація взагалі не вважатиметься персональними даними, а отже, вона в цілому виводиться з-під захисту Закону. Оскільки другий пункт статті 5 зазначає, що персональні дані – це "*інформація з обмеженим доступом*", інформація, зазначена як така, що <u>не</u> має обмеженого доступу, вже за визначенням не належить до персональних даних, а отже – знаходиться поза межами сфери застосування Закону.

27. По-друге, навіть якщо дія цих положень полягає в тому, щоби просто призупинити дію обмеження доступу, а не відступати від застосування Закону в цілому, мені цікаво, чи виправдане визначення в такий спосіб цілих категорій осіб. Адже може мати місце такий випадок, коли дозволяється оприлюднення або інші форми необмеженого доступу до певної інформації про певних осіб за певних обставин. Можна навести приклад оприлюднення відповідної інформації

про кандидата на виборну посаду (що й передбачається в четвертому пункті статті 5). Між тим, у Законі немає застережень, якими б обмежувалися обставини, які можуть приводити в дію цей відступ. На мій погляд, цей відступ трактується неприйнятно широко. Як один з варіантів, можна було б усунути ці положення з тексту та дозволити принципам захисту даних визначати обставини, за яких персональні дані можна повідомляти. З іншого боку, до цієї статті можна було б внести застереження, якими обмежуватимуться обставини, на які поширюється дія відступів.

Стаття 6: Загальні вимоги до обробки персональних даних

28. Стаття 6 розглядає те, що зазвичай називають «принципами захисту даних». В ній також прописуються засади законної обробки персональних даних. Я, в свою чергу, розгляну кожну з цих тем.

Принципи захисту даних

29. Принципи захисту даних, які ми знаходимо в статті 5 Конвенції, встановлюють основні правила поводження з персональними даними та є одним з основних структурних елементів будь-якого режиму захисту даних. Це має центральне значення для ефективності режиму захисту даних, який встановлюється Законом, а отже, і принципи слід цілком внести до складу Закону. Для зручності я наведу кожне положення статті 5 Конвенції, перш ніж коментувати, як вони набувають чинності у Законі.

Конвенція про захист даних: стаття 5

Персональні дані, що піддаються автоматизованій обробці, повинні
a. отримуватися та оброблятися справедливо та законно

30. Питання законності обробки не прописується конкретно в статті 6 Закону. Однак, як зазначалося вище, ця стаття насправді визначає засади, на яких можуть законно оброблятися персональні дані. Відсутність конкретного посилання на законність означає, між тим, що обробка, яка порушує який-небудь інший закон, не стане порушенням закону про захист даних єдино з цієї причини.

31. Відсутнє однозначне посилання на те, що обробка має бути справедливою.

b. зберігатися для визначених і законних цілей та не використовуватися в спосіб, не сумісний із цими цілями

32. Пункт перший статті 6 вимагає "*чітко сформульованої*" в законах або інших документах, які регулюють діяльність володільця, мети обробляння персональних даних. Не розумію значення цього положення. Одним з можливих значень може бути те, що жодному володільцеві не дозволяється

обробляти персональні дані з метою, не прописаною в законодавчих або інших формах нормативно-правового інструменту. Якщо таке тлумачення правильне, то воно, здається, має відношення до вимоги Конвенції щодо «*законності*» мети обробки. Утім, мені цікаво, наскільки реалістичне це положення. Зокрема, чи справді в Україні приватний сектор може здійснювати лише таку діяльність, що конкретно дозволяється законодавчими або іншими нормативно-правовими інструментами? Дія Закону поширюється на осіб, які обробляють персональні дані. Якою мірою їх діяльність в якості володільців даних може визначатися в такий спосіб?

33. Перша частина п'ятого пункту статті 6 Закону також звертається до першої частини статті 5.b Конвенції: у ній вимагається здійснення обробки персональних даних "*для конкретних і законних цілей"*. Однак, я не розумію зв'язку між першим пунктом статті 6 та другою частиною п'ятого пункту статті 6, якою вимагається згода особи на визначену ціль обробки персональних даних суб'єктів, крім "*випадків, передбачених законами України, у порядку, встановленому законодавством* ". Прочитання цих двох положень разом припускає, що особи можуть надавати згоду лише на цілі, передбачені законодавчими або іншими нормативно-правовими інструментами. Це логічно узгоджується. Однак, навіщо тоді потрібен виняток? Не може ж такого бути, що він там є, щоб дозволити обробку (на противагу визначенню цілі) без згоди, оскільки це передбачається в шостому пункті статті 6.

34. Стаття 6 не містить положення, яке б відповідало статті 5.b Конвенції, пов'язаної з несумісним використанням. Це важливе положення дає володільцям певну міру гнучкості у поводженні з персональними даними. Якщо володільці зібрали дані з однією метою, це положення дозволяє їм обробляти персональні дані з іншою метою за умови, що така друга мета не є «несумісною» з першою метою. Вона також дозволяє володільцям розголошувати персональні дані за умови проходження тесту на несумісність. Друге речення першого пункту статті 6 розглядає питання зміни цілі, вимагаючи надання суб'єктом даних згоди в кожному випадку. В іншому місці в Законі передбачене окреме положення стосовно розголошення персональних даних. Хоча таке окреме положення може додавати гарантії безпеки, я вважаю, що відсутність гнучкості, яка забезпечується тестом на не несумісність, може виявитися зайве жорсткою.

с. бути адекватними, відповідними та ненадмірними стосовно цілей, для яких вони зберігаються;

35. Перше речення третього пункту статті 6 вимагає "*відповідного та ненадмірного" с*кладу та змісту персональних даних. Воно не вимагає, щоб дані були адекватними. Вимога щодо адекватності має важливе значення,

оскільки дані хоча й можуть бути відповідними, якщо вони не є адекватними для даної цілі, це може в результаті призвести до поганих рішень, які можуть мати серйозний вплив на суб'єкта даних.

d. бути точними та в разі необхідності оновлюватися

36. Це передбачається другим пунктом статті 6.

e. зберігатись у формі, яка дозволяє ідентифікацію суб'єктів даних не довше, ніж це необхідно для мети, для якої такі дані зберігаються

37. Це передбачається восьмим пунктом статті 6.

Підстави для обробки

38. Як зазначалося вище, Закон не містить загальної однозначної вимоги щодо неодмінної законності обробки персональних даних. Утім, як у статті 6, так і в статті 11 передбачаються певні умови, які повинні бути дотримані, перш ніж дозволяється обробка персональних даних. Ці умови ефективно встановлюють підстави для законної обробки. Конвенція не встановлює докладно наведених підстав для обробки. Вона покладається на загальну вимогу неодмінної законності обробки. Водночас, Директива у сьомій статті передбачає шість підстав для обробки. У Законі передбачаються дуже жорсткі підстави для обробки. Вони, по суті, обмежуються згодою суб'єкта даних (яка, за визначенням цього терміну, яке надається у статті 2, повинна надаватися в письмовому вигляді) з декількома винятками.

39. Пункт шостий статті 6 Закону забороняє обробку персональних даних без згоди особи. Передбачається один виняток до вимоги про надання згоди у випадках, визначених законом, але лише "*... в інтересах національної безпеки, економічного добробуту та прав людини.*" Наголос на згоді, яка є головною (насправді, практично єдиною) підставою для обробки, лунає:
    - У другому реченні першого пункту статті 6, у якому говориться, що у разі зміни мети обробки, від особи знову вимагається згода;
    - У другому реченні третього пункту статті 6, яке вимагає згоду особи на зміст її персональних даних, які зберігаються в базах даних;
    - У п'ятому пункті статті 6, який вимагає згоду осіб на мету обробки їх персональних даних, крім "*випадків, передбачених законами України"*.

40. За пунктом сьомим статті 6, якщо обробка персональних даних є необхідною для захисту життєво важливих інтересів особи, обробляти персональні дані без її згоди можна до того часу, коли отримання згоди стане можливим.

41. У підсумку, єдиною підставою для обробки персональних даних є згода особи, окрім тих випадків, коли за обмежених обставин цим Законом або іншими

законами України передбачається інше, або коли при обробці йдеться про захист життєво важливих інтересів особи. Обмеження підстав для обробки в такий спосіб безперечно, надійно захищає. Однак, воно викликає запитання стосовно того, чи достатньо воно гнучке, щоб дозволити всіляку законну обробку персональних даних, необхідну для ефективного функціонування сучасних технічно розвинених суспільств. Як уже згадувалося, Директива визнає необхідність шести підстав для обробки, з яких однією є згода особи, а іншою – захист життєво важливих інтересів особи. Було би дивно, якби і Закон також не потребував такої ж чималої гнучкості, яка закладена в Директиві.

42. Також виникає питання щодо того, чи є достатньо широкими винятки, що передбачені в пункті шостому статті 6. Зокрема, може виникати необхідність здійснювати обробку без згоди у тих випадках, коли потрібно захистити самих суб'єктів даних та права і свободи інших, як передбачається у статті 9.2.b Конвенції. Це може бути у випадку, коли подія потрапляє під виняток "прав людини". Однак, тінь сумніву на таке тлумачення кидає перший пункт статті 25, яким передбачаються певні відступи від певних інших положень Закону. Підстави для відступів, визначених у першому підпункті до першого пункту статті 25, повторюють закладені в шостому пункті статті 6. Однак, підстави у другому підпункті першого пункту статті 25 чітко передбачають необхідність захищати права і свободи суб'єкта даних та інших осіб, а от у даному положенні цього немає.

Інші положення статті 6

43. Четвертий пункт статті 6 звертається до того, що він називає "*первинними джерелами відомостей про фізичну особу*". Я не розумію, яку ціль переслідує це положення. Його можна тлумачити так, ніби він вимагає, щоб усі персональні дані збиралися з таких "*первинних джерел*" і ні з жодних інших. Якщо це й мали на увазі, то така вимога дуже жорстка, і на практиці може бути важко її виконувати.

44. Дев'ятий пункт статті 6 звертається до обробки в історичних, статистичних чи наукових цілях. В ньому сказано, що будь-які персональні дані в таких цілях повинні використовуватися "*у знеособленому вигляді*". Це звучить невиправдано суворою вимогою, оскільки інколи з цією метою виникає потреба обробити інформацію про тих, чия особа встановлюється.

Стаття 7: Особливі вимоги до обробки персональних даних

45. У цій статті йдеться про загальновідомі так звані чутливі дані. Першим пунктом статті 7 забороняється обробка даних в категоріях, які надаються в переліку. Перелік містить більшість категорій конфіденційних даних, передбачених статтею 6 Конвенції, і додатково інформацію про членство у профспілках, яку

ми бачимо в першому пункті статті 8 Директиви. Однак, інформація, що стосується засудження в кримінальному порядку, відсутня.

46. Конвенція просто вимагає відповідних застережень при обробці конфіденційних даних. Директива приймає різні підходи та визначає обставини, за яких може відбуватися обробка таких даних. Закон в широкому сенсі відповідає Директиві, прописуючи в другому пункті статті 7 ті обставини, за яких не застосовуються положення першого пункту статті 7. Перелік обставин нібито відтворює модель статті 8 Директиви, хоча й присутні деякі відмінності.

47. Перший підпункт до другого пункту статті 7 дозволяє обробку конфіденційних даних за умови "*однозначної*" згоди особи. Незрозуміло, що саме тут означає "*однозначна*". Визначення "згоди" у статті 2 вимагає, щоби згода завжди була письмовою. Важко встановити, як сюди вписується "*однозначна*".

48. Другий підпункт другого пункту статті 7 узгоджується в широкому сенсі зі статтею 8.2(b) Директив, якою дозволяється обробляти конфіденційні дані для певних цілей закону про працю. Утім, положення Закону набагато ширше, ніж аналогічне в Директиві, і в ньому не вистачає вимоги про правові гарантії.

49. Підпункт третій другого пункту статті 7 дозволяє обробку конфіденційних даних в "*інтересах*" суб'єкта даних або іншої особи у разі недієздатності суб'єкта даних. Це відрізняється від відповідного положення Директиви (Стаття 8.2(c)), яке обмежується обробкою у "*життєво важливих інтересах*".

50. Підпункт четвертий другого пункту статті 7 відповідає статті 8.2(d) Директиви, яка стосується питань обробки певними некомерційними організаціями. Він відрізняється від Директиви тим, що не вимагає, щоб організація була неприбутковою; обмежується організаціями, створеними відповідно до закону (таким чином, виключаються всі добровільні організації); і в ньому відсутнє посилання на гарантії.

51. Шостий підпункт другого пункту статті 7 розглядає обробку в цілях охорони здоров'я та відповідає статті 8.3 Директиви. Сфера його застосування вужча, ніж у Директиви, оскільки тут не охоплюється медичний діагноз або забезпечення медичного обслуговування. Директива вимагає поширювати на осіб, які здійснюють обробку, зобов'язання стосовно збереження професійної таємниці. Закон не містить такої вимоги. В ньому просто сказано, що на заклад охорони здоров'я, до якого належать особи, які здійснюють обробку, покладається "*відповідальність за забезпечення захисту даних*". Не розумію, що означає цей вираз.

52. Сьомий підпункт другого пункту статті 7 усуває заборону на обробку персональних даних у випадку обвинувачення у вчиненні злочину та в аналогічних випадках. Однак, як уже зазначалося вище, перелік категорій

конфіденційних даних, наведений у першому пункті статті 7 - а отже, й заборона на обробку, не охоплює такі дані. Таким чином, ця заборона не має сили. Аби досягнути бажаного результату, треба було б або додати цю категорію інформації до переліку, наведеного в першому пункті статті 7; або, як у статті 8.5 Директиви, визначити в окремому положенні обмежені обставини, за яких дозволяється обробляти такі дані. Крім того, щоб виконати вимоги Директиви, було б необхідно як мінімум визначити, що обробку даних, про яку йде мова, дозволяється здійснювати лише "*під контролем уповноваженого органу*" та додати вимогу про конкретні гарантії.

53. На відміну від статті 8 Директиви, Закон не містить дуже корисного положення, яким дозволяються подальші обмеження до заборони на обробку конфіденційних даних, які будуть передбачатися або в національному законодавстві, або прописані органом нагляду з питань захисту даних. Також він не містить положення, передбаченого у статті 8.7 Директиви, яке стосується умов обробки національних ідентифікаційних або аналогічних кодів.

Стаття 8: Права суб'єкта даних

54. Стаття 8 розглядає права суб'єкта даних. Жодного відповідного положення не містить ні Конвенція, ні Директива.

55. У деяких випадках Закон наділяє осіб такими правами, які вимагають дій від інших осіб, але Законом на інших осіб не покладається обов'язок вчиняти необхідну дію. Приклади бачимо частково у першому, другому, четвертому підпунктах до другого пункту статті 8 та в сьомому підпункті. Я вважаю, що для того, щоб зробити права особи ефективними, слід покласти на відповідну особу – як правило, це володілець – обов'язок, який забезпечить їх чинність.

56. Перший підпункт другого пункту статті 8 передбачає право суб'єкта даних "знати" певну інформацію. Можливо, цим мали на меті відобразити статтю 8.а Конвенції, яка передбачає аналогічне (якщо не ідентичне) положення в тому, що стосується характеру інформації. Однак, Конвенція вимагає доступності інформації будь-якій особі, а не лише суб'єктові даних. Окрім іншого, Закон стверджує, що суб'єкти даних мають право знати найменування та місцезнаходження володільця "*чи розпорядника*". Оскільки саме володілець, а не розпорядник несе правову відповідальність за обробку, інформація про володільця повинна надаватися завжди. Аналогічний момент виникає і у шостому підпункті другого пункту статті 8.

57. Одне з найважливіших прав захисту даних – право суб'єкта на доступ. Це, схоже, і зазначається у третьому підпункті другого пункту статті 8, в якому стверджується, що суб'єкт даних має право "*на доступ до своїх даних*". Аналогічне положення передбачається у четвертому підпункті другого пункту статті 8, в якому стверджується, що суб'єкт даних має право "*отримувати*

зміст своїх персональних даних". Як співвідносяться ці положення, я не розумію. У четвертому пункті статті 12 виникає положення, схоже на повторне формулювання права: воно вимагає надання даних про персональні дані суб'єкта на вимогу суб'єкта. Утім, це може читатися і як обов'язок володільця надавати інформацію.

58. Стаття 8 охоплює не всі права, які ми знаходимо в положеннях статті 12 Директиви про право суб'єкта на доступ. Однак, два загублені положення статті 12 Директиви заходимо в іншому місці Закону. Четвертий пункт статті 12 Закону вимагає надання інформації про джерело персональних даних; а третій пункт статті Стаття 21 охоплює право суб'єктів даних вимагати від володільців повідомляти третім особам, яким надавалися дані про персональні дані суб'єкта, про будь-які зміни в їх даних.

59. П'ятим підпунктом другого пункту статті 8 суб'єктам даних надається право пред'являти вимогу із запереченням проти обробки своїх персональних даних органами державної влади. Це положення, схоже, має відношення до статті 14(a) Директиви, якою передбачається можливість для суб'єктів даних заперечувати проти обробки своїх персональних даних за певних обставин. Водночас, Закон не розглядає статтю 14(b) Директиви, якою суб'єктам даних надається право пред'являти вимогу із запереченням проти обробки своїх персональних даних з метою прямого маркетингу.

60. Сьомим підпунктом другого пункту статті 8 суб'єктам даних надається право на захист своїх персональних даних від незаконної обробки та інших ризиків. Фактично, у ньому стверджується, що суб'єкти даних мають право на те, щоб їхні персональні дані перебували в безпеці. Конвенція вимагає "*належних заходів безпеки*" на захист від визначених ризиків у зв'язку з персональними даними. В Директиві закладене аналогічне положення, й вона зобов'язує володільців здійснення необхідних заходів. Заходи безпеки – суттєва складова ефективного захисту даних. Закон не містить положень з вимогами до володільців стосовно здійснення належних заходів безпеки персональних даних, які ними обробляються.

61. Хоча й у восьмому підпункті другого пункту статті 8 немає повної ясності, він, схоже, дозволяє суб'єктам даних звертатися до органів, що відповідають за забезпечення виконання цього Закону. Відсутнє чітке посилання на орган нагляду з питань захисту даних. Орган нагляду можна додати до "*органів державної влади*". Якщо ні, слід додати однозначне посилання.

62. Дев'ятий підпункт другого пункту статті 8 стверджує, що суб'єкти даних мають право *"...застосовувати засоби правового захисту..."* в разі порушення законодавства про захист персональних даних. Незрозуміло, що саме означає цей термін. Можливо, це означає, що суб'єкти даних мають право звертатися до судових механізмів захисту в разі порушення прав, що належать їм за

Законом. Якщо це не так, слід додати відповідне положення згідно з вимогами статті 8.d. В Законі також слід чітко окреслити, що згідно з вимогами статті 23 Директиви, суб'єкти даних мають право вимагати компенсацію будь-яких збитків, понесених ними в результаті незаконної обробки їх персональних даних.

Стаття 9: Реєстрація баз персональних даних

Положення про Державний реєстр баз персональних даних та порядок його ведення

63. Стаття 9 розглядає питання реєстрації органом нагляду з питань захисту персональних даних. Положення доповнює статтю 9, надаючи докладнішу інформацію про порядок реєстрації.

64. Конвенція не розглядає питання реєстрації. Директива у статтях 18 – 21 містить положення про порядок "*повідомлення*" - саме так він у ній іменується, який насправді і є порядком реєстрації.

65. Стаття 19 Директиви визначає інформацію, яку володільці даних повинні надавати органові нагляду в порядку повідомлення. Цей порядок розглядається в третьому пункті статті 9 Закону та пункті 7 Положення. Стаття 19.1(a) Директиви вимагає наявності положення про найменування та адресу володільця. Стаття 9 у третьому пункті Закону просто передбачає надання «*інформації*» про володільця. Пункт 7 Положення наводить розширений перелік обсягів інформації, яку вимагається надавати про володільця. Схоже, до обсягу цієї інформації не входить адреса володільця. Але присутня вимога про надання інформації стосовно фактичного місцезнаходження «*баз персональних даних*» для баз даних у формі картотек, фактичної адреси зберігання носіїв інформації для баз даних в електронній формі. Це може розглядатися як аналог адреси володільця, хоча й вельми ускладнений. В будь-якому разі, він не обов'язково встановлює юридичну адресу володільця, оскільки фактичну обробку можуть здійснювати один та більше розпорядників.

66. Стаття 19.1(b) Директиви вимагає надання інформації стосовно мети обробки. Хоча це згадується в третьому пункті статті 19 Закону, в Положенні немає окремої вимоги щодо мети обробки. Утім, у тій частині сьомого пункту Положення, в якій іде мова про місцезнаходження «*електронних баз*», є посилання і на «мету». Може статися, це посилання на мету мали намір визначити окремою вимогою, а ці два положення опинилися поруч помилково в англійському перекладі. Аналогічний момент виникає відносно надання інформації про категорії персональних даних, які обробляються, що також вимагається Директивою. Знову ж таки, в третьому пункті статті 9 Закону посилання на це немає, але "*категорії*" згадуються мимохіть у тій же частині сьомого пункту Положення.

67. Стаття 19.1 Директиви також вимагає надання наступної інформації, жодна з яких не з'являється в третьому пункті статті 9 Закону або положення:
    - Інформація про суб'єктів даних;
    - Інформація про отримувачів, яким можуть розкриватися дані;
    - Інформація про пропоновану передачу даних до третіх країн;
    - Загальний виклад заходів безпеки.

68. За винятком відомостей про безпеку, другий пункт статті 21 Директиви вимагає внесення всієї інформації, яка повідомляється володільцями за першим пунктом статті 19 Директиви, в реєстр, відкритий для громадян. Стаття 9 Закону не згадує про відкритість реєстру для громадян. Утім, здається, це питання розкривається в пунктах 14 - 16 Положення (хоча я не розумію, навіщо потрібні всі три положення).

69. Стаття 8.2.Конвенції вимагає надання будь-якій особі можливості з'ясувати, чи здійснюється обробка персональних даних, її мету та «*постійне місце проживання чи головне місце роботи»* розпорядника. Для країн, в яких запроваджений порядок реєстрації, централізований реєстр, відкритий для громадян, забезпечує зручний спосіб виконання цієї вимоги. Це може поширюватися і на Україну. Однак, як уже зазначалося вище, інформація, яка за вимогою Закону та Положення має надаватися володільцем з метою реєстрації, не обов'язково містить відповідні відомості стосовно адреси володільця.

Стаття 10: Використання персональних даних

70. Перший пункт статті 10 надає визначення "*використання персональних даних*". Я не розумію, навіщо потрібен цей термін. За винятком згадки про надання права на обробку персональних даних, незрозуміло, в чому сфера застосування цього терміну відрізняється від "*обробки*". Перший пункт статті 10 стверджує, що він передбачає будь-які дії володільця бази у зв'язку з обробкою персональних даних. Однак, у визначенні терміну "*обробка*" у статті 2 стверджується, що до поняття "*обробка*" входить поняття "*використання*". Отже, визначення одного терміну містить поняття іншого у своїй сфері застосування. Це збиває з пантелику.

71. Незрозуміле друге речення статті 10. Якщо моє прочитання правильне, то, здається, ним запроваджується повна заборона розголошення персональних даних третім особам. Якщо це так, то як же це положення ув'язується з порядком розголошення третім особам, передбаченим далі в Законі (статті 14, 16 - 19)?

Стаття 11: Підстави виникнення права на використання персональних даних

72. Стаття 11.1 передбачає підстави обробки персональних даних. Як я зазначав, стаття 6 також містить такі підстави. Важко зрозуміти зв'язок між шостою статтею та першим пунктом статті 11 у цьому відношенні.

73. Стаття 6 стверджує, що обробка персональних даних може здійснюватися
    - За згодою особи;
    - Відповідно до законодавства, але лише "*...в інтересах національної безпеки, економічного добробуту та прав людини*";
    - Якщо обробка персональних даних необхідна для захисту життєво важливих інтересів особи, але лише протягом обмеженого періоду часу.

74. Перший підпункт першого пункту статті 11 стверджує, що обробка персональних даних може здійснюватися за згодою суб'єкта даних. Це відповідає статті 6 (хоча перший підпункт першого пункту статті 11 далі визначає, що суб'єкт даних має право «*внести застереження*» стосовно обмеження обсягу обробки).

75. Другий підпункт першого пункту статті 11 дозволяє обробку відповідно до закону, але не містить обмежень, наданих у статті 6. Винятки, передбачені у статті 25, звернені до статті 11, але вони ширші, ніж дозволені статтею 6. Плюс до того, другий підпункт першого пункту статті 11 стверджує, що законом володільцю лише дозволяється обробляти персональні дані «*виключно для здійснення його повноважень»*. Такого роду обмеження не знаходимо у статті 6.

76. На відміну від статті 6, перший пункт статті 11 не передбачає захист життєво важливих інтересів особи у зв'язку з обробкою.

Стаття 12: Збирання персональних даних

77. Конвенція не містить докладно розписаних положень у зв'язку зі збиранням персональних даних. Вона просто вимагає, щоб збирання було справедливим та законним. Статті 10, 11 Директиви розвивають далі ідею справедливості, визначаючи, що особам, персональні дані яких збираються, повинна надаватися певна інформація. Стаття 12 Закону, схоже, передбачає аналогічну мету.

78. Я не розумію першого пункту статті 12. Не розумію значення слів "*передбачає дії*".

79. Другий пункт статті 12 вимагає надання особі певної інформації в письмовому вигляді протягом десяти днів з дня включення його персональних даних до бази персональних даних. Вимога про надання інформації в письмовому вигляді в усіх випадках виглядає надмірною, особливо коли на відміну від

Директиви Закон вимагає надання інформації навіть тоді, коли суб'єкт даних уже її має.

80. Інформація, яка надається, містить відомості про права суб'єкта даних, осіб, які збирали дані та мету збирання. Було б краще та ближче до Директиви, якби суб'єктам даних повідомляли про особу володільця, а не тих осіб, які збирали дані. Закон не відповідає Директиві ще й у тому, що не передбачає надання додаткової інформації у тих випадках, коли це виявляється необхідним для забезпечення справедливості обробки.

81. Третій пункт статті 12 - повідомлення не відбувається, якщо персональні дані збираються із «*загальнодоступних джерел»*. Директива не передбачає такого винятку.

82. Четвертий пункт статті 12 вимагає надання суб'єктові даних певної інформації на прохання. Заключна частина статті передбачає виняток у випадках, установлених законом. Припускаю, що це має відношення до права на встановлення обмежень, передбачених у статті 25. Однак, у статті 25 не зазначається таке поширення дії на статтю 12.

Стаття 13: Накопичення та зберігання персональних даних

83. Я не розумію цієї статті. Що до застосування аналогічної фрази в першому пункті статті 12, значення слів *"передбачає дії"* незрозуміле.

Стаття 14: Поширення персональних даних

84. Значення першого пункту статті 14, в якому знову використовується вислів *"передбачає дії"*, незрозуміле. Припускаю, що загальна суть даного пункту полягає в тому, що персональні дані не повинні розголошуватися без (письмової) згоди суб'єкта даних. Якщо це так, то це дуже сувора вимога, яка може стати на заваді багатьох законних заходів у зв'язку з обробкою персональних даних. Для надання чинної згоди суб'єктові даних потрібно буде повідомляти про кожне заплановане повідомлення і питатися, чи дає він свою згоду. Це дуже трудомісткий, витратний процес на предмет часу та коштів. На мій погляд, було б краще дозволити більшу гнучкість, яку можна забезпечити, якщо до статті 6 внести положення, відповідне другій частині статті 5.b Конвенції. Це дозволило б володільцям розкривати дані за умови, що це "*не є несумісним*", з метою збору даних, та й іншим чином задовольнило б принципи захисту даних.

85. Другий пункт статті 14 передбачає виняток до вимоги про згоду у першому пункті статті 14, але лише "*в інтересах національної безпеки, економічного добробуту та прав людини* ". Як і в аналогічному положенні шостого пункту статті 6, відсутній виняток з метою забезпечення захисту суб'єкта даних або

прав та свобод інших осіб, або з метою недопущення кримінальних правопорушень, що й передбачається у статті 9 Конвенції.

Стаття 15: Знищення персональних даних

86. Стаття 15 встановлює порядок знищення персональних даних. Другий підпункт другого пункту статті 15 стверджує, що персональні дані підлягають знищенню у разі припинення правовідносин між суб'єктом персональних даних та «*володільцем чи розпорядником*». Правову відповідальність за обробку слід покладати лише на володільця. Розпорядник має право діяти лише за інструкцією володільця , і йому не слід вступати в окремі правові відносини з суб'єктом даних. Рішення про знищення персональних даних (як і всі рішення у зв'язку з обробкою персональних даних) мають прийматися володільцем.
87. Стаття не передбачає винятків до обов'язку знищення персональних даних. За деяких обставин може виникати необхідність збереження персональних даних після настання терміну знищення: наприклад, у тому випадку, коли персональні дані виступають доказом. Принципи захисту даних вимагають зберігання даних не довше, аніж потрібно. Однак, Конвенцією допускаються винятки до принципів захисту даних на підставах, аналогічних тим, що визначені у статті 25 Закону.

Стаття 16: Порядок доступу до персональних даних
Стаття 17: Відстрочення або відмова у доступі до персональних даних
Стаття 18: Оскарження рішення про відстрочення або відмову в доступі до персональних даних
Стаття 19: Оплата доступу до персональних даних

88. Якщо я правильно розумію цю групу статей, вони розглядають порядок повідомлення персональних даних третім особам. Я так розумію, що їх потрібно читати у в одному рядку зі статтею 10, якою передбачається "*використання*" (включно з повідомленням) персональних даних, та статтею 14, якою передбачаються підстави для повідомлення. Далі у статті 21 йдеться про надання повідомлення суб'єктам даних у випадках розкриття їх персональних даних. Мені складно розібратися в тому, як усі ці положення пов'язуються одне з одним.

89. Я вже коментував з приводу принципів надання згоди, як підстави для повідомлення персональних даних третім особам, у своїх спостереженнях до статті 14. Звертаю увагу на те, що порядок, який встановлюється цією групою статей, доволі складний. У цьому контексті я повторю зауваження, яке вже звучало вище, стосовно того, що для надання чинної згоди суб'єктові даних потрібно буде повідомляти про кожен окремий випадок розкриття його даних. Це означає, що порядок, передбачений у цих статтях, повинен буде застосовуватися у величезній кількості випадків. А якщо заглибитися в деталі,

то я не знайшов у цьому порядку будь-яких конкретних кроків у зв'язку з отриманням згоди суб'єкта даних.

90. Хоча ці статті, схоже, і розглядають питання повідомлення даних третім особам, вони, трапляється, посилаються на доступ суб'єктів даних. Наприклад, статті 16.6, 17.1, 18.2, 19.1. Хоча структура Закону не належить до тих питань, які я зазвичай коментую, відзначу, що якби положення про повідомлення третім сторонам відокремити від положень про доступ суб'єктів даних, це внесло б більшу ясність.

Стаття 20: Зміни і доповнення до персональних даних

91. Перший пункт статті 20 накладає обов'язок на "*володільців чи розпорядників баз даних*" вносити зміни до персональних даних на підставі вимоги суб'єкта даних. Це робити мають бути зобов'язані лише володільці. Як уже зазначалося, правова відповідальність за обробку має в цілому покладатися на володільців.

Стаття 21: Повідомлення про дії з персональними даними

92. Стаття 21 вимагає повідомлення суб'єктів даних за певних обставин про передачу персональних даних третім особам. Третій підпункт другого пункті статті 21 виняток до вимоги у разі "здійснення обробки персональних даних в історичних, статистичних чи наукових цілях *"*. Це, схоже, суперечить дев'ятому пункту статті 6, в якій передбачається обробка в таких цілях лише знеособлених даних.

Стаття 22: Контроль за додержанням законодавства про захист персональних даних

93. В першому пункті статті 22 передбачається здійснення контролю за додержанням законодавства про захист даних органом нагляду та "*іншими органами державної влади та органами місцевого самоврядування* ". Я розгляну питання органу нагляду далі. Що ж до інших органів, незрозуміло, чи мають вони незалежність згідно з вимогою статті 1 Додаткового Протоколу до Конвенції. Крім того, в Законі не прописуються відповідні напрямки компетенції органу нагляду з питань захисту персональних даних з одного боку, а з іншого - інших органів державної влади та органів місцевого самоврядування. Це може призвести до непорозуміння.

Стаття 23: Уповноважений державний орган з питань захисту персональних даних

Положення про Державну службу України з питань захисту персональних даних

94. Стаття 23 запроваджує орган нагляду з питань захисту персональних даних та встановлює його основні функції. Вони доповнюються положенням про Державну службу України з питань захисту персональних даних. У статті 23, як і деінде в Законі, цей наглядовий орган іменується уповноваженим державним органом з питань захисту персональних даних. У Положенні ж він іменується Державною службою з питань захисту персональних даних (ДСЗПД). Я так розумію, саме це і є його офіційна назва.

95. Загальновизнаним є той факт, що однією з найважливіших характерних ознак органу нагляду з питань захисту персональних даних має бути його повна незалежність. Незалежність суттєво необхідна для забезпечення безперечного виконання органами нагляду свого обов'язку контролювати та забезпечувати додержання законодавства про захист даних усіма організаціями, зобов'язаними Законом, включно з урядом. Стаття 1 Додаткового Протоколу до Конвенції розглядає органи нагляду з питань захисту даних. Третім пунктом вона вимагає від органів нагляду *"...виконання своїх функцій у цілковитій незалежності"*.

96. Перший пункт Положення чітко роз'яснює, що ДСЗПД – невід'ємна частина державного апарату. Тут сказано, що його діяльність *"...спрямовується і координується Кабінетом Міністрів України через Міністра юстиції України"*. Такий статус ДСЗПД як державного відомства ще посилюється декількома іншими умовами Положення. Відсутність незалежності органу нагляду – один із найсерйозніших недоліків цього Закону.

97. Я не знайшов жодного положення в Законі або Положенні, якими приводилася б у дію вимога, передбачена четвертим пунктом статті 1 Додаткового Протоколу стосовно того, що *"Ті рішення органів нагляду, які викликають скарги, можна оскаржувати в судах".*

98. Положення вимагає від органу нагляду надавати річний звіт Міністру юстиції. Між тим, я не знайшов положення з вимогою про оприлюднення такого звіту, а така вимога передбачається п'ятим пунктом статті 28 Директиви.

<u>Стаття 25: Обмеження дії окремих статей цього Закону</u>

99. У цій статті розглядаються відступи від певних положень Закону. Я вважаю, що положення про відступи в Законі збивають з пантелику.

100. Інші положення Закону (наприклад, підстави для обробки у шостому пункті статті 6; підстави для розголошення у статті 14) самі по собі містять відступи, але не такі об'ємні, як ті, що передбачені у статті 25. Не розумію, чому одні положення, на які поширюється дія статті 25 (а саме, передбачені статтями 8, 11, 17), мають право на широкі обмеження, наведені у статті 25, тоді як інші - ні.

101. До певних положень, де є потреба в обмеженнях (наприклад, принципи захисту даних у статті Стаття 6; обов'язок знищення персональних даних у статті 15), вони зовсім не передбачаються.

102. Певні положення (наприклад, обов'язок повідомляти суб'єктів даних у четвертому пункті статті 12) посилаються на обмеження, передбачені законодавством, але в жодному не прописується ані сфера застосування обмежень, ані посилання на поширення на них дії статті 25.

Стаття 28: Відповідальність за порушення законодавства про захист персональних даних

Закон України "Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних"

103. Стаття 28 по суті просто передбачає, що закон встановлює порядок вирішення питань порушення законодавства про захист даних. Визначення міри покарання за порушення певних положень законодавства про захист даних – задача закону, згаданого у заголовку вище (закон про посилення відповідальності). Цим законодавством визначаються зміни до Кодексу України про адміністративні правопорушення та Кримінального Кодексу України. Ці зміни передбачають міру відповідальності за порушення різноманітних положень Закону про захист даних. За адміністративні правопорушення передбачається покарання у вигляді, я так розумію, штрафних санкцій різного обсягу, зважаючи на відповідні обставини. Кримінальний Кодекс передбачає штрафи або позбавлення волі на певний термін. Важко з'ясувати, до яких положень Закону про захист даних відносяться різні міри відповідальності, оскільки положення не містять посилання на відповідну статтю.

Кодекс України про адміністративні правопорушення

Нова стаття 188-39

104. Ця нова стаття розглядає порушення вимог Закону про захист даних повідомляти суб'єкта даних про його права, мету збору їх даних та осіб, яким ці дані передаються. Я так розумію, що це положення пов'язане з вимогою повідомляти суб'єктів даних, передбаченою статтями 12.2 та 21.1 Закону про захист даних. Зверну увагу на те, що пункт другий статті 12 також вимагає (згідно з моїм прочитанням цього положення) повідомляти суб'єктів даних про особу, яка збирає персональні дані, а в новій статті про це не згадується.

105. Далі положення нової статті розглядають порушення вимог шостого пункту статті 9 Закону про захист даних стосовно повідомлення володільцями органу

нагляду з питань захисту даних про зміни в персональних даних у їх відомі; та вимог щодо реєстрації в органі нагляду за статтею 9.

106. І зрештою, ця стаття встановлює покарання за "н*едодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних у базі персональних даних, що призвело до незаконного доступу до них*". Незрозуміло, яких положень Закону про захист даних стосується цей пункт нової статті. Можливо, ним планувалося охопити положення статті 6, наприклад. Було б корисно уточнити сферу поширення дії нової статті. Якщо мали на увазі запровадження санкцій за порушення вимог статті 6 Закону про захист даних, незрозуміло, чому це положення нової статті обмежується порушенням норм, яке призводить до незаконного доступу, а не охоплює всю незаконну діяльність.

Стаття 188-40

107. Ця нова стаття передбачає міру відповідальності за невиконання законних інструкцій органу нагляду з питань захисту персональних даних.

Кримінальний Кодекс України

108. Ця зміна встановлює відповідальність за "*незаконний збір, зберігання, використання, знищення, розповсюдження конфіденційної інформації про особу або незаконне внесення змін в таку інформацію*". Це положення, схоже, охоплює сферою свого застосування більшість суттєвих положень закону про захист даних. Утім, незрозуміло, чи поширюється воно на принципи захисту даних, передбачені статтею 6. Я так розумію, що малося на увазі, що мало бути саме так. Цю позицію, можна було б легко уточнити, якби просто передбачити покарання усіх незаконних дій у зв'язку з незаконною обробкою персональних даних.

Загальні положення

109. Звертаю увагу на два істотних упущення в положеннях про міру відповідальності. По-перше, схоже на те, що положення стосовно прав суб'єктів даних відсутні. Я не знаходжу чіткого посилання на порушення прав, і недотримання прав, схоже, не розглядається в жодному іншому положенні. По-друге, можливо, через те, що сам Закон про захист прав не містить жодної однозначної вимоги до володільців про неодмінну безпеку персональних даних, і не передбачається покарання за недотримання вимоги щодо адекватної безпеки.

Стаття 29: Міжнародне співробітництво

110. Пункт третій статті 29, схоже, розглядає питанні передачі персональних даних з України до інших країн. (У цьому пункті отримувачів іменують "*іноземними*" суб'єктами, а не такими, що знаходяться в третіх країнах, але, я

так розумію, мали на увазі саме таке значення) Хоча формулювання цього пункту незрозуміле, основне правило, схоже, полягає в тому, що персональні дані можуть передаватися лише за умови забезпечення належного захисту персональних даних в третіх країнах, які їх отримують. Також передбачається вимога про наявність дозволу за певних обставин. Не розумію, за яких саме обставин потрібен дозвіл; до кого звертатися з вимогою про надання дозволу; та які існують підстави для відмови або надання дозволу. Є посилання, що це відбувається "*у порядку, встановленому законодавством*". Можливо, саме те законодавство, якого я не бачив, і розглядає порядок отримання дозволу на передачу до третіх країн. В останньому реченні цього пункту йдеться про те, що персональні дані не можуть "*поширюватися*" з іншою метою, ніж та, з якою вони були зібрані. Незрозуміло, що означає "*поширюватися*" в даному контексті. Якщо мали на увазі "передачу", то це дуже сувора вимога, оскільки не передбачає винятків та унеможливлює передачу навіть за умови наявності згоди суб'єкта даних.

ВИСНОВОК

Загальне положення

Закон важкий для виконання та містить деякі очевидні внутрішні суперечності. Деякі з його положень нереально жорсткі.

Основоположні проблеми

- Сфера застосування Закону, дія якого поширюється лише на обробку персональних даних, які містяться в базі даних, надто вузька, оскільки виключає інші види автоматизованої обробки. (Стаття 5)
- Принципи захисту даних статті 5 Конвенції не виконуються в повному обсязі. (Стаття 6)
- Закон передбачає права особи, але в деяких моментах не покладає на володільців обов'язок їх забезпечити. Передбачені не всі права, встановлені Конвенцією та Директивою. (Стаття 8)
- Орган нагляду не має незалежності від влади. (Стаття 23; Положення про орган нагляду)
- На володільців не покладається обов'язок здійснювати відповідні заходи безпеки.

Інші проблемні питання

- Обмеження на обробку особами, які діють не професійно, для журналістів та інших творчих працівників незадовільні. (Стаття 1)
- Відмінність володільців від розпорядників незрозуміла. В деяких аспектах, схоже, розпорядники можуть діяти незалежно від володільців. (Статті 2, 8, 15, 16, 20)
- Особи, які обробляють персональні дані іншим чином, аніж відповідно до закону, не вважаються володільцями. (Статті 2, 4)
- Визначення поняття "*згода*" неповне та дуже жорстке. (Стаття 2)

- Визначення поняття “*обробка*” не таке комплексне, як те, що надається в Директиві. (Стаття 2)
- Персональні дані кандидатів на виборну посаду, народних обранців та посадових осіб високого рангу вочевидь не охоплюються Законом. (Стаття 5)
- Вимога про те, що мета обробки має бути прописана в законах чи інших нормативних документах, дуже жорстка. (Стаття 6)
- Підстави для обробки дуже вузькі. Акцент на згоду, як на чи не єдину підставу для обробки, не реалістичний. (Статті 6, 11)
- Заборона обробки даних в історичних, статистичних чи наукових цілях нереалістична та внутрішньо непослідовна. (Статті 6, 21)
- Підстави для обробки конфіденційних даних суперечать передбаченим у статті 8 Директиви. Положення про обробку інформації у зв’язку з обвинуваченням у скоєнні злочину тощо не діє. (Стаття 7)
- Інформація, яка підлягає реєстрації в органі нагляду та вноситься в державний реєстр, вужча, аніж цього вимагає Директива. Вимога Конвенції стосовно того, що будь-яка особа повинна мати змогу з’ясовувати певні відомості стосовно обробки, не виконується належним чином. (Стаття 9; Положення про державний реєстр баз)
- Правила розкриття персональних даних третім особам незрозумілі. В деяких аспектах вони виявляються дуже жорсткими. (Статті 10, 14, 16 - 19, 21)
- Положення, якими визначається порядок повідомлення осіб, стосовно яких здійснюється збір даних, суперечать Директиві (Стаття 12).
- Відповідна сфера відповідальності визначеного органу нагляду та інших органів державної влади не зазначається. Незрозуміло, чи інші органи є незалежними у виконанні своїх функцій нагляду. (Стаття 22)
- Положення про обмеження суперечливе і в деяких аспектах надто вузьке. (Статті 25, 6, 8, 11, 12, 14, 15, 17)
- Відсутнє положення про оскарження в суді рішень органу нагляду чи про оприлюднення річного звіту органу нагляду. (Стаття 23; Положення про орган нагляду)
- Сфера застосування положень про міру відповідальності незрозуміла. Схоже, мають місце деякі упущення. (Стаття 28, Закон про правопорушення)
- Правила передачі персональних даних до третіх країн незрозумілі. (Стаття 29)

Грехем Саттон
Лондон
6 січня 2012 року