КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
імені ТАРАСА ШЕВЧЕНКА

На правах рукопису

ПАЗЮК Андрій Валерійович

УДК 342.721

МІЖНАРОДНО-ПРАВОВИЙ ЗАХИСТ ПРАВА ЛЮДИНИ НА ПРИВАТНІСТЬ ПЕРСОНІФІКОВАНОЇ ІНФОРМАЦІЇ

Спеціальність: 12.00.11 – міжнародне право

Дисертація на здобуття наукового ступеня кандидата юридичних наук

Науковий керівник
ЗАДОРОЖНІЙ Олександр Вікторович
кандидат юридичних наук, доцент

КИЇВ–2004

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Значний прогрес у розвитку засобів автоматизованої обробки даних у двадцятому столітті і пов'язане з ним збільшення обсягів і напрямків використання персоніфікованої інформації у різних сферах суспільного життя, її передача через кордони новітніми комунікаційними засобами викликає необхідність належного правового регулювання відносин з використання персоніфікованої інформації як для забезпечення прав і свобод людини, так і ефективної реалізації правомірних інтересів інших осіб і держави. На даний момент часу гостро відчувається потреба в науковому узагальнені чинних норм міжнародного і національного права, здобутків правової думки у цій галузі з метою визначення основних елементів і особливостей міжнародно-правового захисту права людини на приватність персоніфікованої інформації.

Комплексне дослідження проблеми міжнародно-правового регулювання відносин, що виникають у зв'язку з обробкою (збиранням, зберіганням, використанням, поширенням) персоніфікованої інформації, є необхідним також для запровадження адекватного правового механізму в правову систему України, який гарантував би правомірне поводження з персоніфікованою інформацією, без чого неможливо забезпечити ефективну реалізацію гарантованого статтею 31 Конституції України права громадян на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції, а також проголошеного у статті 32 Конституції України права на невтручання у приватне і сімейне життя.

З іншого боку, невідповідність національних правових положень у цій галузі міжнародно-правовим стандартам загрожує застосуванням обмежень на передачу персоніфікованої інформації громадян інших країн до України, а це матиме негативні політичні й економічні наслідки для держави і вітчизняних суб'єктів господарювання, створюватиме перешкоди для міжнародного співробітництва у багатьох сферах

(зокрема, в питаннях боротьби із злочинністю), де відбувається міжнародний обмін персоніфікованою інформацією.

Актуальність теми дослідження обумовлюється також недостатнім ступенем її наукової розробки в доктрині міжнародного права. В українській науці доволі активно розвивається теорія міжнародно-правового захисту прав людини, досліджуються питання реформування правової системи України у відповідності з міжнародно-правовими стандартами, зокрема, в працях М.М. Антонович, М.В. Буроменського, В.Г. Буткевича, В.Н. Денисова, А.І. Дмитрієва, А.С. Довгерта, В.К. Забігайла, Л.Г. Заблоцької, О.В. Задорожнього, А.С. Мацка, В.І. Муравйова, П.М. Рабиновича, Л.Д. Тимченка, Ю.М. Тодики, С.В. Шевчука, Ю.С. Шемшученка.

Однак специфічним питанням міжнародно-правового захисту права людини на приватність персоніфікованої інформації приділяється незначна увага. В кращому випадку розглядаються окремі аспекти проблеми (у працях О.А. Баранова, Ю.К. Бабанова, В.М. Брижка, Т.А. Костецької, О.О. Мережка, К.Б. Полінкевич, В.О. Серьогіна та інших). В західній правовій науці над згаданими питаннями працювали Ф. Агре, К. Беннетт, Л.Д. Брендейс, Д. Боркін, С.Д. Воррен, С.Г. Дейвіс, Р. Кларк, В. Котші, М.Д. Кьорбі, Майер-Шонбергер, В.Л. Проссер, Ч.Д. Рааб, М. Ротенберг, Д.Х. Флехерті та інші. Російські дослідники присвятили цій проблематиці декілька наукових розробок, найбільш помітними з яких є праці І.М. Гостева, В.П. Іванського, Ю.М. Колосова, В.А. Копилова, Б.В.Кристального, І.С. Мелюхіна, М.Є. Петросяна, Н.Н. Разумовича, В.І. Ярочкіна.

Відсутність ґрунтовних досліджень окреслених питань в українській науці міжнародного права ускладнює процес пошуку адекватної моделі національного механізму регулювання відносин з використання персоніфікованої інформації, узгодженої з міжнародно-правовими стандартами, яка гарантувала би ефективний захист прав і свобод громадян України.

Зв'язок роботи з науковими програмами, планами, темами. Дослідження виконане в рамках наукового проекту Комплексної державної програми науково-дослідницької роботи Київського національного університету імені Тараса Шевченка "Розбудова державності України 1996-2005 рр.", планової наукової теми Інституту

міжнародних відносин Київського національного університету імені Тараса Шевченка “Розробка міжнародних правових, політичних та економічних основ розбудови Української Держави” № 97128, а також наукової теми відділення міжнародного права Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка “Міжнародно-правові основи зміцнення державності України” № 97132.

Мета і завдання дослідження. Метою дослідження є комплексний аналіз міжнародно-правових актів, законодавства країн англосаксонської і континентальної правових сімей, законодавства України, доктрини і судової практики щодо забезпечення реалізації і захисту права людини на приватність персоніфікованої інформації. У дисертації подається теоретичне узагальнення здобутків науки міжнародного права з цієї проблеми й нове вирішення наукового завдання, що полягає у з’ясуванні особливостей міжнародно-правового захисту права людини на приватність персоніфікованої інформації і узгодження національних підходів до проблеми транскордонної передачі цієї інформації, визначенні мінімального стандарту правового регулювання обробки персоніфікованої інформації для подальшої розробки науково-теоретичних та практичних рекомендацій з удосконалення законодавства України.

Для досягнення поставленої мети в дослідженні поставлено такі **завдання**:

- виявити причини, що обумовлюють необхідність міжнародно-правового захисту права людини на приватність персоніфікованої інформації;
- визначити нормативний зміст права людини на приватність персоніфікованої інформації, підстави і умови його легітимного обмеження;
- охарактеризувати сукупність міжнародно-правових норм, якими регулюються відносини щодо реалізації і захисту права на приватність персоніфікованої інформації, і визначити їх місце в системі міжнародного права;
- виявити існуючі мінімальні стандарти міжнародно-правового захисту приватності й безперешкодної передачі персоніфікованої інформації через державні кордони;

- розробити науково обґрунтовані пропозиції щодо вдосконалення законодавства України з урахуванням вимог міжнародних документів, досвіду демократичних країн для ефективного забезпечення прав громадян під час обробки персоніфікованої інформації.

Об'єктом дослідження є юридичний механізм реалізації основних прав і свобод людини, зокрема, права на приватність персоніфікованої інформації.

Предметом дослідження є міжнародно-правові акти та національне законодавство різних країн, доктрина і судова практика щодо забезпечення реалізації і захисту права людини на приватність персоніфікованої інформації.

Методи дослідження. Під час дослідження широко використовувався історико-правовий метод для вивчення генезису та еволюції правового регулювання обробки персоніфікованої інформації, формально-юридичний метод під час вивчення міжнародно-правових стандартів захисту права на приватність, а також порівняльно-правовий метод у ході аналізу національних нормативно-правових актів різних країн та міжнародно-правових документів. У роботі використовувалися й інші наукові методи пізнання, властиві як загальній теорії права, так і науці міжнародного права.

Наукова новизна одержаних результатів полягає у тому, що в українській науці міжнародного права вперше проведене системне дослідження сучасної міжнародно-правової основи реалізації і захисту права людини на приватність персоніфікованої інформації. Наукові положення, що найбільшою мірою відбивають новизну дослідження, зводяться до наступного:

1. В роботі встановлено, що необхідність належного міжнародно-правового захисту прав людини у зв'язку з використанням та передачею персоніфікованої інформації обумовлюється особливостями цього виду інформації, який відображає індивідуальність людини як носія певних елементів фізичної, фізіологічної, психічної, економічної, культурної або соціальної тотожності, що породжує ризик її неправомірного використання на шкоду інтересам людини, зокрема, втручання у приватне життя.

2. Визначено, що сукупність міжнародно-правових норм, якими регулюються відносини з міжнародно-правового захисту приватності персоніфікованої інформації,

становлять міжнародно-правовий інститут. Встановлено особливість предмету регулювання цього інституту, яка полягає у подвійній функціональності: захист права людини на приватність та забезпечення безперешкодності транскордонної передачі персоніфікованої інформації.

3. З'ясовано, що право на приватність персоніфікованої інформації становить складову права на повагу до приватного життя, а не права на доступ до інформації. Специфіка захисту приватності персоніфікованої інформації обумовлюється необхідністю забезпечення конкуруючих інтересів людини у захисті від несанкціонованого розголошення чи іншого використання персоніфікованої інформації без її відома, а також інтересів держави та інших осіб у використанні персоніфікованої інформації. Це право не є абсолютним і підлягає пропорційному обмеженню на визначених законом підставах, в інтересах забезпечення свободи слова, боротьби із злочинністю тощо.

4. Встановлено, що відсутність загальновизнаних універсальних стандартів міжнародно-правового захисту персоніфікованої інформації обумовлюється розбіжностями у концептуальних підходах до захисту права на приватність персоніфікованої інформації на національному рівні, зокрема, в законодавстві Європейського Союзу та Сполучених Штатів Америки.

5. Встановлено, що правове регулювання відносин з використання персоніфікованої інформації в праві Європейського Союзу ґрунтується на стандартах Ради Європи, носить системний характер і соціально-захисну орієнтацію.

6. З'ясовано, що міжнародна договірна модель забезпечення безперешкодності транскордонної передачі персоніфікованої інформації є одним із шляхів розв'язання проблеми узгодження розбіжностей в національних правових підходах (зокрема, між Європейським Союзом і США), яка, однак, не вирішує її повною мірою внаслідок обмеженості сфери застосування.

7. Доведено, що чинне законодавство України з питань захисту приватності персоніфікованої інформації не відповідає міжнародно-правовим стандартам у цій сфері. З метою запровадження європейської (соціально-захисної) моделі в Україні необхідно врегулювання відповідних правових відносин шляхом ухвалення закону,

який би ґрунтувався на положеннях Конвенції Ради Європи № 108 “Про захист осіб стосовно автоматизованої обробки персональних даних” 1981 року та Директиви Європейського Союзу № 95/46/ЕС 1995 року, враховував би досвід провідних європейських держав.

Теоретичне і практичне значення одержаних результатів. Проведене дослідження міжнародно-правового захисту права на приватність персоніфікованої інформації має сприяти більш глибокому розумінню сучасного стану міжнародного регулювання відносин щодо захисту приватності та безперешкодної транскордонної передачі персоніфікованої інформації, перспектив його подальшого розвитку, а також шляхів удосконалення чинного законодавства України.

Результати дослідження, теоретичні розробки й висновки можуть бути використані в навчальному процесі при викладенні курсів із правових дисциплін (“Міжнародне публічне право”, спецкурсів “Міжнародне право у галузі захисту прав людини”, “Європейське право у галузі прав людини” тощо), а також у науково-дослідних і прикладних цілях для подальшої розробки й удосконалення національних нормативно-правових положень і міжнародно-правових стандартів поводження з персоніфікованою інформацією, міжнародно-правових засобів узгодження розбіжностей у національних підходах для забезпечення безперешкодної транскордонної передачі даних. Сформульовані практичні пропозиції були використані під час підготовки проекту Закону Верховної Ради України “Про інформацію персонального характеру” (реєстраційний № 7432 від 12.11.2001 р.) робочою групою, до складу якої входив здобувач.

Апробація результатів дослідження здійснювалась у виступах на міжнародних конференціях і семінарах:

- міжнародній науково-практичній конференції “Європа-Японія-Україна: шляхи демократизації державно-правових систем” (м. Київ, 17-20 жовтня 2000 року), матеріали опубліковані;
- міжнародному семінарі “Впровадження міжнародних стандартів захисту даних у законодавство України”, організованому Комітетом Верховної Ради України з питань правової політики за участю експертів Ради Європи, ОБСЄ (м. Київ, 17-18

грудня 2001 року), на якому автор брав участь у якості експерта Комітету Верховної Ради України з питань правової політики;

- міжнародному симпозіумі “Свобода інформації та захист даних: транспарентність і електронне урядування в Центральній та Східній Європі” (м. Потсдам, Німеччина, 10-11 листопада 2003 року).

Публікації. Основні положення, теоретичні висновки і практичні рекомендації, що містяться у дисертації, викладені автором у 10 наукових публікаціях, у тому числі у 6 наукових статтях у фахових виданнях, 1 тезах виступу на науковій конференції, а також трьох монографіях.

Структура дослідження зумовлена метою та завданнями дослідження, логікою викладення. Дисертаційна робота складається зі вступу, трьох розділів, якими охоплюється дев’ять підрозділів, висновків до розділів, узагальненого висновку та списку використаних джерел. Загальний обсяг дисертації 205 сторінок, у тому числі 29 сторінок – список використаних джерел (312 найменувань).

РОЗДІЛ 1
МІЖНАРОДНО-ПРАВОВИЙ ЗАХИСТ ПРИВАТНОСТІ ПЕРСОНІФІКОВАНОЇ ІНФОРМАЦІЇ: ЗАГАЛЬНОТЕОРЕТИЧНІ Й ІСТОРИЧНІ ОСНОВИ

Питання міжнародного захисту прав людини не є новими для сучасної науки міжнародного права. Однак буде перебільшенням вважати їх такими, що однозначно вирішені на теоретичному й практичному рівнях. Значною мірою це стосується питання правового захисту від втручання у приватне життя осіб шляхом неправомірного поводження з персоніфікованою інформацією, що вбачається надзвичайно актуальним з огляду на стрімкий розвиток інформаційних технологій і поширення транскордонних інформаційних обмінів. Пов'язана з цим проблема належного міжнародно-правового забезпечення прав людини у зв'язку з використанням персоніфікованої інформації потребує ґрунтовного дослідження, яке, насамперед, вимагає вивчення загальнотеоретичних основ проблеми та її історичних аспектів.

У першому розділі дослідження ставиться завдання розглянути особливості правового забезпечення реалізації та захисту права людини на приватність персоніфікованої інформації, зробити огляд розвитку наукової думки у цьому напрямку з тим, щоб виявити питання, які потребують додаткового вивчення (підрозділ 1.1); дослідити розвиток на теоретичному й нормативному рівнях концепцій захисту права на приватність, підстав і умов його легітимного обмеження, зокрема, в інтересах реалізації свободи вираження поглядів, а також під час правоохоронної діяльності (підрозділ 1.2); охарактеризувати сукупність чинних міжнародно-правових норм, якими забезпечується захист права на приватність персоніфікованої інформації (підрозділ 1.3).

1.1. Приватність персоніфікованої інформації як об’єкт правового захисту

Що таке персоніфікована інформація? Якою є правова природа відносин, предметом яких є персоніфікована інформація? Чим обумовлюється особливість правового регулювання відносин щодо використання персоніфікованої інформації? Відповідь на ці запитання неможливо дати без з’ясування поняття “персоніфікована інформація”, яке є видовим стосовно поняття “інформація”.

З точки зору соціально-філософської концепції, поняття *інформація* нерозривно пов’язано з категорією відображення. За визначенням, яке пропонує представниця української науки Н. Джинчарадзе, “інформація – це найвищий, найскладніший результат впорядкованого відображення у вигляді повідомлень, знань, відомостей про природу, суспільство, в цілому про об’єктивну реальність, які охоплюють усі сфери людської діяльності, використовуються в процесі спілкування, управління, виробництва, пізнання, творчості, виховання, освіти тощо” [[1], *9*]. Розглядаючи сутність зв’язку відображення та інформації, вона дійшла висновку, що інформація може розглядатися як діалектична єдність поновлення різноманітності і як її обмеження. Ми поділяємо цю думку, оскільки вона зосереджується на основній функції інформації – давати уявлення (інформувати) про об’єкт, відображаючи його властивості.

Персоніфікована інформація є різновидом інформації, яка відображає як індивідуальність окремої особи, так і її загальнолюдські біологічні й соціальні властивості. Персоніфікована інформація відображає людську різноманітність, індивідуальність кожної людини як носія унікальних елементів фізичної, фізіологічної, психічної, економічної, культурної або соціальної тотожності. Отже, визначальною ознакою персоніфікованої інформації є її індивідуалізований характер, здатність ідентифікувати конкретну особу за допомогою тих чи інших критеріїв. Під час такої ідентифікації відбувається процес *персоніфікації* тих чи інших відомостей, тобто прив’язування їх до конкретної людини. Інформація, яка ідентифікує

(ототожнює), дозволяє безпосередньо або за допомогою інших чинників ідентифікувати особу, є *персоніфікованою інформацією*. Разом із тим, відомості (як документовані, так і в усному вигляді) є формою відображення біологічної й соціальної тотожності, а також індивідуальності кожної людини. У свою чергу, для позначення відомостей про особу, які вже зазнали певної обробки людиною, зафіксовані на певному носії, упорядковані, і придатні для автоматизованої обробки, цілком виправданим є вживання терміна "персональні дані" (**лат.** *personalitas* – особистість).

Науково-технічний прогрес спричинився до актуалізації правового захисту приватності персоніфікованої інформації від раніше невідомих ризиків життю, здоров'ю, репутації, добробуту людини внаслідок неправомірного збирання й використання персоніфікованої інформації, тобто від небажаного вторгнення у внутрішню сферу життя людини, яка охороняється правом на повагу до приватного життя.

Неправомірне збирання, використання й поширення персоніфікованої інформації завдає шкоду сформованому суспільством уявленню про індивіда, його соціальній "масці". Джерелом такого уявлення є інформація, яку індивід явно чи не явно демонструє суспільству. Це не тільки біографічні дані, як-то прізвище, ім'я, по батькові, дата і місце народження особи, національність, релігійні, політичні чи філософські переконання, освіта, місця навчання і роботи, відомості про сімейний стан, наявність дітей, ставлення до військової служби. До персоніфікованої інформації також належать відомості про матеріально-фінансовий стан (банківські рахунки, платежі по них, нерухоме та рухоме майно, майнові права), стан здоров'я, особисті стосунки приватного характеру та багато інших відомостей в матеріальній формі у різних сферах суспільного життя, які створюються, збираються, зберігаються, поширюються та використовуються в інший спосіб як з відома особи – суб'єкта даних, так і без її відома. Ця інформація дозволяє суспільству оцінювати людину як індивідуальність, формувати її репутацію (**лат.** *reputatio* – оцінка). Вона також може бути використана для заподіяння особі шкоди.

Якщо іще півстоліття тому для здобуття інформації про людину необхідно було витратити значні зусилля, сучасний рівень розвитку технологій дозволяє здійснити обробку даних про тисячі людей за лічені секунди і без надмірних витрат. Феномен "відчуження" людини від персоніфікованої інформації покладено в основу конструкції "цифрова особа" (*digital persona* – **англ.**), моделі публічного прообразу особи, яка базується на персональних даних і підтримується під час контактів і покликана виступити в ролі представника індивіда. Найпростішим технічним засобом, що використовує таку конструкцію, є звичайний телефонний автовідповідач. На думку австралійського вченого Р. Кларка, модель "цифрової особи" дозволяє особі самостійно її конструювати, визначаючи, яка інформація і яким чином буде використовуватися, тим самим залишати контроль за своїм "цифровим" прообразом [[2], *7*].

Це перетворюється на певну проблему, якщо "цифрова особа" створюється іншими особами, які мають у розпорядженні різні за обсягом і якістю дані про особистість, одержані з різних джерел і в різний час. Поєднання неточних чи застарілих персональних даних створюватиме спотворене уявлення про особу.

Практика створення цифрового образу особи набула поширення за допомогою, так званих, процедур "співставлення даних" (*data matching* – **англ.**), під час якої здійснюється збирання, співставлення й об'єднання персональних даних, які знаходяться у різних базах даних; а також "профілювання" (*profiling* – **англ.**) – створення профілю людини, сукупності характеристик особи за певними критеріями на підставі аналізу відомостей про особу з різних баз даних. Ці види таємного збору відомостей про особу отримали складноскорочену назву *"дейтавейленс"* (**англ.** *dataveillance*), що перекладається як "стеження за даними".

Можливості технічних засобів, що дозволяють збирати й обробляти персоніфіковану інформацію, постійно й стрімко розширюються; технології вдосконалюються, а ціна на них зменшується. Навіть за звичайними технологіями збору інформації значна кількість персональної інформації постійно збирається. У розвинутих країнах, де поширене використання платіжних карток для повсякденних грошових витрат, будь-яка платіжна операція, будь-то покупка, продаж чи

інвестування, створює сукупність персональних даних. Ця інформація використовується як із комерційною метою, так і для звітування перед фіскальними органами держави.

Певні соціальні ризики виникають у зв'язку з появою нових багатофункціональних кредитних карток із мікропроцесором (**англ.** *multi-function smart card*), так званих, "смарт-карток", які використовуються для ідентифікації особи у різних сферах суспільних відносин. Для вивчення таких ризиків і підготовки пропозицій щодо адекватного правового регулювання цих питань Міністерство юстиції Нідерландів сформувало робочу групу експертів, яка підготувала доповідь за назвою "Соціальні ризики використання смарт-карток" [3]. У ході дослідження експерти встановили 45 ризиків різного роду й важливості впродовж "життєвого" циклу таких карток. Серед найбільш важливих, ризики, які пов'язані з ідентифікацією особи й можливістю неправомірного використання персоніфікованої інформації. Питання захисту від "крадіжок ідентичності" є, серед іншого, одним із завдань Міжнародної організації поліції – Інтерполу [4].

Слід відзначити, що з точки зору безпеки особи та чи інша персоніфікована інформація має різний ступінь важливості для індивіда, що зумовлюється рівнем ризику заподіяння шкоди. Загроза неадекватного сприйняття оточуючими, дискримінації за якоюсь ознакою, іншого протиправного використання персоніфікованої інформації вимагає передбачення її потенційної "вразливості" для людини. Врахування інтересів особи і її суб'єктивного ставлення до тієї чи іншої інформації, яке неможливо повною мірою охопити в узагальнених нормативних приписах, вимагає законодавчого віднесення об'ємного переліку даних до категорії "вразливих даних" (про расове або етнічне походження чи національність, політичні погляди, релігійні або філософські переконання, членство у профспілках чи громадських організаціях, дані, які стосуються стану здоров'я чи надання медико-санітарної допомоги, сімейних і особистих стосунків приватного характеру чи статевого життя, відомості про кримінальні вчинки чи протиправну поведінку), а також надання особі права самостійно визначати межі циркуляції персоніфікованої інформації у суспільстві. Цим створюється територіальний простір, в якому особа

може контролювати межі своєї індивідуальності. Для ефективного захисту цього простору, особа повинна мати право сама окреслювати ці межі, тобто встановлювати яка персоніфікована інформація, для яких цілей, в якому обсязі і яким одержувачам може передаватися.

Такий підхід зумовлений тим, що тільки особа, якої стосується персоніфікована інформація може оцінити вразливість, тобто ймовірний ризик неправомірного використання такої інформації. Це становить основу суб'єктивного інтересу, який захищається відповідним суб'єктивним правом особи (яке не є абсолютним, а потребує узгодження з інтересами суспільства, що досліджується у наступних підрозділах цього дослідження), а також обумовлює й визначає особливості правової природи права на приватність персоніфікованої інформації.

На думку Р.Н. Мнукіна, необхідність автономії особи від свого соціального оточення послужила підставою для реалізації концепції розмежування приватної й публічної сфер активності людини [5]. Така форма соціальної "демаркації" є природною для розвитку сучасного суспільства, регулювання соціальної поведінки й усвідомлення такого феномена як "приватна сфера" життя людини.

У західній правовій доктрині для позначення цього правового інституту використовується термін "прайвесі" (**англ.** *privacy*). Найбільш вдалим його перекладом українською мовою, на нашу думку, є "приватність", яке походить від слова "приватний". Воно характеризує якісний стан об'єкта, що випливає з його належності до "приватної сфери" життя людини. До того ж, цей термін одразу асоціюється з тим, що належить безпосередньо приватній особі і є недоступним для людського загалу, є "приватною справою" і протиставляється публічному. Його антонім англійською мовою "паблісіті" (**англ.** *publicity*) також близький за звучанням до українського еквівалента "публічність", що означає відкритість для публіки, гласність.

Юридична термінологія відображає ставлення держави й суспільства до певних правових цінностей. За часів Радянського Союзу, слово "приватне" у вітчизняній юридичній термінології вживалося вкрай рідко, оскільки було, як і приватна власність, "пережитком минулого", із яким нещадно боролися. Натомість

використовувався термін “особисте”: “особиста власність”, “особисті стосунки”, “особисте життя”.

Для передачі поняття “приватне життя” (**англ.** *private life*), що вживається у багатьох міжнародних документах з прав людини, в українській науці міжнародного права до сих пір і послуговуються терміном “особисте життя”, хоча ним охопити всі аспекти приватного життя неможливо. На думку дослідника Р.Б. Холлборга, право на приватність (**англ.** *right to privacy*) є моральним принципом поваги до індивідуальної свободи [[6], *175*]. Захист приватної сторони життя людини є тією правовою цінністю, яка дозволяє людині відчути свою індивідуальність у суспільстві, що поважає цю індивідуальність.

Право на приватність оформилось в окреме правове поняття не так давно, наприкінці 19-го століття, хоча його коріння можна знайти у ранніх джерелах права. Проводячи дослідження витоків права на приватність, науковці відзначають, що у західних країнах захист приватності також має давні традиції [[7], *7-8*].

Для виокремлення права на приватність у самостійне поняття людству потрібно було дійти до такого рівня розвитку цивілізації, при якому автономність життя стала вкрай необхідною для збереження й реалізації людиною своєї особистості.

Безпосередньою причиною, що надала поштовху для створення першої правової концепції правового захисту приватності стала публікація на шпальтах газет Бостона (США) подробиць одного весілля. Обурений цим фактом батько нареченої, бостонський юрист Самуель Воррен разом з його колегою Луїсом Брандезом вирішили розробити правове поняття, що змогло б захистити приватне життя людини від втручань з боку інших осіб. У згаданій статті, що була опублікована у “Гарвардському Огляді Законів”, датованому 1890 роком, вони відзначали, що вже тогочасні методи провадження бізнесу вимагали відповідних заходів для правового захисту індивідів. На їхню думку, право на приватність – це право бути залишеним на самоті (**англ.** *let to be alone*) [[8], *193-220*].

Перша концепція права на приватність пройшла судову апробацію в США. У практиці американських судів нерідко розглядалися випадки комерційного використання персональних характеристик індивідів, таких як зовнішній вигляд, ім’я

та голос. Нерідко такі випадки порушення прав людини супроводжувалися порушеннями права власності. Американські суди вбачали в цих індивідуальних рисах особистості, на які посягали інші особи, певний об'єкт захисту майнового інтересу.

Як відмічає американський дослідник Л. Мортон, традиційне західне уявлення про право на приватність бере свій витік з права на недоторканність домоволодіння, а західна доктрина приватності має територіальний характер, оскільки захищає персональний життєвий простір особи [[9], *3*].

Американський юрист Вільям Л. Проссер після вивчення прецедентів, створених американськими судами під час розгляду справ щодо втручання у приватне життя людини, запропонував класифікацію можливих деліктів у цій сфері. Серед них: розкриття фактів, що стосуються приватного життя; повідомлення неправдивої інформації про людину; неправомірне використання зображень зовнішності, голосу людини і, нарешті, останнє, – фізичне домагання [[10], *811*].

Інший американський дослідник, Е. Блауштайн у своєму дослідженні вбачає у всіх цих чотирьох аспектах порушення приватності: "втручання в право особи робити те, що вона хоче" [[11], *1003*].

Свою класифікацію втручань у приватне життя пізніше запропонував шведський дослідник С. Стромхольм. Виділивши чотирнадцять видів неправомірних посягань на приватність, він об'єднав їх у три групи, виходячи зі спрямованості дій правопорушників:

дії, спрямовані на вторгнення у приватну сферу життя особи, – незаконний обшук, відправлення листів з образами, домагання телефонними дзвінками;

незаконні дії, завдяки яким порушники одержують інформацію про приватне життя особи: підслухування телефонних розмов, перехоплення кореспонденції тощо;

поширення чи інше використання відомостей про приватне життя особи: публікація у пресі інформації про приватне життя, використання імені і зовнішнього вигляду особи [[12], *213-238*].

Саме вплив розвитку техніки на права людини, з приводу якого американські науковці Самуель Воррен та Луїс Брандез висловлювали занепокоєння, і послужив

причиною появи першої концепції приватності. Поширення комп'ютерів і автоматизованої обробки персональних даних дозволило досліднику Колумбійського університету А. Вестіну сформулювати у згаданій вище праці визначення приватності для "електронного віку" як інтерес індивіда визначати для себе, коли, у який спосіб і якою мірою інформація про нього передається іншим особам, як вільне й термінове уникнення загалу у фізичному чи психологічному розумінні" [13, *7*]. Зазначена дефініція стала загальновизнаною у наукових колах. Погоджуючись із нею, Артур Міллер зазначає, що основною умовою для ефективної реалізації права на приватність є особиста можливість контролювати циркуляцію інформації, що стосується особи, яка є суттєвою для підтримання соціальних стосунків і особистих свобод [14, *25*].

Оскільки саме право людини на приватність персоніфікованої інформації стає об'єктом правового захисту, цей вид приватності одержав назву "інформаційна приватність" (**англ.** *informational privacy*). На думку російських дослідників Р.М. Юсупова, В.П. Заболотського, В.П. Іванова, цей вид приватності також має територіальний вимір, оскільки інформаційні потоки циркулюють у певному фізичному просторі. Людина ж є основним джерелом інформації, яка генерується всередині її життєвого простору, і є споживачем інформації, яка надходить до неї ззовні [15, *4*].

Згідно з класифікацією, запропонованою американськими дослідниками, слід розмежувати сфери, в яких реалізується суспільна активність людини. Це дозволяє розбити загальну проблему захисту приватності людини на сектори, які вимагають окремого законодавчого регулювання. За цим критерієм виділяють чотири види приватності:

- інформаційна приватність, якою охоплюються правила стосовно збору й обробки персональних даних;
- тілесна (фізична) приватність, яка стосується захисту фізичної недоторканності людини від примусових процедур, таких як наркологічне тестування та ін.;
- комунікаційна приватність, яка охоплює безпеку й конфіденційність поштових відправлень, телефонних розмов, електронної кореспонденції та інших форм зв'язку;

- територіальна приватність, яка стосується встановлення правових рамок для захисту від втручання в сімейну сферу, інше оточення, на робочому місці або в транспортному засобі [16, 7].

Така класифікація дозволяє зрозуміти комплексність і взаємопов'язаність усіх елементів цього правового поняття. Разом із тим, питання правового регулювання збору й передачі інформації, на нашу думку, є ключовими для захисту приватності інформації про особистість. При цьому комунікації й бази даних виступають як носії персоніфікованої інформації. Відокремленням цього об'єкта правового регулювання від сфери "інформаційна приватність" в окреме поняття "комунікаційна приватність", відділяється певна частина від цілого.

Очевидно, розвиток інформаційних технологій поступово стирає грані між цими поняттями. Стрімке поширення електронних комунікацій, в яких повідомлення передаються у цифровому вигляді, не дозволяє технічно й нормативно розмежувати де закінчується комунікаційна приватність і починається приватність персональних даних. Це вимагає пристосування нормативно-правового регулювання до розвитку інформаційних технологій з метою зробити його "технічно нейтральним".

Таким чином, особливістю захисту права на приватність персоніфікованої інформації є спрямованість на забезпечення свободи особи у визначенні просторових й часових рамок інформаційного контакту з іншими суб'єктами, підконтрольності циркуляції персоніфікованої інформації в суспільстві, що є важливим для підтримання автономії особи, захисту приватної сфери її життя.

Досягнення вищезазначених цілей захисту персоніфікованої інформації ставиться під загрозу з огляду на наднаціональний характер її транскордонної передачі на сучасному етапі розвитку інформаційних технологій. Ці питання набули актуальності у 70-х роках двадцятого століття, однак надзвичайно загострились у зв'язку із появою Інтернет.

Глобальна, наднаціональна мережа Інтернет, у порівняні з уже звичайними засобами передачі інформації, такими як телебачення й радіомовлення, представляє собою новий медіум з унікальними характеристиками. Унікальність цієї мережі

полягає у тому, що вона функціонує не тільки як засіб масової інформації, але до того ж є комунікаційним засобом.

Проблема забезпечення права на приватність користувачів Інтернет ускладнюється екстериторіальним характером інформаційного обміну. Інтернет дозволяє встановлювати безпосередній контакт між людиною-суб'єктом даних, який перебуває під юрисдикцією однієї держави, і іншими суб'єктами інформаційного обміну, які можуть перебувати на території інших держав. Забезпечити дію національних положень, а значить гарантувати належний рівень захисту приватності для своїх громадян у цьому середовищі для держави стає проблематичним. У той же час створення національними урядами штучних перешкод для вільного транскордонного обігу персоніфікованої інформації негативно відбиватиметься на міжнародному співробітництві у багатьох сферах. Розуміння цієї проблеми спонукало міжнародне співтовариство до розвитку співробітництва з метою забезпечення безперешкодності інформаційного обміну, яке призвело до створення сукупності міжнародних норм і принципів, що охоплюються міжнародно-правовим інститутом захисту приватності персоніфікованої інформації.

Міжнародно-правовий інститут захисту приватності персоніфікованої інформації містить відповідні норми й принципи спрямовані на забезпечення безперешкодності передачі інформації через кордони. Однак ця мета нерозривно пов'язана з міжнародно-правовим захистом права людини на приватність персоніфікованої інформації, що становить стрижневий елемент всього міжнародно-правового механізму регулювання транскордонної передачі персоніфікованої інформації.

Зазначеним проблемам присвячують лічені праці вітчизняних науковців. При цьому питання захисту права людини на приватність і забезпечення безперешкодності транскордонної передачі персоніфікованої інформації розглядались ними здебільше відокремлено одне від одного: перше – в контексті теорії прав людини, друге – з точки зору міжнародно-правового регулювання інформаційних обмінів у різних галузях міжнародного права.

В контексті теорії прав людини ті чи інші проблеми правового регулювання відносин щодо використання персоніфікованої інформації розглядає низка

українських науковців у різних площинах. Окремі аспекти забезпечення інтересів суспільства в доступі до інформації, які є конкуруючими з інтересами осіб на захист від розголошення персоніфікованої інформації, досліджені в українській правовій науці більшою мірою, що можна пояснити сучасними політико-правовими проблемами відкритості влади, дотримання свободи слова в Україні тощо. Серед наукових публікацій за цією тематикою можна окремо виділити праці О. Жуковської [17, 18], Є. Захарова та І. Рапп [19, 20, 21], Т.А. Костецької [22, 23], М. Місьо та Н. Петрової [24], В.Ф. Іванова [25]. У більшості із зазначених робіт аналізуються відповідні закони і підзаконні акти України, а також судова практика щодо реалізації конституційного права на інформацію як судами України, так і Європейським Судом з прав людини. Проблема правового захисту приватності персоніфікованої інформації не є безпосереднім об'єктом цих досліджень, а розглядається ними як одна з можливих підстав застосування обмеження права на інформацію, свободи слова тощо. Загальнотеоретичні питання правового захисту інформації розглядають російські дослідники Л.П. Кураков, С.Н. Смирнов [26]. Теоретичні питання співвідношення й установлення регулятивного балансу між правом на свободу інформації й правом на приватність у контексті теорії прав людини в українській правовій науці ще й досі залишаються належним чином не дослідженими. Вони, на нашу думку, мають важливе теоретичне значення з огляду на проблеми співіснування різних національних підходів у країнах континентальної й англосаксонської правових сімей, а також практичне – для впровадження відповідних принципів з метою вдосконалення чинного законодавства України.

Безперечно, актуальними для нашої молодої демократичної держави є правові питання доступу до архівних даних, у тому числі матеріалів про репресованих за часів тоталітарного режиму осіб. Це питання є вузькоспеціальним і виходить за визначені рамки дослідження, однак потребує окремого ґрунтовного вивчення українською правовою наукою. При цьому корисними можуть бути наукові розробки таких зарубіжних дослідників, як: Г.П. Буль [27], А.П. ван Влієт [28], А. Жеплінський [29],А.Г. Куінтана [30].

Серед найперших у радянській науці міжнародного права, питання міжнародно-правового регулювання масової інформації (комунікації) розглянув Ю.М. Колосов у своїй монографії датованій 1974 роком. Погоджуючись з канадським юристом Е. Макуіні, він зазначає, що розвивається нова галузь міжнародного права – право масової інформації (комунікації), "яке повинно слугувати підтриманню високих темпів наукового і технічного прогресу ... вільного поширення інформації та ідей без зайвих штучних перешкод, створюваних національними кордонами" [31, *32*].

Надзвичайно цікавим з наукової точки зору й практично-корисними для нашої держави є дослідження правового регулювання захисту приватності персоніфікованої інформації в праві Європейського Союзу. Проблеми запровадження загальноєвропейських правових стандартів захисту приватності персоніфікованої інформації досліджуються в численних працях іноземних дослідників. Вивченню розбіжностей у національних підходах до захисту приватності персоніфікованої інформації у країнах Європейського Союзу та шляхів їх вирішення на підставі норм європейського права присвячені дослідження низки науковців: Г. Пірс, Н. Платтен [32], Т. Леонард, І. Поуле [33], М.-Х. Боуланер, Ц. де Терванґнер і Т. Леонард [34, 35], М.-К. Понторіу [36], В. ван де Донк, Х. ван Дьювенбоден, Ч.Д. Рааб [37]. Питання захисту приватності персоніфікованої інформації у контексті процесів європейської інтеграції розглядає У. Бруханн [38]. Ґрунтовне дослідження еволюції законів про захист персональних даних європейських країн провів Майор-Шонбергер [39]. На проблемах імплементації європейських стандартів у датське законодавство з урахуванням національних правових традицій і правової культури поводження з персоніфікованою інформацією зосереджує свою увагу П. Блюм [40]. Національним проблемам впровадження загальноєвропейських стандартів присвячуються також роботи А. Саренпа [41] щодо законодавства Фінляндії, С. Челтона [42], Дж. Мортона [43] та Ч.Д. Рааба [44] щодо законодавства Об'єднаного Королівства; Ф. де Броувьєр [45] щодо бельгійського права; Г. Гарстка [46], В. Мейор-Шонбергер, Г. Мегер та Д. Кронеггер [47] щодо законодавства Німеччини; Р. Кастоно Суареса – Іспанії [48], К.М. Руіз [49]; Р. І. д'Афлітто [50], А. Нова [51] щодо права Італійської республіки.

Проблемами імплементації загальноєвропейського підходу до захисту права на приватність з точки зору конституційних традицій окремих європейських країн займалися також І. Вассілакі [52], Г. Брейбент, У. Бруханн, Ч.Д. Рааб [53], Н. Маллет-Поль, Ж.Ф. Местре Делагадо, І. Поуле [54], Л.Кадоу, Дж. Б. Рул [55], Б. Варуфсел, Х. Беркет [56], Ж.-К. Кокс [57].

Окремі питанням галузевого застосування принципів захисту приватності персоніфікованої інформації порушують: С. Сімітіс у галузі трудового законодавства Об'єднаного Королівства [58]; Д. Крімпхов [59], Г. Волгемут [60] – законодавства Німеччини; Р. Харала, А-Л. Рейнікайнен щодо адміністративного законодавства Фінляндії [61]; з актуальних питань електронної комерції – У. Бруханн [62]; в контексті адміністрування податків – К. Лінант де Беллефондс [63]; в телекомунікаційному секторі – Г.-Г. Шілд [64] та І. Гейс [65].

З огляду на відсутність відповідних досліджень європейських правових стандартів захисту приватності персоніфікованої інформації в українській науці міжнародного права цьому актуальному питанню присвячується підрозділ 2.2 дисертації.

Окремо слід відзначити наукові праці російського вченого В.П. Іванського, присвячені проблемам захисту приватної сфери життя людини у зв'язку з використанням інформаційних технологій [66, 67]. У своїй дисертаційній роботі він, зокрема, зосереджує увагу на порівняльному аналізі положень, що містяться в національних законах деяких європейських країн, датованих 80-90-и роками двадцятого століття. Проте учений не враховує той факт, що з 1995 року країни-члени Європейського Союзу приводять свої законодавства у відповідність з європейськими правовими стандартами, усуваючи наявні в них розбіжності. Окресливши наявні проблеми забезпечення безперешкодної передачі даних між країнами з різним рівнем захисту, В.П. Іванський залишає поза увагою питання, яке є суттєвим для розуміння причин наявності розбіжностей у національних підходах країн континентальної й англосаксонської правових сімей, насамперед країн ЄС і США, та шляхів їх подолання в контексті транскордонної передачі.

Дослідженню принципових розбіжностей у підходах до обраних європейськими країнами і Сполученими Штатами Америки моделей регулювання обробки

персоніфікованої інформації, зокрема, статутного регулювання (країни ЄС) і саморегуляції приватного сектора (США) приділяють увагу Н. Платтен [68], П. Мей [69], П. Реган [70]. З точки зору узгодження цих протилежних підходів у контексті транскордонної передачі даних між ЄС і США зазначені питання розглядаються в роботі А. Флейшмена [71]. Вплив європейських стандартів захисту приватності персоніфікованої інформації на законодавство Канади досліджує К.Дж. Беннетт [72].

Проблеми узгодження міжнародних стандартів, які містяться у документах Європейського Союзу, Ради Європи й Організації Економічного Співробітництва і Розвитку, досліджує іспанець С.Л. де ла Ескобар [73] та творчий колектив у складі професорів К.Дж. Беннетта (Канада) і Ч.Д. Рааба (Велика Британія) [74, 75, 76].

Питанням, що виникають у зв'язку з передачею даних до країн, які не надають адекватного, у європейському розумінні, рівня правового захисту приватності персоніфікованої інформації, присвячується робота Ф.М. Карліна [77]. Розв'язати ці проблеми за допомогою договірних механізмів пропонують дослідники Е. Логворс [78], В. Котші [79], А. Дікс [80]. З огляду на відсутність відповідних досліджень в українській науці міжнародного права, а також їх актуальність для розробки й впровадження відповідного механізму для передачі персональних даних як одержувачам в Україні, так і відправниками з України, міжнародно-правові механізми захисту приватності персоніфікованої інформації під час транскордонної передачі аналізується в підрозділі 2.3 цього дослідження.

Теоретичні і практичні питання впровадження міжнародно-правових, зокрема, європейських, стандартів у галузі прав людини в законодавство України були предметом досліджень українських науковців у різних площинах і контекстах. Серед перших фундаментальних робіт у науці міжнародного права з питань взаємодії міжнародного і внутрішньодержавного права можна назвати працю В.Г. Буткевича [81]. Ця тема дістала подальший розвиток в численних наукових розробках В.Н. Денисова [82, 83, 84, 85], а також його спільних працях з В.І. Євінтовим [86, 87].

Окремі питання взаємодії міжнародного і внутрішньодержавного права України в інформаційній сфері розглядають І.Ю. Онопчук [88, 89], В. Опришко [90], О. Павличенко [91]. Висвітлюючи проблеми інформатизації, питання вдосконалення

інформаційного законодавства вивчає авторський колектив Донецького Інституту економіки і промисловості [92].

Проблемам приведення законодавства України у галузі правового захисту приватності персоніфікованої інформації у відповідність до вимог європейських стандартів присвячено лише кілька публікацій українських науковців. Серед них стаття С.В. Шевчука, в якій розглядаються актуальні питання реалізації конституційного права на доступ до персоніфікованої інформації [93], а також статті Т.А. Костецької [94], К.Б. Полінкевич [95, 96]. У зазначених роботах наголошується на необхідності впровадження європейського підходу до захисту приватності персоніфікованої інформації, однак не пропонуються політико-правові моделі, які б враховували особливості правової системи України.

З іншого боку, в працях авторського колективу українських дослідників у складі О. Баранова, В. Брижка, Ю. Базанова [97, 98] пропонується правова модель захисту персональних даних, яка однак викликає низку суттєвих зауважень, оскільки побудована не на концепції приватності, а на праві інтелектуальної власності. З огляду на недостатню розробленість зазначеного питання в українській правовій науці, нами дається спроба окреслити шляхи вдосконалення чинного законодавства України з урахуванням досвіду європейських країн у третьому розділі дисертації.

Отже, проведений огляд літератури з теми дисертації дозволяє констатувати недостатню розробленість в українській науці міжнародного права вищезазначених актуальних питань міжнародно-правового захисту приватності персоніфікованої інформації, що й визначає основні напрямки цього дослідження і його структуру.

1.2. Нормативна природа і межі здійснення права на приватність персоніфікованої інформації

У цьому підрозділі пропонується розглянути нормативну природу права на приватність персоніфікованої інформації як загальновизнаного права людини, закріпленого в міжнародно-правових документах, а також зарубіжному і вітчизняному конституційному праві. Дослідження зазначеної проблеми є важливим також для визначення правових рамок здійснення права на приватність, що безпосередньо пов'язано з проблемою узгодження цього права людини з конкуруючими інтересами інших осіб та всього суспільства. Саме в цих положеннях закладаються основи, стрижневі елементи і принципи сучасного міжнародно-правового інституту захисту приватності персоніфікованої інформації, які визначають тенденції його подальшого розвитку.

Міжнародно-правовим проблемам захисту прав людини, особливо останнім часом, приділяється все більше уваги в українській науці міжнародного права, що є позитивним чинником для подальшого розвитку правової держави і виховання суспільства у дусі поваги до загальнолюдських цінностей, до яких, зокрема, відносяться фундаментальні права і свободи людини.

У науці міжнародного права немає однозначного погляду на місце норм і принципів захисту прав людини в сучасній системі міжнародного права, зокрема, щодо віднесення їх до окремої галузі міжнародного права з прав людини чи до міжнародного гуманітарного права. Докладний аналіз цієї проблематики дається у працях відомих українських вчених М.М. Антонович [99] та А.І. Дмитрієва [100], позиції яких у цьому питанні є протилежними. М.М. Антонович розділяє точку зору зарубіжних вчених Й. Дінстейна [101] і Ф. Хемпсона [102], що ці галузі обидві включають норми, основною метою яких є захист прав людини. При цьому, якщо міжнародне право з прав людини базується на відповідних фундаментальних правах осіб (зобов'язання erga omnes), то міжнародне гуманітарне право ґрунтується на

взаємних зобов'язаннях держав, за порушення яких міжнародне право вимагає покарання [[103], *38*].

За визначенням А.І. Дмитрієва, "міжнародне гуманітарне право включає принципи і норми, що регулюють відносини між державами з приводу захисту прав людини й основних свобод для усіх, незалежно від раси, статі, мови й релігії як у мирний час, так і в період збройних конфліктів"[1)]. Аналогічну думку поділяють й відомі російські міжнародники Ю.М. Колосов та В.І. Кузнєцов [[104], *297*]. На думку іншого відомого російського вченого-міжнародника В.А. Карташкина, саме міжнародним правом з прав людини охоплюються відповідні норми щодо захисту прав людини як у мирний час, так і у період військових конфліктів, а також норми, що передбачають відповідальність за їх злочинне порушення [[105], *492-495*].

Це питання потребує подальшого наукового обґрунтування і виходить за рамки даного дослідження. Відзначимо, що відповідні норми щодо захисту прав людини у зв'язку з використанням і передачею персоніфікованої інформації через кордони розраховані на їх застосування у мирний час, а тому цілком виправдано вважати сукупність цих норм як складову частину (інститут) міжнародного права з прав людини.

Докладний аналіз розвитку міжнародних стандартів з прав людини подається в роботах Л.Г.Заблоцької [[106]], П.М. Рабиновича [[107]]. Нас це питання цікавить виключно з точки зору визначення місця права на приватність у системі прав і свобод людини, а разом із тим і його становлення як загальновизнаного права людини, закріпленого в численних міжнародних документах.

Право на приватність одержало своє міжнародне визнання із прийняттям Загальної декларації прав людини. Право на приватність проголошується у Статті 12 Декларації:

[1)] [100] Дмитрієв А.І. Міжнародне гуманітарне право: основи концепції / Інститут держави і права ім. В.М.Корецького НАН України; Вища школа права при Інституті держави і права ім. В.М.Корецького НАН України. — К. : Логос, 1999. — С. 14

“Ніхто не може зазнавати безпідставного втручання у його особисте й сімейне життя, безпідставного посягання на недоторканність його житла, таємницю його кореспонденції або на його честь і репутацію. Кожна людина має право на захист закону від такого втручання або таких посягань” [108][1)].

Численні універсальні міжнародні документи визнають право на приватність як невід’ємне право людини. Зокрема, у статті 17 Міжнародного Пакту про громадянські й політичні права проголошується:

“1. Ніхто не повинен зазнавати свавільного чи незаконного втручання в його особисте й сімейне життя, свавільних чи незаконних посягань на недоторканність його життя або таємницю його кореспонденції чи незаконних посягань на його честь і репутацію.

2. Кожна людина має право на захист закону від такого втручання чи таких посягань” [109][2)].

Аналогічна правова “формула” для позначення права на приватність використана в Статті 16 Конвенції ООН про права дитини 1989 року [110] і Статті 16 Конвенції ООН про захист прав усіх трудящих-мігрантів та членів їхніх родин 1990 року [111]. Тут слід звернути увагу на той факт, що у перекладі більшості міжнародних документів українською мовою термін “privacy” (приватність) невиправдано, за нашим глибоким переконанням, ототожнюється з поняттям “особисте життя”. При цьому втрачається важливий нюанс, оскільки захисту потребує не “особисте життя”, а саме “приватність” як гарантована цим правом захищеність від будь-яких посягань.

Право на повагу до приватного життя визнається як фундаментальне право людини Європейською Конвенцією про захист прав людини та основних свобод.

Стаття 8 Конвенції проголошує:

“1. Кожна людина має право на повагу до її особистого й сімейного життя, житла й таємниці кореспонденції.

---

1) [108] Загальна декларація прав людини. — К.: Право, 1995.

2) [109] Міжнародний пакт про громадянські та політичні права і Факультативний проокол № 1 до Міжнародного пакту по громадяньку та політичні права. — К.: Право, 1995.

2. Держава не може втручатися у здійснення цього права інакше ніж згідно із законом та у випадках, необхідних у демократичному суспільстві в інтересах національної та громадської безпеки або економічного добробуту країни, із метою запобігання заворушенням і злочинам, для захисту здоров'я або моралі чи з метою захисту прав і свобод інших людей" [112][1)].

Спосіб, у який викладено це право у статті 8 Конвенції, є унікальним. У статті йдеться про "право на повагу…", і не вказується на будь-які дії, що підлягають захисту. Не згадується в тексті статті й термін "приватність", хоча вищевказані міжнародні документи вживають його для позначення одного з об'єктів захисту.

Така редакція статті є результатом узгодження позицій творців проекту Конвенції та свідчить про їх намір залишити за державами-учасницями право самостійно визначати правові рамки здійснення проголошеного в цій статті права. Однак це створювало певні проблеми під час розгляду справ Комісією й Судом і залишилося проблемним для новоствореного Суду з прав людини.

Дослідники прецедентного права Конвенції відзначають труднощі, що виникають під час застосування статті 8, які полягають у необхідності пошуку шляхів вироблення спеціальних звужувальних характеристик для права на повагу до приватного життя [113, *251*].

Конвенція не дала чіткого визначення поняттю "право на повагу…". Але це не завадило Комісії та Суду – контрольним органам Конвенції – під час розгляду справ про порушення цього права конкретизувати шляхом тлумачення зміст відповідної правової норми. В одному зі своїх рішень із цього питання Комісія зазначила різницю між правом на повагу до приватного життя й правом на приватність, наголосивши, що "право на повагу" не обмежується тільки правом на приватність, а включає також право "встановлювати та розвивати стосунки з іншими людьми, особливо в емоційній сфері, для розвитку та реалізації людиною своєї особистості" [114][2)].

[1)] [110] Конвенція про захист прав людини та основних свобод. Із поправками, внесеними відповідно до положень Протоколу №11. Офіційний переклад МЗС України та Української правничої фундації. — К.: УПФ. — 31 с.

Під час розгляду справ і тлумачення положень Конвенції Комісія та Суд не обмежили предмет захисту Статті 8 лише внутрішньою сферою приватного життя людини, а цілком закономірно поширили її дію на інші прояви соціального буття людини.

На думку Комісії та Суду, право на повагу захищає права: на власне ім'я [115], честь і репутацію [116], свободу зібрання [117], право на підтримання приватних ділових стосунків [118], на захист від фізичного насильства [119], свободу вибору сексуальної орієнтації [120], визнання зміни соціального статусу внаслідок зміни статевої належності [121], на благополучне навколишнє середовище [122, 123], на захист приватності персональних даних тощо [124].

Вдається цілком вірним, що новий Цивільний кодекс України втілив саме це, широке розуміння правового захисту приватної сфери життя людини, зокрема, визначивши у статті 271 зміст особистого немайнового права, як *можливість фізичної особи вільно, на власний розсуд визначати свою поведінку у сфері приватного життя* [125].

Як Таким чином, "право на повагу" у контексті Статті 8 Європейської Конвенції включає право на приватність персоніфікованої інформації як складову частину, що підлягає захисту. У зв'язку з цим виникає питання, до якої категорії прав людини можна віднести право на приватність персоніфікованої інформації. Міжнародно-визнані права прийнято класифікувати у категорії, зокрема за ознакою їх належності до того чи іншого "покоління" прав людини, що має не лише теоретичне, а й практичне значення, зокрема, під час визначення структури й змісту міжнародних документів, присвячених правам людини. Це розрізнення було вперше реалізовано на практиці у 1966 році під час підготовки й ухвалення двох Міжнародних Пактів: "Про громадянські і політичні права", "Про економічні, соціальні і культурні права", які були ратифіковані Українською РСР у 1973 році [126].

Появу першої категорії прав людини відносять до епохи буржуазних революцій. Громадянські й політичні права становлять основу для інших прав людини, оскільки

[2)] [112] Доповідь Європейської Комісії з прав людини по справі Ван Остервійк проти Бельгії. — Рада Європи, 1979.

закладають фундамент для демократії. Ця категорія прав людини фактично відображає протистояння між державою й людиною і спрямована на приборкання свавілля публічної влади шляхом заборони зазіхання на інтереси особи. Відповідні громадянські права людини покладають на державу "негативне" зобов'язання не вчиняти певних дій для уникнення порушень.

Друга категорія – економічні, соціальні і культурні права, – на відміну від громадянських прав, покладає на державу "позитивне" зобов'язання, вимагаючи від неї вжиття необхідних заходів для ефективної реалізації прав людини. За своєю суттю це колективні, а не індивідуальні права, оскільки "споживачами" результатів їх втілення виступають не окремі особи, а групи людей.

Ця класифікація пізніше була доповнена "новим" поколінням прав людини. Третя категорія охоплює право на мир, право на розвиток і екологічні права (на задовільне навколишнє середовище).

Між тим, така класифікація прав людини залишається більш теоретичною, ніж практичною. Основна маса міжнародно-правових документів у цій галузі не є структурованими для виокремлення категорій прав людини. За підходом, який обрала Європейська Комісія й Суд з прав людини під час розгляду справ та тлумачення положень статті 8 Конвенції, "право на повагу" не може бути віднесено лише до категорії громадянських прав. Воно охоплює певною мірою сферу економічних прав (право на підтримання ділових стосунків) і соціальних прав (свободу зібрання), – тобто прав другого покоління. До того ж, вимога захисту "якості" приватного життя зумовила поширення дії статті 8 і на сферу екологічних прав (право на благополучне навколишнє середовище), які належать до третього покоління прав людини.

Право на приватність персоніфікованої інформації історично з'явилось як складова частина права на захист від неправомірного втручання держави у приватне життя, а тому може бути віднесено до категорії "громадянські права". Використання персоніфікованої інформації в економічних стосунках, образно кажучи, "перетворює" людину – суб'єкта прав на їх споживача, що дозволяє умовно віднести "право на приватність інформації про споживача" до категорії економічних прав.

Тут слід звернути увагу ще на один аспект – поширюється тенденція відокремленого вживання термінів “право на приватність” (**англ.** *right to privacy*) і “право на захист даних” (**англ.** *right to data protection*), що простежується в документах Європейського Союзу. На своєму засіданні 4 липня 1999 року у Кельні Рада Європейського Союзу ухвалила рішення про підготовку проекту Хартії основних прав Європейського Союзу. У зв'язку з цим Робоча група Статті 29, підтримуючи рішення Ради ЄС, ухвалила 7 вересня 1999 року рекомендацію, якою запропонувала включити *право на захист персональних даних* до Європейського “каталогу фундаментальних прав”. При цьому Робоча група обґрунтувала свою позицію тим, що у своїх висновках і рішеннях Європейська Комісія і Європейський Суд розвинули і визначили фундаментальне право, що основане на різних правах людини, яке стосується захисту персональних даних [127]. Ця позиція була підтримана Європейським Парламентом й Радою, які ухвалили Хартію основних прав громадян Європейського Союзу, включивши до неї спеціальну статтю 8 присвячену саме праву на *захист персональних даних* [128].

Між тим, у текстах спеціальних міжнародно-правових актів у галузі захисту приватності персоніфікованої інформації, зокрема, у третій частині преамбули Конвенції Ради Європи “Про захист осіб стосовно автоматизованої обробки персональних даних” 1981 року [129, *33-45*], у п. 10 преамбули до Директиви 95/46 СЕ Європейського Парламенту й Ради “Про захист фізичних осіб стосовно автоматизованої обробки персональних даних та безперешкодного руху цих даних” 1995 року [130, *51-80*] для позначення цього права людини щодо персоніфікованої інформації використовується термін “приватність”.

Аналогічну позицію поділяє і Європейський Суд з прав людини. У справі *“Z проти Фінляндії”* конфіденційні медичні дані заявниці про захворювання на СНІД була розкрита без її попередньої згоди в інтересах кримінального процесу проти її чоловіка, який був звинувачений у вчинені серії зґвалтувань. У рішенні, датованому 25.02.1997 року, Суд наголосив, що захист приватності персональних даних, не тільки медичних, є надзвичайно важливим для реалізації права на повагу до приватного й сімейного життя, гарантованого статтею 8 Конвенції [131].

Отже, поширеною залишається концепція, яка розглядає право на приватність персоніфікованої інформації як складову частину права на повагу до приватного життя. Окреме вживання цих понять, на нашу думку, свідчить про намагання зробити акцент на важливості права на приватність персоніфікованої інформації, особливо з огляду на важливість саме інформаційного аспекту для захисту прав людини у зв'язку з розвитком інформаційних технологій.

Відповідна адаптація доктрини права на приватність персоніфікованої інформації до сучасного стану розвитку суспільних відносин відбувається і на національному рівні. Основним правовим джерелом прав людини на національному рівні, як правило, є конституція, яка містить каталог основних прав і свобод людини. Увага, яку ми приділяємо конституційно-правовим аспектам проблеми правового захисту приватності персоніфікованої інформації викликана також тим фактом, що саме конституційне право відіграє головну роль у визначенні взаємодії національного і міжнародного права, зокрема, у питанні забезпечення прав людини й основних свобод.

Аналіз чинних конституцій більшості розвинутих країн світу свідчить про визнання за правом на приватність статусу невід'ємного права людини [132]. Однак пристосування конституційної доктрини права на захист приватного життя до реалій суспільного життя з його рівнем розвитку інформаційних технологій не завжди відбувається шляхом простого доповнення існуючої конституційної теорії новими положеннями. Зокрема, Сполученим Штатам Америки для цього знадобилося пройти певний шлях визнання за правом на приватність конституційного статусу судовою гілкою влади.

Будучи суддею Верховного Суду США, один з авторів першої концепції приватності, Луїс Брандез повторив своє відоме визначення приватності як "права бути залишеним на самоті" у справі "*Олмстід проти Сполучених Штатів*" у 1928 році. Ця справа займає важливе місце в конституційній історії розвитку концепції приватності в США. Верховний Суд своїм рішенням, яке він прийняв із "рахунком": 5 судів – "за", 4 – "проти", постановив, що ні заборона невиправданих обшуків і

вилучень Четвертої поправки до Конституції, ні захист П’ятої поправки від самообвинувачення, не надають права на захист від підслухування [133].

Позиція, сформульована Верховним Судом по справі Олмстіда, була переглянута лише 40 років потому. У справі “*Катц проти Сполучених Штатів*” у 1967 році Суд постановив, що підслухування являє собою обшук у розумінні Четвертої поправки і для цього не вимагається фізичне посягання, оскільки Четверта поправка захищає людей, а не місця. В обґрунтування цього рішення, суддя Джон Харлан сформулював положення, що мало великий вплив на подальшу судову практику у справах, де оцінювалися дії уряду щодо їх відповідності Четвертій поправці. Запропонований підхід вимагав відповіді на два запитання: чи продемонструвала особа справжнє або суб’єктивне очікування приватності, і чи є таке очікування виправданим з точки зору суспільства? Разом з тим, більшість у справі Катца висловилася за те, що Четверта Поправка не надає загального конституційного права на приватність [134].

Однак свій конституційно-правовий статус право на приватність у США одержало у 1964 році у справі Верховного Суду “*Грісвольд проти Коннектикута*”, в якому суддя-засідатель Вільям О. Дуглас проголосив свою теорію “сфер переломлення приватності” (**англ.** *penumbra theory of privacy*). Він, зокрема, відзначив, що різні гарантії Білля о Правах, створюють зони приватності, які захищаються Першою, Третьою, Четвертою, П’ятою і Дев'ятою поправками до Конституції США [135]. На відміну від країн із “старою” демократією, молоді незалежні держави у своїх конституціях мають можливість спиратися на сучасні правові концепції і більш адекватно, у дусі часу, закріпити певні права, враховуючи розвиток суспільних відносин.

Стосовно права на приватність персоніфікованої інформації це знайшло своє відображення у закріпленні “нових” інформаційних прав, які покликані надати людині можливість контролювати поводження з її персоніфікованою інформацією іншими суб’єктами.

Суттєвими для розуміння особливостей правового механізму захисту персоніфікованої інформації є питання взаємодії суб’єктивних прав особи, чия персоніфікована інформація використовується чи може бути використана, а також

легітимних, тобто таких, що є правомірними і визначеними відповідними законами, інтересів інших суб'єктів цих відносин. Правова конкуренція задіяних інтересів покладає на державу зобов'язання щодо балансування під час їх оцінки, що передує правозастосуванню. Європейський Суд з прав людини так окреслив це зобов'язання держави у рішенні по справі Рііс проти Сполученого Королівства у 1986 році:

"З'ясовуючи, чи існує позитивне зобов'язання, слід враховувати, що між загальним інтересом суспільства і інтересами окремої особи повинна бути встановлена справедлива рівновага, пошук якої – характерна риса усієї Конвенції. Для встановлення цієї рівноваги, певне значення можуть мати цілі, зазначені у другій частині статті 8, хоча у цьому положенні говориться лише про "втручання" у право, що користується захистом першого пункту, – іншими словами, воно стосується негативних зобов'язань, які випливають з цього пункту" [136].

Згідно з європейським підходом, щоб обмеження права на приватність не перетворились на його порушення, вони повинні:

- запроваджуватися на підставі закону;
- мати легітимну ціль;
- бути необхідними у демократичному суспільстві.

Серед конкуруючих інтересів, які можуть стати підставою для обмежування права на приватність персоніфікованої інформації, найбільш проблематичними для погодження залишаються права інших осіб, зокрема, права на вільне вираження поглядів і переконань (свободу інформації).

Це право є фундаментальним і визнається як одна із засад демократичного суспільства, оскільки без права на вільне вираження поглядів і переконань немає політичної свободи у суспільстві. На превеликий жаль, порушення свободи слова є поширеним явищем у світі. Трапляється так, що для справдовування таких випадків держави посилаються на інтереси людини у захисті недоторканності приватного життя [137].

На жаль, така практика набула поширення і в Україні. За даними Програми правового захисту та освіти засобів масової інформації "IREX ПРОМЕДІА" з 93 справ, у яких за цією програмою протягом 1999 року була надана консультативна

допомога представникам засобів масової інформації України, 46% позивачів були посадовими особами різного рівня, що відстоювали власне чесне ім'я і репутацію очолюваних ними державних організацій. І майже всі ці позови (93%) були реакцією на критичні газетні публікації, в яких подавалася інформація про офіційні дії посадових осіб [[138], *3*].

В той же час, загальновизнаним у правових системах країн з розвинутими демократичними інститутами є принцип, за яким громадські діячі мають бути більш відкритими для загалу, а тому більш толерантними до критики. Європейський Суд з прав людини відзначив з цього приводу:

"…свобода вираження поглядів, яка гарантується у першому параграфі Статті 10, становить одну із суттєвих засад демократичного суспільства і одну з основних умов для його прогресу і самореалізації кожного індивіда … це має застосовуватися не тільки до "інформації" чи "ідей", які поблажливо отримані або вважаються необразливими, чи до яких ставляться байдуже, а також і до тих, що ображають, шокують або заважають. Такими є вимоги щодо плюралізму, толерантності і широти поглядів, без яких не може бути "демократичного суспільства"… Ці принципи є особливо важливими, оскільки це стосується преси…"[[139], *41*].

Яким чином це погоджується із принципом рівності, адже громадський діяч в такому разі зазнає більшого обмежування права на приватність персоніфікованої інформації, ніж пересічний громадянин? Сам же принцип рівності складається із двох під-принципів: рівності в правах і рівності перед законом, що закріплено в статті 26 Міжнародного пакту про громадянські і політичні права.

Цей принцип визнається і в Конституції України. Стаття 21 Конституції України проголошує, що всі люди є вільні і рівні у своїй гідності та правах, а Стаття 24 – громадяни є рівними перед законом.

Між тим, легітимне обмежування права не свідчить про дискримінацію. До того ж, обираючи для себе життя публічної особи, пересічний громадянин свідомо йде на те, що стає предметом уваги громадськості. Остання, у свою чергу, хоче одержати якомога більше інформації про особу, якій вона довіряє публічну владу. Європейський Суд з прав людини таким чином сформулював це положення:

"Свобода преси дає громадськості одну з найкращих можливостей дізнатися про ідеї і позиції політичних лідерів і сформувати свою думку про них … Відповідно, межі допустимої критики є ширшими, коли вона спрямована на політика, а не на приватну особу. На відміну від останньої, перший неминуче і свідомо розкривається для прискіпливого аналізу кожного слова і вчинку як з боку журналістів, так і громадськості і, як наслідок, повинен виявляти до цього більше терпимості …"[140, *313*].

Комісія з прав людини ще раніше сформулювала зв'язок між обмеженням права на приватність і добровільними вчинками особи у доповіді по справі "*Брюггеманн і Шойтен проти ФРН*" у 1977 році таким чином:

"Вимога поваги до особистого життя автоматично обмежується в тій мірі, в якій окрема особа сама ставить своє приватне життя у залежність від громадського життя або інших інтересів, що перебувають під захистом" [141].

Зазначена конкуренція між правом людини на приватність персоніфікованої інформації і правом інших людей на свободу інформації вимагає оцінки задіяних інтересів під час правозастосування. Для цього мають бути вироблені певні критерії, використання яких дозволить врахувати сформульовані Європейським Судом з прав людини чинники, що роблять обмежування права на приватність персоніфікованої інформації легітимним.

Загальним критерієм для встановлення балансу між двома фундаментальними правами є дотримання принципу пропорційності при впроваджені обмежень. Цей принцип був сформульований Європейським Судом з прав людини під час розгляду справи "*Сільвер та інші проти Об'єднаного Королівства*" у 1983 році:

"… фраза "бути необхідним у демократичному суспільстві" означає, щоб бути сумісним з Конвенцією, втручання повинно, inter alia, відповідати "нагальній соціальній потребі" і бути "пропорційним до законної мети, що переслідується" [142, *61*].

Верховний Суд ФРН застосував один з критеріїв, що стосується такої умови обмежування як необхідність в демократичному суспільстві, під час розгляду справи щодо поширення пресою фактів з приватного життя публічної особи. Приводом для

справи стало фотографування журналістами принцеси Монако Кароліни під час романтичного обіду в одному з французьких ресторанів.

Верховний Суд у рішенні, датованому 19 грудня 1995 року, зазначивши про конкуренцію між публічним інтересом в отриманні інформації та правом позивачки на власну особистість, використав принцип пропорційності і застосував оціночний критерій інформаційної важливості певної події для громадськості:

"Захист приватної сфери життя людини має особливу важливість, коли оцінюються два інтереси. Право людини на повагу до приватного життя випромінюється із загального права на власну особистість, яке наділяє кожну людину автономним простором приватного життя, в якому вона може розвивати власну індивідуальність вільно від стороннього втручання. Право бути залишеним на самоті та "належати собі" складають частину цього простору ... Коли оцінюються різноманітні порушені інтереси, інформаційна цінність подій має відігравати суттєву роль. Чим більший інтерес громадськості бути інформованим, тим більше інтереси особи мають бути відсунуті на користь публічних потреб в інформації. І навпаки, потреба у захисті приватності особи набуває більшого значення, коли цінність інформації, яку громадськість отримує з фотографій, зменшується" [143].

Між тим, такий підхід, як нам здається, навряд чи зможе встановити стабільний баланс між правом на захист приватності персоніфікованої інформації і правом на публічність інформації, оскільки важливість тієї чи іншої інформації є суб'єктивним критерієм, а отже, вимагає застосування процедури безсторонньої оцінки.

Про роль незалежного органу держави, уповноваженого встановлювати баланс між правом людини на доступ до своїх персональних даних як складової частини права на приватність інформації і інтересами інших осіб у захисті конфіденційності, зокрема, висловився й Європейський Суд з прав людини під час розгляду справи "*Гаскін проти Об'єднаного Королівства*". Посилаючись на вироблений практикою принцип пропорційності в оцінці задіяних інтересів, у рішенні датованому 7 липня 1989 року, Суд відзначив:

"Така система є лише тоді у відповідності з принципом пропорційності, коли вона передбачає, що незалежний орган остаточно вирішує, чи буде надано доступ, якщо повідомники не можуть відповісти чи не дають згоди. Така процедура не була доступна для заявника у цій справі. Отже, наявні процедури не спромоглися забезпечити повагу для приватного і сімейного життя пана Гаскіна, як цього вимагає Стаття 8 Конвенції..."[144][1)].

Для ефективної реалізації людиною права на приватність персоніфікованої інформації від держави вимагається створення механізму, який дозволив би врахувати конкуруючі інтереси інших осіб і держави шляхом застосування легітимних обмежувань. За європейським підходом, складовою частиною такого механізму має бути незалежний орган держави, покликаний встановлювати справедливий баланс, використовуючи принцип пропорційності під час оцінки задіяних інтересів.

Отже, для європейського розуміння характерним є рівноцінний підхід до цих двох фундаментальних прав, згідно з яким сам факт регулювання питань використання персоніфікованої інформації не вважається, *a priori*, обмеженням свободи слова.

Принципово відрізняється від європейського підходу конституційно-правова доктрина і судова практика США в питанні співвідношення й узгодження права на приватність і свободи слова. За американським підходом, прийняття будь-якого нормативно-правового акту з інформаційних питань, у тому числі щодо правового захисту приватності персоніфікованої інформації, розглядається як обмеження свободи слова, тому повинно бути виправданим і не зазіхати непропорційно на свободу вільного одержання і поширення інформації. Яскравим підтвердженням зазначеного є справа, розглянута Апеляційним судом Десятого округу США 8 серпня 1999 року. Рішенням по справі визнано неконституційним Акт Федеральної Комісії з комунікацій (FCC), який покладав на телекомунікаційні компанії обов'язок одержувати однозначну згоду абонентів перед використання даних про телефонні дзвінки та інших персональних даних в цілях реклами. У справі "*U.S. West, Inc. v.*

[1)] [141] *Gaskin v. UK* (1989). — Reports of Judgments and Decisions. — 1989. — Series A. — No.160.

FCC” Суд встановив, що ці положення порушували право телекомунікаційних компаній на свободу слова, гарантоване Першою поправкою до Конституції США. Акт, прийнятий Федеральною Комісією з комунікацій (ФКК) після ухвалення Закону про телекомунікації у 1996 році, заборонив телекомунікаційним компаніям використовувати персональні дані абонентів у цілях реклами, якщо тільки абоненти однозначно не погодяться на це.

“U.S. West” та інші телекомунікаційні компанії аргументували свою позиції тим, що положення ФКК порушують Першу поправку обмеженням можливості поширювати комерційну інформацію своїм абонентам. Суд погодився, що має місце обмеження комерційної свободи слова, оскільки ціллю цих положень було запобігти рекламуванню (що також охороняється свободою слова) абонентам, які не бажають, щоб їх персональні дані використовувалась в рекламних цілях. За існуючою в США конституційною доктриною, уряд може обмежувати, так зване, “не-обманливе комерційне вираження поглядів” (**англ.** *non-misleading commercial speech*) в разі якщо доведе, що, по-перше, уряд має суттєвий інтерес у регулюванні вираження поглядів; по-друге, регулювання безпосередньо і матеріально спрямоване на цей інтерес; по-третє, регулювання не більш обмежувальне ніж потрібно для забезпечення цього інтересу.

Вирішуючи спір, Суд дійшов висновку, що приватність споживачів не є суттєвим інтересом, який міг би виправдати обмеження прав на свободу слова телекомунікаційних компаній. Суд наголосив, що людина може відчувати себе некомфортно, знаючи, що персоніфікована інформація циркулює вільно у світі, однак люди живуть у відкритому суспільстві, де інформація за звичай передається вільно. При цьому, загальний рівень дискомфорту не є достатнім для виправдання обмеження свободи слова. Обмеження має ґрунтуватися на дійсній загрозі заподіяння шкоди, на зразок, запобігання розголошенню інформації, що може бути використана для заподіяння шкоди, дратування чи обману когось. Уряд, на думку Суду, “*не надав доказів, які б демонстрували, що шкода … приватності є дійсною*” [145].

Отже, можна констатувати наявність суттєвих розбіжностей у підходах до розв’язання проблеми узгодження цих двох фундаментальних прав – права на

приватність і свободу слова – у європейській і американській конституційно-правових доктринах.

Інтерес людини відчувати свою автономію в суспільстві, яка захищається правом на приватність (недоторканність приватного життя), знаходиться у діалектичному протиріччі з певними інтересами інших осіб і суспільства, зокрема, у забезпеченні безпеки і добробуту, захисті прав і свобод інших осіб. Заради цих інтересів здійснюється боротьба із злочинністю, у ході якої нерідко має місце втручання у приватне життя. Як встановити справедливий баланс між індивідуальними і суспільними інтересами щодо використання персоніфікованої інформації у правоохоронній діяльності? Зрозуміло, що у демократичному суспільстві це діалектичне протиріччя не може бути вирішено ігноруванням одних інтересів на користь інших. Для його вирішення вимагається оцінка задіяних інтересів і їх узгодження. Правова конкуренція задіяних інтересів, особи – у захисті приватності, з однієї сторони, і суспільства у здійснені обробки персональних даних, з другої сторони, – покладає на державу зобов'язання щодо визначення, встановлення і підтримання балансу цих інтересів.

Аргумент, який часто наводять представники правоохоронних структур під час обговорення питань упровадження принципів захисту приватності персоніфікованої інформації в регулювання правоохоронної діяльності [146], що, мовляв, для успішної боротьби із злочинністю необхідно збирати і опрацьовувати якомога більше відомостей про осіб і бажано у негласний спосіб, – не витримує критики. Це так само неправомірно, як суцільне стеження, тотальний обшук житла чи огляд усіх транспортних засобів громадян з метою знаходження доказів вчинення злочину, що суперечило б презумпції невинуватості. Правовий зв'язок між особою і її персональними даними, який захищається правом на приватність, не може розриватися свавільно на розсуд державних службовців, у тому числі тих, на які за законом покладаються повноваження здійснювати правоохоронні заходи.

Зрозуміло, що ризик порушення прав людини і, зокрема, права на приватність під час здійснення негласних оперативно-розшукових заходів існує навіть за наявності чітких правових гарантій захисту прав людини, – через недодержання процесуальних

норм внаслідок службової недбалості або ж навмисного перевищення повноважень посадовими особами. У випадку ж відсутності детального регулювання питань збирання, використання і знищення персоніфікованої інформації, а також відсутності законних гарантій відновлення обмежених під час правоохоронної діяльності прав громадян – такий ризик зростає значною мірою.

Показовою для розуміння проблеми узгодження права на приватність персоніфікованої інформації і інтересів суспільства у боротьбі із злочинністю є справа, розглянута Конституційний Судом Російської Федерації, що стосується перевірки конституційності окремих положень Федерального закону "Про оперативно-розшукову діяльність". Вона варта уваги як вітчизняних правознавців, так і правозахисників, оскільки правові традиції регулювання правоохоронної діяльності в Україні і Росії корінням сягають спільного минулого, а тому навіть більш ніж через десять років після відокремлення правових систем формулювання правових приписів у законодавчих актах, що регулюють правоохоронну діяльність, є досить схожими, залишаючи можливості для зловживань і порушення прав людини.

Громадянка Російської Федерації І.Г. Чернова звернулась до Конституційного Суду РФ із скаргою на порушення її конституційних прав положеннями вказаного закону. В червні 1995 року у зв'язку з підготовкою критичних публікацій про роботу волгоградської міліції, журналістка І.Г. Чернова була піддана шантажу з боку посадових осіб УВС Волгоградської області, які погрожували публічно поширити відомості про її приватне життя, здобуті оперативним шляхом. Згідно зі статтею 5 Закону РФ "Про оперативно-розшукову діяльність", вона звернулася зі скаргою для захисту своїх прав до органів прокуратури і суду. В цей час їй стало відомо, що на підставі "агентурного повідомлення" (частина перша ст. 7 федерального закону) про незаконну підприємницьку діяльність на неї було заведено справу оперативного обліку (ст. 10), здійснювалося стеження (ст. 6) з використанням технічних засобів, з ініціативи правоохоронних органів було одержано судове рішення на прослуховування квартирного телефону "для встановлення і документування злочинних зв'язків" (ст. 9).

Після втручання Генеральної прокуратури Російської Федерації їй було повідомлено, що оперативно-розшукові заходи щодо неї були припинені в січні 1996 року, при цьому жодних порушень закону встановлено не було, однак при цьому не було встановлено і самого факту правопорушення з боку І.Г. Чернової або інших осіб. Незважаючи на вимоги заявниці, щодо неї не було прийнято жодних процесуальних рішень ні про порушення, ні про відмову в порушені кримінальної справи, що стало причиною відмови в наданні їй для ознайомлення зібраної про неї інформації (ч. 3 статті 5 Федерального закону). Після тривалих і неодноразових вимог судді певна оперативна інформація була направлена у секретному порядку до Волгоградського обласного суду, де розглядалась скарга заявниці. Однак Управління внутрішніх справ віднесло цю інформацію до відомостей, що містять "державну таємницю" (стаття 12 Федерального закону), на цій підставі заявниці було відмовлено в ознайомлені з ними. Після чого, за "непотребом" оперативні матеріали були повернуті до УВС і знищені у вересні 1997 року на підставі "відомчих інструкцій", що стало причиною припинення розгляду справи за скаргою заявниці.

Конституційний Суд Російської Федерації не розглядав справу по суті, а визнав її неприйнятною, мотивуючи це тим, що права заявниці були порушені невірним застосуванням положень Федерального закону "Про оперативно-розшукову діяльність", а не його невідповідністю Конституції [147].

Разом з тим, чотири судді з п'ятнадцяти, що становили склад суду, не погодилися з прийнятою ухвалою і висловили окремі думки. Найбільш ґрунтовною, вдається позиція судді А.Л. Кононова, який піддав справедливій критиці висновки Конституційного Суду Російської Федерації по цій справі, а також відповідні положення Федерального закону "Про оперативно-розшукову діяльність".

Зокрема, позиція судді А.Л. Кононова щодо невідповідності положень Федерального закону "Про оперативно-розшукову діяльність" Конституції Російської Федерації була обґрунтована посиланнями на принципи, які виробив Європейський Суд під час розгляду численних справ щодо правомірності застосування обмежень певних прав людини. Указані принципи суддя Конституційного Суду Російської

Федерації застосував до обставин конкретної справи. Ідеться про підстави, а також межі для втручання в права людини під час оперативно-розшукової діяльності:

- обмеження можуть бути встановлені тільки у федеральному законі у цілях захисту не від будь-якого правопорушення, а лише від найбільш небезпечних злочинних порушень закону;
- оперативно-розшукові заходи можуть здійснюватися лише тоді, коли в інший спосіб досягнути поставленої мети неможливо;
- рамки правомірного обмеження права на приватність персоніфікованої інформації під час оперативно-розшукової діяльності повинні встановлюватися, зважаючи на характер, суб'єктний склад, термін можливих обмежень і повинні гарантувати їх підконтрольність;
- в органа оперативно-розшукової діяльності повинен виникати обов'язок повідомити зацікавленій особі про наявність щодо нього документованої чи іншої інформації і надати таку інформацію на її вимогу;
- має існувати регламентація процедури перевірки доказів і оцінки доводів оперативних органів для вирішення судом загальної юрисдикції питання про проведення оперативно-розшукових заходів, які обмежують конституційні права громадян.

Більш докладний аналіз цієї справи подається у монографії, написаній автором цієї дисертації [[148], *19-23*].

Підсумовуючи зазначене, можна сформулювати такі узагальнені вимоги до нормативно-правового регулювання обмежень прав громадян у зв'язку з обробкою персональних даних в правоохоронній діяльності: на всіх етапах від збирання до знищення персоніфікованої інформації мають бути встановлені правові рамки для дій службовців через детальну регламентацію службових прав і обов'язків і бути запроваджені дієві гарантії додержання законності і відновлення обмежених прав громадян.

1.3. Інститут захисту приватності персоніфікованої інформації в міжнародному праві

Закріплення права людини на приватність в універсальних і регіональних міжнародних договорах послужило основою для розвитку системи спеціальних норм і принципів, які становлять сучасний міжнародно-правовий інститут захисту приватності персоніфікованої інформації. При цьому, стимулом для становлення і подальшого розвитку цього інституту міжнародного права служать не тільки інтереси міжнародної спільноти у захисті права людини на приватність, а й, значною мірою, інтереси держав у забезпеченні безперешкодності транскордонної передачі персоніфікованої інформації. Останнє пов’язано з тим фактом, що персоніфікована інформація використовується у різних сферах суспільного життя. З огляду на розширення міжнародних інформаційних обмінів, вільна передача інформації незважаючи на кордони стає чинником, що обумовлює успіх міжнародного співробітництва.

У той же час, створення національними урядами штучних перешкод для вільного транскордонного обігу персоніфікованої інформації негативно відбиватиметься на міжнародному співробітництві у багатьох сферах. Розуміння цієї проблеми спонукало міжнародне співтовариство до розвитку співробітництва з метою забезпечення безперешкодності інформаційного обміну, яке призвело до створення сукупності міжнародних норм і принципів, що охоплюються міжнародно-правовим інститутом захисту приватності персоніфікованої інформації.

Міжнародно-правовий інститут захисту приватності персоніфікованої інформації містить відповідні норми й принципи спрямовані на забезпечення безперешкодності передачі інформації через кордони. Однак ця мета нерозривно пов’язана з міжнародно-правовим захистом права людини на приватність персоніфікованої інформації, що становить стрижневий елемент всього міжнародно-правового механізму регулювання транскордонної передачі персоніфікованої інформації.

Російський вчений Ю.М. Колосов зазначає, що “міжнародно-правові норми в галузі здійснення масової інформації, не створюють загальної галузі міжнародного права ... в основі цих норм знаходяться принципи різних галузей права у залежності від того, до якої галузі вони належать в цей час” [24, *153*]. Погоджуючись з цим твердженням відзначимо, що ці норми можуть належати не тільки до певних галузей міжнародного права, а й відноситись до окремих міжнародно-правових інститутів, зокрема, інституту міжнародно-правового захисту приватності персоніфікованої інформації.

Питання комплексного міжнародно-правового забезпечення транскордонних інформаційних обмінів в загальному розумінні, включає не тільки безперешкодність передачі, але й низку проблем забезпечення свободи створення, пошуку, доступу, перетворення та інших операцій з інформацією. Крім того, це нерозривно пов’язано із низкою політико-правових, економічних і технічних аспектів, що стосуються міжнародно-правового забезпечення функціонування і розвитку міжнародних телекомунікацій. Окрім згаданого принципу свободи інформації незалежно від кордонів, американські вчені Марк Зачер і Брент Сьюттон виділяють такі принципи міжнародного режиму телекомунікацій як свобода комерційної діяльності (обов’язок держав усунути перешкоди вільному пересуванню товарів і послуг); ефективність (обов’язок держав забезпечити товари і послуги своєму населенню за найнижчу можливу ціну); транснаціональний контроль за шкодою (обов’язок держав вживати превентивних заходів для унеможливлення неправомірної діяльності резидентів); міжнародний політичний контроль (право держав здійснювати юрисдикцію і контроль за діяльністю на їх територіях) і, останній, принцип рівності, згідно з яким, держави повинні забезпечувати рівність у доступі до ресурсів і фінансових можливостей міжнародної комерції [[149], *136*].

Дослідження цих аспектів міжнародно-правового регулювання телекомунікацій потребує окремого ґрунтовного дослідження і виходить за окреслені рамки дослідження. Питання забезпечення безперешкодності транскордонної передачі персоніфікованої інформації цікавить нас з точки зору захисту права людини на

приватність персоніфікованої інформації (незалежно від кордонів) як складової частини міжнародно-правового захисту прав людини.

Стрімкий розвиток інформаційно-комунікаційних технологій вимагає відповідного пристосування правового регулювання. Під тиском цих обставин, міжнародне правове регулювання питань поводження з персоніфікованою інформацією пройшло певні етапи, що будуть розглянуті нижче.

Російським вченим В.П. Іванським відповідно до періодизації фаз розвитку інформаційного суспільства сформульовані, так звані, "еволюційні форми" інформаційної приватності – масмедійна, комп'ютерна і мереживна [150]. На його думку, вони відповідають домінуючим у визначений час засобам збору й обробки інформації – "основним носіям інформації", у якості яких виступають засоби масової інформації, комп'ютерні бази даних і телекомунікаційні мережі.

Використовуючи запропоновану В.П. Іванським класифікацію, спробуємо охарактеризувати специфіку міжнародно-правового регулювання зазначених форм інформаційної приватності. Концепція масмедійної приватності з'явилася як результат втручання з боку засобів масової інформації (ЗМІ) у приватне життя людини. Хоча національно-правове регулювання захисту масмедійної приватності почало розвиватися більш ніж сто років тому, однак і на сьогоднішній день порушення приватності з боку ЗМІ є поширеними. Регулювання масмедійної приватності ґрунтується на принципі балансування між інтересами людини у недоторканності її приватного життя й інтересами інших осіб в одержані за допомогою ЗМІ інформації, що становить публічний інтерес. Найбільш проблематичним залишається захист приватності громадських діячів, які беруть активну участь у публічному житті, про що вже згадувалось у попередньому підрозділі цієї роботи.

У Декларації про засоби масової інформації та права людини, яка була ухвалена Резолюцією № 428 Парламентської Асамблеї Ради Європи у 1970 році, відзначається складність захисту недоторканості приватного життя публічних осіб. При цьому, зокрема, наголошується, що "приватне життя громадських діячів має захищатися

правом за винятком випадків, коли воно пов’язано з суспільно важливими подіями” [151, *8*].

Результати дослідження проведеного експертами Ради Європи, свідчать про численні втручання у приватне життя навіть у країнах, що мають спеціальне законодавство для його захисту [152]. Однією із причин такої ситуації є надзвичайна прибутковість публікацій, що торкаються приватної сторони життя відомих діячів політики, культури, спорту та ін. А ті грошові суми, що присуджуються судом як компенсація за порушення приватності, не на один порядок нижчі за прибутки засобів масової інформації (ЗМІ) від публікації таких матеріалів.

Ці та інші фактори були відзначені в Резолюції Асамблеї від 26 червня 1998 року №1165, яка являє собою реакцію Ради Європи на нещасний випадок, що стався восени 1997 року із принцесою Уельською Діаною. Зазначена резолюція закликає держави-учасниці привести своє законодавство у відповідність до проголошених у ній керівних принципів. Останні можна поділити на дві категорії. До першої належать ті, що гарантують особі, яка зазнає або вже зазнала втручання у її приватне життя, право на захист у порядку цивільного судочинства:

- судові заборони на переслідування та домагання;
- компенсація моральної шкоди;
- публічне спростування неправдивої інформації;
- спрощений та прискорений судовий розгляд таких справ.

До другої – ті, що передбачають превентивні заходи для запобігання можливим втручанням у приватне життя з боку засобів масової інформації:

- заохочення саморегулювання ЗМІ та розроблення кодексу журналістської поведінки;
- правова освіта журналістів;
- застосування економічних санкцій до редакції ЗМІ, що вдаються до систематичних порушень права на приватність.

Розвиток міжнародного співробітництва з питань регулювання масмедійної приватності стикається з проблемою наявності різних національних правових традицій і розбіжностями щодо проблеми узгодження права на приватність

персоніфікованої інформації і свободи слова. Підходи, обрані європейськими країнами щодо регулювання питань поводження засобів масової інформації з персоніфікованою інформацією, були предметом вивчення Радою Європи та Європейським Союзом. За наслідками дослідження встановлено три основні моделі, що використовуються в національних правових системах деяких європейських країн для регулювання цього питання [153]:

1) Законодавство з захисту приватності персоніфікованої інформації не містить будь-яких спеціальних винятків щодо застосування їх положень до засобів масової інформації. Такою є ситуація в Бельгії, Іспанії, Португалії, Швеції і Великій Британії.

2) ЗМІ виключені із застосування певних положень законодавства із захисту приватності персоніфікованої інформації. Таким є національні положення Німеччини, Франції, Нідерландів, Австрії, Фінляндії та Італії.

3) Зазначене питання регулюється спеціальними нормативними актами. В Данії це застосовується до всіх ЗМІ, а в Німеччині – лише до державних телерадіокомпаній.

Незважаючи на ці розбіжності у законодавчому регулюванні, простежується єдність у підходах зазначених європейських країн – загальні правила захисту приватності персоніфікованої інформації не застосовуються повною мірою до засобів масової інформації з огляду на спеціальний конституційний статус права на свободу інформації. Це, насамперед, стосується питань збору й поширення персоніфікованої інформації. В той же час, інші операції з такою інформацією, зокрема – зберігання, модифікація, передача й знищення, мають підпадати під дію законодавства про захист приватності.

У той же час, запровадження будь-яких регулятивних обмежень на поширення персоніфікованої інформації засобами масової інформації в Сполучених Штатах не можливо з огляду на норму Першої поправки до Конституції США, яка захищає свободу слова. Практика американських судів по тлумаченню Першої поправки надзвичайно цікава і об’ємна. Створені ними прецеденти визначають, серед іншого, межі свободи вираження поглядів, які обумовлені змістом поглядів. За загальним правилом, урядові обмеження свободи слова є неконституційними, якщо вони не обумовлені конкуруючими інтересами держави. Це певним чином співпадає з

формулюванням Європейської Конвенції “необхідне у демократичному суспільстві”, однак критерії оцінки в Сполучених Штатах сформульовані жорсткіше.

Серед основних принципів судової доктрини захисту свободи слова в США є наступні:

- якщо закон не дає чіткого визначення щодо типу висловлювань, які він забороняє, він є недійсним внаслідок неконкретності;

- якщо закон обтяжує більше висловлювань, ніж це потрібно для конкуруючих інтересів держави, він неконституційний через перевищення повноважень;

- урядові обмеження щодо часу, місця і манери вираження поглядів, за яких висловлювання дозволяються, є конституційними, лише за таких умов, що вони є нейтральними щодо змісту, як за формою так і за застосуванням; залишають суттєві можливості, щоб висловлювання мали місце; слугують виключно суттєвим інтересам держави.

Правомірність поширення персоніфікованої інформації взагалі не розглядається судами США, натомість, оцінюється тільки її достовірність. Дифамація може тягнути цивільно-правову відповідальність, однак за таких умов: якщо об’єкт дифамації є публічною фігурою, він повинен довести, що поширювач діяв навмисно; якщо об’єкт не є публічною фігурою, однак заява зачіпає питання суспільної важливості, позивач повинен довести, що поширювач діяв необережно, не перевіривши достовірність персоніфікованої інформації.

Відзначимо, що питання встановлення правових гарантій для запобігання порушенням масмедійної приватності залишається проблематичним. Існуючий засіб національно-правового захисту шляхом подання позову до суду з вимогою про спростування недостовірної інформації та компенсацію моральної шкоди є правовим реагуванням на скоєне деліктне правопорушення “постфактум”. Це можна пояснити специфікою діяльності ЗМІ, для яких перевірка достовірності інформації чи, тим паче, одержання попередньої згоди на публікацію від зацікавлених осіб загрожує якщо не забороною на поширення інформації, то втратою її актуальності. Отже, для захисту масмедійної приватності проблемним залишається врегулювання таких

операцій з персоніфікованою інформацією, як її збір і поширення засобами масової інформації, які не можуть контролюватися зацікавленою особою.

Проблема регулювання змісту, який поширюється засобами масової інформації, не є новою для міжнародного права. Однак вищенаведені розбіжності національних підходів щодо узгодження права на приватність і свободи слова мають наслідком відсутність консенсусу з цього питання на міжнародному рівні. Хоча з інших питань унормування міжнародної масової інформації світове співтовариство знаходило компроміс, який зафіксований, зокрема, в таких міжнародно-правових джерелах: Міжнародна конвенція про припинення обігу порнографічних видань та торгівлі ними 1923 року [154], Міжнародна конвенція про використання радіомовлення в інтересах миру 1936 року [155], Резолюція 110 (II) Генеральної Асамблеї ООН "Заходи, що повинні бути вжиті проти пропаганди і розпалювачів нової війни" 1947 року [156], Резолюція 127 (II) Генеральної Асамблеї ООН "Брехлива або спотворена інформація" 1947 року [157], Міжнародна конвенція про ліквідацію всіх форм расової дискримінації 1965 року [158], Резолюція 2037 (XX) Генеральної Асамблеї ООН Декларація про поширення серед молоді ідеалів миру, взаємної поваги і взаєморозуміння між народами 1965 року [159], Декларація щодо основних принципів, що стосуються внеску засобів масової інформації у зміцнення миру та міжнародного взаєморозуміння, у розвиток прав людини і у боротьбу проти расизму і апартеїду та підбурення до війни 1978 року [160] тощо.

Вищезазначені міжнародні документи науковці відносять до нової галузі міжнародного права, що знаходиться у стані становлення, - міжнародного права масової інформації (комунікації). У підручнику відомих російських вчених міжнародників Ю.М. Колосова і В.І. Кузнєцова, зокрема, зазначається, що необхідність міжнародного співробітництва у галузі поширення масової інформації викликається, серед іншого, "доцільністю заборони деяких ідей і заохочення інших, що впливають на формування громадської думки" [161, *456*]. Огляд цих міжнародних документів свідчить, що регулювання змісту інформації під час міжнародного інформаційного обміну, має на меті реалізацію здебільше публічних інтересів щодо обмеження поширення інформації, що може завдавати шкоду суспільству. У той же

час, будь-яке обмежувальне регулювання свободи поширення інформації несе загрозу можливого використання не на користь інтересам суспільства, зокрема, для політичної цензури, приборкання демократичної опозиції.

Суттєвим для розуміння особливостей міжнародно-правового регулювання масмедійної приватності є врахування вимоги щодо узгодження двох фундаментальних прав людини, права на приватність і свободи слова. Міжнародні документи у галузі прав людини передбачають можливість обмеження свободи вираження поглядів (свободи слова) в інтересах суспільства, а також для захисту прав інших осіб. Частина 3 статті 19 Міжнародного Пакту про громадянські і політичні права “накладає особливі обов'язки і особливу відповідальність” у зв’язку з користуванням правом на свободу вираження поглядів. Таке користування може обмежуватися на підставі закону, якщо це є необхідним: а) для поважання прав і репутації інших осіб; б) для охорони державної безпеки, громадського порядку, здоров'я чи моральності населення. Право людини на приватність персоніфікованої інформації підпадає під категорію а), оскільки порушення права на приватність з боку засобів масової інформації, у більшості випадків, має наслідком завдання шкоди репутації окремої особи.

Перелік обмежень свободи вираження поглядів, передбачений у статті 10 Європейської Конвенції про захист прав людини та основних свобод, є дещо більшим і включає, до того ж, вимогу запобігання розголошенню інформації, одержаної конфіденційно. Це також включає розголошення персоніфікованої інформації, як один з видів порушення права на приватність.

Необхідність балансування інтересів окремої особи у захисту приватності персоніфікованої інформації і інтересів суспільства у доступі до суспільно-важливої інформації визнається як один із стрижневих принципів міжнародно-правового регулювання захисту приватності персоніфікованої інформації у сфері діяльності засобів масової інформації, що обумовлює складність вирішення проблеми захисту приватності персоніфікованої інформації за допомогою міжнародних інструментів. Саме ці, згадані у попередньому підрозділі норми основних міжнародно-правових домовленостей у галузі прав людини, що передбачають можливість легітимного

обмеження як права на свободу вираження поглядів, так і права на приватність становлять основу міжнародного регулювання масмедійної приватності. Однак ці загальні норми з огляду на розбіжності в практиці їх застосування на національному рівні потребують уніфікації шляхом ухвалення спеціальних міжнародно-правових актів.

Наступною формою інформаційної приватності за класифікацією В.П. Іванського є комп'ютерна. Міжнародно-правові питання поводження з персоніфікованою інформацією стають надзвичайно актуальними, коли потреби міжнародного співтовариства у використанні такої інформації стають все більшими. На початку 70-х років двадцятого століття, з появою перших комп'ютерів і автоматизованої обробки інформації, починають розроблятися перші національні нормативні акти, спрямовані на регулювання поводження з інформацією про індивідів у машинописній формі даних. Так набуває свого розвитку концепція комп'ютерної приватності, яка перед тим як знайти своє відображення в міжнародному праві, пройшла певну еволюцію на національному рівні.

Поширеним терміном, що використовується для позначення сукупності правил поводження з персональними даними у законодавстві європейських країн, датованому 70-80-и роками двадцятого століття, є "захист даних" ("data protection"). Проаналізувавши еволюції законів деяких європейських країн, німецький науковець Майор-Шонбергер, відмітив, що переважна більшість чинного законодавства країн Європи, що захищає право на приватність персоніфікованої інформації, бере свої витоки з положень про технічний захист інформації [[162], *224*]. Звідси походить не зовсім коректне, на нашу думку, формулювання "захист даних", оскільки захисту потребують не стільки дані, скільки права осіб, яких стосується персоніфікована інформація, а також легітимні інтереси усього суспільства. Суб'єктові даних, тобто особі, чиї дані знаходяться в автоматизованих системах, першим поколінням нормативних актів надається незначний обсяг прав. Індивід має лише право доступу й виправлення даних, якщо вони були неточними. Надання таких прав було зумовлено, серед іншого, і вимогами щодо підтримання ефективності функціонування автоматизованих систем.

На цьому етапі розвитку правового регулювання комп'ютерної приватності можна відмітити певну спадковість концепції масмедійної приватності. Основний інтерес особи за концепцією комп'ютерної приватності на цій стадії розвитку полягає саме в якості інформації. Дані про особу мають бути точними й поновленими. Відмітимо, що так само і в масмедійній приватності: публікація недостовірної інформації про людину має бути спростована на вимогу зацікавлених осіб. Крім того, правові питання, що виникають під час збору й обробки персоніфікованої інформації не вважаються такими, що можуть мати під собою підстави у вигляді певних інтересів людини: збір і обробка персоніфікованої інформації виправдовується публічними інтересами щодо адміністрування баз даних державними органами під час виконання покладених на них функцій чи приватними організаціями для здійснення комерційної діяльності. У той час як в концепції масмедійної приватності таким публічним інтересом, що виправдовує збирання й поширення відомостей про особу без її згоди, є права інших осіб на свободу інформації.

Подальший розвиток комп'ютерної приватності знаменувався значним розширенням прав суб'єктів даних і правовою регламентацією всіх операцій з персональними даними від збирання до знищення. Створений у більшості розвинутих країн механізм захисту приватності персональних даних надає суб'єктові даних можливість контролювати поводженням із даними під час будь-яких операцій з ними. Ця можливість ґрунтується на таких правах суб'єкта даних, як право знати про ціль збору і правомірні підстави для цього, їх майбутніх одержувачів; отримати копію даних, що були зібрані, включаючи інформацію про їх використання; вносити корективи, знищувати або блокувати (забороняти використання) даних, що обробляються з порушенням закону; також вимагати повідомлення про це сторонам, яким ці дані було розкрито тощо.

До того ж, в концепції комп'ютерної приватності запроваджується докладна регламентація правил поводження з даними. Персональні дані повинні:

(а) оброблятися на правомірних і законних підставах;

(б) збиратися для спеціальних, визначених і правомірних цілей та використовувати у спосіб, сумісний з такими цілями;

(в) бути адекватними, достатніми і не надмірними щодо таких цілей;

(г) бути точними і не застарілими;

(д) не зберігатися у формі, що дозволяє ідентифікацію особи, довше, ніж це потрібно для таких цілей.

Ця система прав суб'єкта даних, якій кореспондують відповідні обов'язки інших суб'єктів цих відносин, дозволяє реалізувати людині право на приватність персоніфікованої інформації в автоматизованих і неавтоматизованих базах даних. Отже, правове забезпечення комп'ютерної приватності вимагає не лише захисту "постфактум" як за масмедійною формою приватності, а й створення правового механізму активної реалізації права на приватність. Це право не є негативним, тобто таким, що лише забороняє іншим суб'єктам його порушувати. Його головним елементом є активні інформаційні права суб'єкта даних на доступ до інформації, виправлення неточної інформації, право визначати умови, за яких здійснюються операції з даними, право заперечувати обробці певної категорії даних та вимагати перевірки законності обробки тощо.

Зрозуміло, що перелічені вимоги до регулювання комп'ютерної приватності не можуть повною мірою застосовуватися до засобів масової інформації, з огляду на специфіку їх діяльності, в основі якої – право на свободу інформації, вільне отримання й поширення інформації про індивідів тощо. Разом з тим, відсутність належного регулювання цього питання може спричинитися до порушення прав осіб на захист у зв'язку із збором і обробкою інформації про них засобами масової інформації. Треба враховувати й сучасні тенденції розвитку масмедійного сектора, зокрема, використання новітніх телекомунікаційних і мультимедійних технологій для створення й поширення інформаційного продукту. Ці ж технології полегшують збір, зберігання й обробку інформації про користувачів інформаційних послуг, що посилює значення захисту приватності.

Серед проблем регулювання захисту комп'ютерної приватності найбільш актуальним залишається питання обмеження збору персоніфікованої інформації. Активіст правозахисної організації "Прайвесі Інтернешнл" Саймон Девіс вважає, що це є основним недоліком сучасного покоління нормативних актів у цій галузі,

оскільки вони залишають поза увагою законодавця питання обмеження збирання персоніфікованої інформації, а зосереджується в основному на регулюванні процедури їх збирання, зберігання, використання й доступу [163, *150-152*]. Колишній Федеральний уповноважений Канади з питань приватності і свободи інформації, Девід Флехерті також відзначає на прикладі Британської Колумбії, що на законодавчому рівні інтереси особи у захисту від суцільного збирання персоніфікованої інформації визначені неадекватно, хоча це питання є основним для захисту права особи на приватність [164, *171*].

Вироблені на національному рівні норми й принципи захисту комп'ютерної приватності закріплені в спеціальних міжнародно-правових актах: Конвенції Ради Європи про захист осіб стосовно автоматизованої обробки персональних даних 1981 року, "Керівних принципах, що регулюють захист приватності і транскордонні потоки персональних даних" Організації Економічного Співробітництва і Розвитку 1980 року, "Керівних принципах стосовно комп'ютеризованих файлів персональних даних", ухвалених Генеральною Асамблеєю ООН у 1990 році тощо. Зазначені міжнародно-правові акти докладно розглядаються нами у наступному розділі дослідження.

Наступною формою інформаційної приватності за класифікацією В.П. Іванського є мереживна приватність. Саме прогрес інформаційних (телекомунікаційних і мультимедійних) технологій уможливив виникнення цієї форми, яка зобов'язана своєю появою поєднанню комп'ютерів із телекомунікаціями. Концепція мереживної приватності лише починає формуватися. На цьому етапі існують значні труднощі із міжнародно-правовим забезпеченням захисту мереживної приватності, пов'язані зі стрімким технічним прогресом, за яким не поспіває міжнародно-правове регулювання, насамперед з регулюванням правових відносин щодо збирання, передачі і використання персоніфікованої інформації в глобальній телекомунікаційній мережі Інтернет.

Зупинимось на характеристиці причин, які обумовлюють наявність цих труднощів. Через відкритість Інтернет та її особливість як системи, що може накопичувати й обробляти інформацію про людину, надзвичайно актуальним стає

питання забезпечення приватності під час користування трансляційно-комунікативними можливостями цієї глобальної мережі. Кожний з операторів Інтернету є проміжною ланкою і має можливість втручання у цей процес. Оператори можуть дізнатися не тільки про зміст повідомлення, а й отримати додаткову інформацію. Стандартне повідомлення електронною поштою містить заголовок з інформацією про відправника та кореспондента, яка включає в себе ім'я, Інтернет-адресу, назву вузла, час листування. Інтернет несе загрозу приватності користувачів не тільки під час обміну повідомленнями. З появою унікального адресного простору у вигляді веб-сторінок право на повагу до приватного життя користувача доповнюється новим змістом. Ідеться про захист недоторканності "віртуального життя" користувача в мережі. Кожна веб-публікація має свою унікальну адресу, за якою вона знаходиться. Щоб дістати потрібні публікації чи послуги "он-лайн", користувач має вступити у контакт із постачальниками цих публікацій чи послуг у діалоговому режимі. При цьому інформація про користувача починає збиратися програмними засобами з його комп'ютера під час першого звернення до інформаційних ресурсів веб-сторінки ще до встановлення будь-якого контакту з постачальником інформаційного змісту.

Рухаючись рівень за рівнем в інформаційному "павутинні" Інтернет, користувач залишає за собою інформаційний слід у вигляді операційних даних (**англ.** *transactional data*). Ці дані включають Інтернет-адресу комп'ютера користувача, інформацію про програмне забезпечення, тип комп'ютера, відвідувані веб-сторінки, а також про попередні візити до цієї сторінки. Такі дані є багатим джерелом інформації про поведінку користувача у мережі, що, у свою чергу, може бути використано і використовується для створення "профілю" користувача – сукупності характеристик, якими охоплюються його смаки, звички, мотивації під час користування Інтернет. Зіставлення цієї інформації з іншими даними дозволяє ідентифікувати людину, причому здебільшого у випадках, коли людина й гадки не має про те, яка персоніфікована інформація і з якою метою збирається й опрацьовується. Про зазначені загрози приватності в Інтернет зазначається, зокрема, в Рекомендаціях, ухвалених Робочою групою Європейського Союзу [165].

Ризик приватності людини існує й при користуванні такою можливістю Інтернет як електронні послуги (електронна пошта, пошукові послуги, ігри, участь у дискусійних групах за інтересами або спілкування в режимі реального часу), які є доступними через телефонну мережу з використанням модему й комп'ютера [166]. Як для функціонування будь-якої із традиційних електронних систем, для послуг "он-лайн" потрібна інформація про користувача. Вона використовується в таких процесах, що відбуваються під час роботи в електронних системах: авторизація, ідентифікація й посвідчення, контроль права доступу, ревізія й розрахунок. Постачальники послуг "он-лайн" збирають і опрацьовують персональні дані про особу користувача, оскільки це потрібно для роботи електронних систем. Однак контроль за їх використанням у користувача обмежений.

Ризики приватності людини в мережі посилюються тим, що Інтернет дає можливість порушення права на приватність не лише операторам, які безпосередньо збирають дані про користувача. Програмне забезпечення на сучасному етапі розвитку дозволяє здійснювати цілеспрямований пошук, зіставлення й систематизацію всієї доступної у мережі інформації про визначеного користувача, яка колись туди потрапила. Це включає адресу й телефоні номери, місце народження, навчання, роботи, професію, смаки й звички, висловлювання та інші відомості.

Отже, можна стверджувати, що Інтернет успадкував існуючі проблеми захисту прав людини за масмедійною і комп'ютерною формами приватності. Як засобу масової комунікації, Інтернету властиві основні проблеми зазначених форм приватності, а саме, технічне ускладнення можливості для користувача контролювати й обмежувати збір і подальше поширення персоніфікованої інформації.

Вирішити питання захисту приватності користувачів Інтернет можливо за умов застосування комплексу заходів на організаційному, технічному і нормативному, насамперед міжнародно-правовому, рівнях. Перш за все, на організаційному рівні науковцями пропонується створити міжнародний наглядовий механізм за дотриманням приватності користувачів Інтернет у рамках існуючої системи технічно-нормативного регулювання Інтернет за допомогою стандартизації. Разом із тим, процес стандартизації відображає динаміку ринку і сам є підприємницькою

діяльністю. Внаслідок спрямованості процесу стандартизації на потреби ринку, публічні інтереси і права користувачів не завжди мали належне нормативно-технічне втілення [167]. На сучасному етапі ситуація починає змінюватися. Так, з'являються концепції і технічні розробки, які дають можливість користування телекомунікаційними послугами без ідентифікації особи користувача [168]. Анонімність послуговування Інтернет визнається як один із суттєвих принципів, що дозволяє гарантувати певний рівень приватності під час користування цією глобальною мережею. З іншого боку, справедливо відзначається, що принцип анонімності, завдяки чому можна уникнути ідентифікації, ускладнює роботу правоохоронних органів по боротьбі з незаконним змістом в Інтернет, фінансовим шахрайством або порушенням авторських прав. Ці доводи, з якими важко не погодитися, зазначаються у спеціальній Рекомендації Робочої групи Європейського Союзу [169].

Слід звернути увагу і на такий механізм, як саморегуляція телекомунікаційного сектора через прийняття кодексів "чесної інформаційної практики" і систему засвідчення відповідності такої практики проголошеним стандартам. Щоправда, такий підхід справедливо критикується прихильниками ідеї державного регулювання за його слабкість у вирішенні питання притягнення порушників до відповідальності [170].

Закріплені в існуючих міжнародно-правових актах основні засади захисту права на приватність потребують адаптації для застосування в Інтернет. З цією метою відомий учений, колишній керівник робочої групи з розробки Керівних принципів захисту приватності ОЕСР 1980 року, М.Д. Кербі пропонує, відповідаючи на вимоги часу, розробити нові або адаптувати наявні міжнародно-правові акти у галузі захисту приватності персоніфікованої інформації для застосування в глобальній телекомунікаційній мережі. Зокрема, він пропонує включити "нові" суб'єктивні права, які зможуть гарантувати захист приватності в Інтернет:

- право не бути внесеним до списків;
- право на ефективне шифрування персоніфікованої інформації;

- право на справедливе поводження з людиною у сфері використання системи шифрування “відкритим ключем”;

- право на розкриття людині даних, що можуть бути використані для створення його споживчого профілю [[171], *3*].

Важливість забезпечення захисту права осіб на приватність під час користування Інтернет підкреслюється в Рекомендаціях Комітету Міністрів Ради Європи, ухвалених 23 лютого 1999 року на 660-у засіданні заступників міністрів. В зазначених Рекомендаціях, що мають дотримуватися країнами-членами Ради Європи, наголошується на наступних принципах:

- застосування програмних та технічних засобів захисту персоніфікованої інформації повинно заохочуватись;
- анонімний доступ і використання послуг, у тому числі здійснення оплати анонімно – є найкращим захистом приватності;
- збирання, обробка й використання персоніфікованої інформації в Інтернет підпадає під дію міжнародних норм й принципів, зокрема тих, що містяться у Конвенції Ради Європи № 108 1981 року;
- таємниця електронних комунікацій повинна поважатись і забезпечуватись, у тому числі шляхом застосування постачальниками послуг відповідних засобів захисту;
- передача персоніфікованої інформації через кордони під юрисдикцію інших країн дозволятиметься на підставі закону, якщо це не призведе до порушення або навіть до зменшення рівня захисту.

Для захисту права людини на приватність персоніфікованої інформації в Інтернет, суттєву роль мають відігравати саме міжнародні інструменти, оскільки це глобальне, як сам Інтернет, питання має вирішуватися саме на міжнародному рівні. Не випадково, що питання захисту приватності персоніфікованої інформації з огляду на розвиток інформаційних технологій є предметом уваги Великої Вісімки. На Бірмінгемському самміті у травні 1998 року це питання розглядалося у контексті проблеми боротьби з міжнародною злочинністю, а на самміті 2000 року в Окінаві – через призму розвитку Інформаційного Суспільства. В Хартії з питань

Інформаційного Суспільства учасники самміту, прагнучи максимізувати соціальні й економічні вигоди Інформаційного Суспільства, дійшли згоди про важливість такого пріоритету як “розвиток ефективного й комплексного захисту приватності для споживачів, а також захист приватності під час обробки персональних даних, гарантуючи, водночас, вільні потоки інформації” [172][1)].

Слід звернути увагу на той факт, що у зазначеному документі, так само як і у більшості інших міжнародних документів у цій галузі (вони детально досліджуються нами у другому розділі цієї роботи), питання захисту приватності розглядається нерозривно від забезпечення вільного або безперешкодного руху інформації, що є життєво важливим для будь-якого суспільства, а також міжнародного співробітництва.

Проблема міжнародно-правового забезпечення безперешкодності передачі персоніфікованої інформації є актуальною в усіх трьох згаданих концепціях приватності: масмедійній, комп’ютерній і мереживній. В концепції масмедійної приватності основою цьому є право на свободу вираження поглядів, що є основою демократичного розвитку суспільств; в концепції комп’ютерної приватності, з огляду на національні розбіжності, – економічні і політичні інтереси окремих держав; в концепції мереживної приватності – інтереси розвитку інформаційного суспільства. Усі вони знайшли своє відображення у відповідних міжнародно-правових нормах і принципах. Розглянемо їх детальніше.

Свобода вираження поглядів визнається як фундаментальне право людини в численних міжнародних документах присвячених правам людини: статті 19 Загальної Декларація прав людини 1948 року, статті 19 Міжнародного пакту про громадянські і політичні права, статті 10 Європейської Конвенції про захист прав людини та основних свобод тощо.

Як справедливо зазначають відомі захисниками свободи слова в Інтернет Дж. Демпсі, Д. Вейцнер: “Прозорливе формулювання Статті 19, “будь-якими засобами”, робить його цілком придатним щодо свободи вираження за допомогою Інтернет. Права “шукати” і “поширювати” інформацію виглядає особливо придатним для

[1)] [168] Okinawa Charter on Global Information Society. — Okinawa, 2000.

“серфінгу” в мережі і розміщення інформації для всіх на веб-сторінках для читання, у той час як право “одержувати” інформацію охоплює обмін електронною поштою і зчитування інформації” [[173], *13*].

Крім цих основоположних норм, які закладають фундамент для забезпечення безперешкодності транскордонної передачі персоніфікованої інформації, існує низка універсальних і регіональних міжнародних домовленостей спрямованих на усунення можливих технічних або комерційних перешкод для передавання масової інформації, зокрема, Конвенція про розповсюдження сигналів, що несуть програми і передаються через супутники 1974 року [[174]], Конвенція Міжнародного союзу електрозв'язку 1991 року [[175]], Європейська Конвенція про транскордонне телебачення 1989 року та інші.

Як зазначалось вище, в міжнародно-правових актах, які нормативно втілюють концепцію комп’ютерної приватності, мета забезпечення безперешкодності має основу в економічних і політичних інтересах окремих держав. В Рекомендаціях Ради ОЕСР стосовно Керівних принципів, що регулюють захист приватності і транскордонні потоки персональних даних, зокрема, зазначається, що “... автоматизована обробка і транскордонні потоки персональних даних породжують нові форми відносин між країнами і вимагають вироблення відповідних правил і практики; транскордонні потоки персональних даних сприяють економічному й соціальному розвитку; внутрішнє законодавство з захисту приватності стосовно транскордонних потоків персональних даних може перешкоджати таким транскордонним потокам...”[[176], *46-50*].

Саме необхідність забезпечення інтересів спільного ринку є ключовою причиною запровадження загальноєвропейських стандартів захисту приватності персоніфікованої інформації в праві Європейського Союзу. Підтвердження цьому ми знаходимо в тексті Директиви 95/46 СЕ Європейського Парламенту і Ради “Про захист фізичних осіб стосовно автоматизованої обробки персональних даних та безперешкодного руху цих даних”, де мета її ухвалення окреслюється не тільки необхідністю захисту фундаментальних прав і свобод людини, але й потребами вільної конкуренції та забезпечення діяльності державних органів. Європейська Комісія звертає увагу на важливості саме останніх інтересів, які обумовили прийняття

цього акту на рівні ЄС. На цьому наголошується й у першій доповіді щодо імплементації Директиви [177].

Слід зазначити, що в міжнародно-правових актах, які нормативно втілюють концепцію комп'ютерної приватності, питання забезпечення безперешкодності безпосередньо пов'язано з реалізацією як норм, що встановлюють правила транскордонної передачі, так і механізму міжнародного співробітництва у цій сфері, використання процедури консультацій і діяльності координаційних і робочих органів. Міжнародно-правове забезпечення безперешкодності потоків персоніфікованої інформації в глобальній мережі Інтернет знаходиться на початковій стадії свого розвитку, так само як й низка інших політико-правових проблем, пов'язаних з Інтернет.

Необхідність усунення перешкод для вільної передачі інформації в Інтернет викликала прийняття 28 травня 2003 року Комітетом Міністрів Ради Європи Декларації про свободу комунікацій в Інтернет, що була затверджена на 840-у засіданні заступників міністрів. Декларація торкається низки політико-правових питань, пов'язаних з правами й свободами користувачів Інтернет. Декларація забороняє обмеження загального доступу до комунікацій в Інтернет з політичних мотивів чи інших мотивів, що суперечить демократичним принципам; вимагається усунення бар'єрів для індивідуального доступу до Інтернет; наголошується на свободі надання послуг через Інтернет, що сприятиме забезпеченню права користувачів на доступ до плюралістичного вмісту з низки місцевих і зарубіжних джерел, на встановлені балансу між інтересом користувачів Інтернет не розкривати своєї особи і потребами правоохоронних органів відслідковувати осіб відповідальних за кримінальні вчинки тощо. Останнє є суттєвим для захисту права на приватність в мережі Інтернет, про що згадувалось нами вище при розгляді концепції мереживної приватності.

Висновки до розділу 1

Проведене у першому розділі дослідження загальнотеоретичних та історичних основ міжнародно-правового захисту приватності персоніфікованої інформації можна підсумувати, сформулювавши наступні наступні висновки:

Персоніфікована інформація є відображенням індивідуальності людини як носія певних елементів фізичної, фізіологічної, психічної, економічної культурної або соціальної тотожності. Розвиток засобів збирання і передачі інформації несе ризики неправомірного використання персоніфікованої інформації, втручання у приватне життя, що потребує адекватного правового забезпечення.

У світовій правовій теорії і практиці для позначення правового інституту, який захищає недоторканність приватного життя та інші пов'язані права, зокрема, щодо поводження з персоніфікованою інформацією, використовується термін "прайвесі", який пропонується перекладати українською мовою як "приватність".

Право на приватність персоніфікованої інформації як складова частина права на приватність (right to privacy) є загальновизнаним правом людини, що підтверджується його закріпленням в міжнародно-правових актах, присвячених правам людини, в спеціальних міжнародних документах, а також в національних конституціях серед інших основних прав і свобод людини. Визнання й утвердження права на приватність персоніфікованої інформації на національному рівні відбувається як шляхом судового тлумачення, так і через нормативне закріплення в текстах конституцій. Закріплення в статті 34 Конституції України права громадянина на контроль за використанням та доступ до персоніфікованої інформації як складової права на приватність відповідає сучасній міжнародно-правовій доктрині у галузі прав людини.

Право на приватність персоніфікованої інформації не є абсолютним, оскільки існують конкуруючі інтереси інших осіб, суспільства і держави. Щоб бути легітимними, обмеження права на приватність мають відповідати таким вимогам: запроваджуватися на підставі закону, мати легітимну ціль, бути необхідним у

демократичному суспільстві. Правова конкуренція права на приватність персоніфікованої інформації з правом на свободу інформації та інтересами суспільства у боротьбі із злочинністю вимагає від держави створення механізму погодження задіяних інтересів шляхом встановлення справедливого балансу, а також оцінки застосованих обмежень на відповідність принципу пропорційності.

Міжнародно-правовий інститут захисту приватності персоніфікованої інформації складається з системи загальних і спеціальних норм, які забезпечують право людини на приватність, у тому числі під час передачі персоніфікованої інформації через кордони. Стимулом для його становлення і подальшого розвитку є соціальні (захист загальновизнаного права людини на приватність) та економічні (безперешкодність транскордонної передачі) інтереси держав.

Міжнародно-правовим регулюванням охоплюються питання використання персоніфікованої інформації засобами масової інформації (проблема узгодження із свободою слова), комп'ютерна обробка персоніфікованої інформації (правила збирання, зберігання, використання та поширення, у тому числі через кордони), а також гарантування захисту приватності в глобальній телекомунікаційній мережі Інтернет.

Міжнародно-правовий інститут захисту приватності персоніфікованої інформації містить відповідні норми й принципи спрямовані на забезпечення безперешкодності передачі інформації через кордони. Безперешкодність транскордонної передачі персоніфікованої інформації забезпечується загальними міжнародно-правовими нормами щодо свободи інформації незважаючи на кордони, положеннями міжнародно-правових актів щодо усунення перешкод для обміну персоніфікованою інформацією між країнами, що гарантують захист права на приватність, а також нормами спеціальних міжнародно-правових актів у галузі розвитку телекомунікацій.

РОЗДІЛ 2
МІЖНАРОДНО-ПРАВОВЕ РЕГУЛЮВАННЯ ВІДНОСИН ЩОДО ОБРОБКИ ПЕРСОНІФІКОВАНОЇ ІНФОРМАЦІЇ ТА ЇЇ ПЕРЕДАЧІ ЧЕРЕЗ КОРДОНИ

Усвідомлення важливості захисту права людини на приватність персоніфікованої інформації під час її обробки і передачі через кордони спонукало міжнародне співтовариство до пошуку компромісів з метою узгодження національних підходів для ліквідації штучних перешкод інформаційному обміну. Діяльність міжнародних організацій у цій сфері спрямовується як на універсалізацію правових стандартів, так і на вироблення міжнародно-правових засобів розв'язання існуючих розбіжностей.

Другий розділ дослідження присвячується актуальним питанням міжнародно-правового регулювання відносин щодо обробки персоніфікованої інформації та забезпечення її безперешкодної передачі через кордони. З цією метою ставиться завдання здійснити аналіз чинних міжнародно-правових актів з цих питань, прийнятих такими міжнародними організаціями як Рада Європи, Організація Економічного Співробітництва і Розвитку та ООН , а також виявити тенденції подальшого розвитку міжнародних стандартів (підрозділ 2.1). У підрозділі 2.2 розглядаються особливості регулювання зазначених відносин за правом Європейського Союзу, у тому числі в контексті правоохоронної діяльності. Дослідженню міжнародно-правових засобів розв'язання проблеми захисту приватності в контексті транскордонної передачі персоніфікованої інформації присвячується третій підрозділ другого розділу роботи. Розгляд зазначених питань викликаний необхідністю дослідження проблеми узгодження національних правових розбіжностей для забезпечення безперешкодності інформаційного обміну через кордони і, зокрема, вільної від штучних перешкод транскордонної передачі персоніфікованої інформації.

2.1. Міжнародно-правові акти щодо захисту приватності і безперешкодної транскордонної передачі персоніфікованої інформації

Проблема забезпечення безперешкодного руху персоніфікованої інформації між різними юрисдикціями почала означуватися на початку 80-х років двадцятого століття. Неузгодженість національних підходів і діяльності відповідних органів мала наслідком появу заборон на передачу персональних даних через кордони, що стало бар'єром для зовнішньоекономічних стосунків партнерів по бізнесу у різних країнах. Так, у 1978 році один з Комітетів Великої Британії доповідав про два випадки відмови з боку владних структур Швеції дозволити експорт персональних даних на підставах, що національне законодавство Великої Британії на той час не містило положень, які б гарантували захист приватності персональних даних. У свою чергу, у грудні 1990 року, Реєстратор персональних даних Великої Британії заборонив передачу даних до США, обґрунтувавши своє рішення тим, що законодавство США не надає адекватного рівня захисту у приватному секторі [178].

Вирішити цю проблему на національному рівні було неможливо з огляду на існуючі розбіжності у національних підходах. Зростаючий транскордонний обмін інформацією вимагав ужиття негайних заходів на міжнародному рівні. Зусилля, спрямовані на створення міжнародних стандартів для узгодження національних положень щодо захисту приватності й транскордонної передачі персональних даних, були здійснені, зокрема, такими міжнародними організаціями, як Рада Європи, Організація Економічної Співпраці і Розвитку (ОЕСР) і Організація Об'єднаних Націй. Починаючи з 70-х років двадцятого століття, створені цими міжнародними організаціями групи експертів займаються розробкою і вдосконаленням стандартів у галузі захисту приватності і безперешкодності транскордонних потоків персональних даних з метою гармонізації національних положень, ліквідації неузгодженостей в питанні передачі даних через кордони.

На відміну від Організації Економічного Співробітництва і Розвитку, організації створеній на основі спільного економічного інтересу держав-членів, основним завданням Ради Європи був і залишається захист прав людини та основних свобод. На Раді Європі лежить політична відповідальність за розвиток права на повагу до приватного життя, яке гарантовано статтею 8 Європейської Конвенції про захист прав людини та основних свобод 1950 року, а також права на свободу інформації незважаючи на кордони, гарантованого статтею 10 цієї ж Конвенції.

Комітет Ради Європи з правових питань сформував Комісію експертів з приватності та комп'ютерів у 1971 році. Перші кроки були зроблені у напрямку встановлення спеціальних принципів та норм для запобігання неправомірному збору і обробці персональних даних у електронних базах даних. Комісія підготувала проекти двох резолюцій: однієї – для застосування у приватному секторі економіки (№22), другої – у публічному (№29). Комітет Міністрів затвердив першу в 1973 році, другу – в 1974 році.

Під час підготовки цих документів стало зрозумілим, що для досягнення ефективності у захисті приватності необхідно укріпити існуючі національні норми, використовуючи міжнародні інструменти. Така ж сама пропозиція пролунала під час конференції Європейських міністрів юстиції у 1972 році і була відзначена у її резолюції №3.

Комітет Ради Європи з правових питань зважив на вказану пропозицію і почав розробку проекту майбутньої конвенції. У 1976 році для цього була сформована нова комісія. Комісія експертів із захисту даних, як її назвали, збиралася чотири рази на пленарні засідання і підготувала проект у травні 1979 році, а остаточний варіант Конвенції у квітні 1980 року. У тому ж році Парламентська Асамблея Ради Європи прийняла Рекомендацію № 890, у якій вказувалось на необхідність ефективного захисту приватності персональних даних і було запропоновано включити відповідне положення до тексту Європейської Конвенції про захист прав людини та основних свобод.

Конвенція Ради Європи № 108 "Про захист осіб стосовно автоматизованої обробки персональних даних" була відкрита для підписання 28 січня 1981 року і

вступила в дію 1 жовтня 1985 року, після того, як п’ять держав-членів Ради Європи висловили своє бажання бути пов’язаними положеннями Конвенції. Ними стали Швеція, Франція, Норвегія, Іспанія та ФРН. Усі ці країни, за винятком Іспанії, мали національні акти про захист даних на час ратифікації.

Станом на грудень 2003 року учасницями Конвенції стали 30 країн, ще п’ять її підписали, але не ратифікували. Конвенція “Про захист осіб стосовно автоматизованої обробки персональних даних” є одним з перших міжнародних інструментів, який завдяки своєму обов’язковому характеру закріпив мінімальні стандарти у галузі захисту інформаційної приватності. Україна цю Конвенцію ще не підписала.

Конвенція складається з семи глав, які умовно можна об’єднати в три частини, що містять загальні принципи, спеціальні правила стосовно передачі даних через кордони і механізми співпраці між державами-учасниками Конвенції.

Центральною частиною Конвенції є Глава 2, яка містить основні принципи захисту персональних даних, що становить “стрижень” цього документа. Це принципи якості даних (стаття 5): правомірності і законності обробки, обмеження ціллю використання, адекватності, точності, обмеження ідентифікації тощо. Стаття 6 Конвенції передбачає особливий режим певних категорій даних, зокрема тих, що свідчать про расову приналежність, політичні погляди або релігійні чи інші переконання, а також персональні дані, що стосуються здоров’я або статевого життя, кримінальних вчинків, з огляду на загрозу їх використання для дискримінації індивідів за тією чи іншою ознакою. Слід відзначити, Конвенція лише вказує на мету, яка має бути досягнута через застосування цих принципів, але залишає кожній державі-учасниці право визначати спосіб, у який ті мають бути впроваджені у національному законодавстві.

Стаття 8 Конвенції передбачає гарантії для суб’єкта даних для ефективної реалізації права на приватність персоніфікованої інформації, які включають такі правові можливості:

- бути ознайомленим про існування файлів персональних даних, умови їх обробки, у тому числі про особу “контролера файлу” (особу, яка визначає цілі обробки);
- одержувати підтвердження обробки і ознайомлюватися з самою інформацією, що обробляється;
- вимагати виправлення або знищення персональних даних, які обробляються з порушенням указаних принципів і, нарешті,
- звертатися за правовим захистом у разі порушення відповідних прав контролером файлу.

Розробники Конвенції впровадили в її текст певні стандарти, вироблені Європейською Комісією і Судом з прав людини в частині оцінки правомірності застосування державами обмежень основних прав і свобод людини. Зокрема, стаття 9 Конвенції дозволяє відступ від проголошених принципів, а також обмеження відповідних прав суб’єкта даних, якщо це передбачається національним законодавством і є у демократичному суспільстві необхідним заходом, спрямованим на: а) захист державної безпеки та громадського спокою, грошових інтересів держави або на боротьбу із кримінальними злочинами; б) захист суб’єкта даних або прав і свобод інших осіб. Можливість застосування обмежень передбачається також для реалізації інших суспільних інтересів. Це стосується використання персональних даних для цілей статистики або наукових досліджень.

Запропоновані в Главі 3 Конвенції вимоги стосуються питань транскордонної передачі даних і покликані погодити, збалансувати одночасно існуючі вимоги щодо безперешкодної передачі персоніфікованої інформації і захисту приватності персональних даних. Проголошується, що транскордонні потоки даних між державами-членами Конвенції не можуть бути об’єктом будь-якого спеціального контролю. Однак щодо певних категорій персональних даних, які мають спеціальний режим згідно з національним законодавством, Конвенція все ж таки передбачає можливість відступу від вимог щодо безперешкодної передачі даних до країн-членів Конвенції, якщо тільки цій категорії даних не надається еквівалентний захист у цій країні. Така ж можливість обмеження транскордонної передачі даних залишається у

випадку реекспорту даних до третіх країн, що не є членами Конвенції. Розв'язанню проблем, що виникають у зв'язку із застосуванням таких обмежень, приділяється більше уваги в підрозділі 2.3 цієї роботи.

Міжнародно-правовий механізм взаємодії між державами-учасницями у справах, що стосуються окремих індивідів, деталізується у четвертому розділі Конвенції. З цією метою кожна країна зобов'язується призначити національні органи, відповідальні за міжнародне співробітництво у цій галузі. Особам, які мешкають на території країн-членів Конвенції, гарантується можливість подати запит щодо реалізації своїх прав через посередництво таких органів. На практиці такими органами виступають національні наглядові інстанції у галузі захисту приватності персоніфікованої інформації. Взаємна допомога, яку члени Конвенції надають одна одній, зокрема, представлення інформації про свої законодавство та адміністративну практику в галузі захисту даних, відомостей про умови конкретної автоматизованої обробки, а також допомога суб'єктам даних, що мешкають за кордоном, – надається на безоплатній основі. У п'ятій главі Конвенції виписано механізм конвенційної співпраці через створення Консультативного комітету, до складу якого входять представники та заступники представників, призначені державами-членами Конвенції.

З прийняттям Конвенції у 1981 році діяльність Ради Європи в цій галузі не зменшилася. Проектна група з питань захисту даних (CJ-PD), до складу якої входять експерти з кожної держави-члена Конвенції, підготувала серію рекомендацій, які значною мірою розширюють та конкретизують проголошені у Конвенції принципи.

Оскільки умови та методи роботи з даними залежать від призначення останніх, то рекомендації розраховані на їх обробку в таких секторах: медичному (картотеки і практика) [179,180], науково-дослідному [181], рекламного бізнесу [182], соціального забезпечення [183], поліцейському [184], працевлаштування [185], фінансовому [186], телекомунікаційних послуг [187] і в статистиці [188], а також під час передачі публічними органами даних третім сторонам [189]. Передостання з затверджених Комітетом Міністрів рекомендацій стосується питання забезпечення приватності під час користування мережею Інтернет і розрахована на її застосування користувачами

та постачальниками інформаційних послуг [190], а остання – торкається захисту персоніфікованої інформації у сфері страхування [191].

Указаний спосіб адаптації принципів приватності до нових умов роботи з персональними даними виявився вдалим бо процедура прийняття рекомендацій і їх затвердження Комітетом Міністрів є простішою за процедуру внесення змін до тексту Конвенції, що вимагало б їх ратифікації кожною державою-учасницею Конвенції.

Розглянемо спеціальні норми й принципи міжнародного регулювання використання й транскордонної передачі персоніфікованої інформації у цілях боротьби із злочинністю в рамках Ради Європи. Міжнародно-правові документи у галузі захисту приватності персоніфікованої інформації відносять поліцейські файли до категорії відомостей, обробка яких несе підвищений ризик правам суб'єктів даних, отже до тих, що є вразливими. Чим більша вразливість даних, тим більший ризик порушення прав осіб під час обробки персональних даних, а значить тим сильнішими повинні бути правові гарантії захисту від порушень. Оцінка вразливості даних, а отже, і всіх обставин їх обробки, повинна передувати самій обробці. Цей принцип є визначальним для побудови всієї правової конструкції відносин з обробки персональних даних у правоохоронній діяльності, оскільки безпосередньо пов'язаний з загально-інституційним принципом пропорційності, який у сфері правоохоронної діяльності означає пропорційність обмеження прав громадян відповідно до рівня суспільної небезпечності злочину.

Ці вимоги деталізуються у Рекомендації № R (87)15 Комітету Міністрів Ради Європи державам-членам, що регулює використання персональних даних у секторі поліції. Схвалена 1987 року на 410-й зустрічі заступників міністрів, вона не втратила своєї актуальності й на сьогоднішній день. Сам текст Рекомендації містить всього вісім принципів, розгорнуте тлумачення яких додається у пояснювальній записці. Не випадково, що *першим принципом* є принцип контролю за обробкою персональних даних. Ідеться про запровадження механізму нагляду за додержанням поліцією встановлених законом вимог до обробки персоніфікованої інформації. Такий нагляд повинен здійснюватися незалежним органом державної влади, діяльність якого не пов'язана з діяльністю поліції. На цей же наглядовий орган може бути покладено

функцію реєстрації файлів (масивів) персональних даних, які оброблятимуться поліцією.

Процедура повідомлення покликана, по-перше, запровадити попередній контроль за законністю обробки тієї чи іншої категорії персональних даних, по-друге, спростити процедуру і підвищити ефективність нагляду за допомогою одержаних при цьому відомостей про орган і його посадових осіб, відповідальних за обробку і наступну передачу даних.

Враховуючи все активніше впровадження новітніх інформаційних технологій у діяльність поліції, незалежний наглядовий орган повинен виконувати важливу роль попередньої перевірки нових засобів чи пристроїв, які використовуються для обробки персональних даних, а отже, можуть нести великий ризик для прав людини. Зокрема, може йтися про технології негласного стеження чи збирання інформації за допомогою зіставлення інформації з різних баз даних, що є потенційно небезпечним.

Принцип 2 Рекомендації присвячується питанням збирання відомостей про особу правоохоронними органами і адаптує вимоги статті 5 Конвенції Ради Європи 1981 року до умов діяльності поліції. Зокрема, окреслюються межі збирання персональних даних. Вони можуть збиратися для запобігання реальній небезпеці або припинення особливого кримінального злочину. Для негласного збирання персональних даних, у тому числі з використанням технічних засобів, у національному законодавстві повинні бути запроваджені детальні правила і гарантії від зловживань.

Окрема увага приділяється збиранню, так званих, "вразливих даних", які розкривають расову або етнічну належність, релігійні переконання, політичні погляди або філософські переконання, сексуальну поведінку тощо. Їх збирання дозволяється лише у разі "виключної потреби для цілей особливого запиту", тобто коли існують серйозні підстави вважати, що злочин скоєний чи може бути скоєним особою, яка може бути ідентифікована за допомогою таких вразливих даних. При цьому роз'яснюється, що відомості про сексуальну поведінку можуть збиратися лише для розслідування вже скоєних злочинів.

До процедури зберігання даних також пред'являються вимоги, які надають гарантії запобігання порушенням прав осіб під час їх подальшого використання. Ці ж

вимоги сприяють не тільки захисту прав людини, а й покращують ефективність правоохоронної діяльності, що підтверджується досвідом європейських країн. Зокрема, *Принцип 3* Рекомендації передбачає необхідність запровадження системи класифікації даних, розрізняючи підтверджені дані від непідтверджених, дані одержані з надійних джерел від ненадійних. До речі, саме така система класифікації успішно використовується вже не один десяток років у Великій Британії [192].

Крім того, рекомендується, щоб, за можливістю, дані про скоєні злочини або про підготовку до вчинення злочинів зберігалися окремо від даних, зібраних для адміністративних цілей, у тому числі про адміністративні правопорушення. Тим самим буде забезпечуватися, по перше, принцип додержання цілі збирання під час зберігання, по друге, унеможливиться помилкове їх використання внаслідок змішування.

Четвертий принцип закріплює вимогу використання даних, зібраних в поліцейських цілях, тобто для запобігання чи припинення злочинів або підтримання громадського порядку, лише в цих цілях. Це не означає, що дані з поліцейських файлів не можуть передаватися іншим органам, оскільки вказану функцію певним чином виконують також інші державні органи та установи. Ці випадки, які становлять не правило, а виняток з нього, конкретизуються у *Принципі 5*.

Однією з вимог для легітимної передачі даних поліцейською установою іншим органам і установам є наявність процедури уповноваження, під час якої уповноваженим органом, наприклад, судом або незалежним наглядовим органом, перевіряється її доцільність і законність.

За відсутності такої санкції передача дозволяється, якщо це необхідно для виконання державним органом покладених на нього за законом обов'язків, в інтересах особи, якої стосується інформація (суб'єкта даних), а також коли це необхідно для відвернення серйозної реальної небезпеки (навислої загрози).

Міжнародна передача поліцейських даних дозволяється лише між органами поліції. Правовою підставою для таких передач є наявність відповідних домовленостей між державами. Однак слід звернути увагу на дуже важливе питання, яке безпосередньо торкається України. В цьому принципі закріплюється вимога, що

міститься в статті 12 Конвенції Ради Європи № 108. Вона також включена до текстів європейських угод у галузі співробітництва між органами поліції, що більш докладно розглядається у підрозділі 2.2 дисертації. Ідеться про відповідність національного законодавства країни одержувача даних вимогам щодо захисту права на приватність персональних даних, викладеним у Рекомендаціях. Забезпечення цієї вимоги покладається на поліцейську установу, яка передає дані до країни, в якій рівень правового захисту не є адекватним. При цьому передбачається можливість застосування застережень з боку передаючої сторони щодо процедури обробки і використання персональних даних одержувачем для задоволення інформаційного запиту.

Важливою гарантією законності обробки персональних даних у цілях боротьби із злочинністю, відновлення обмежених і захисту порушених прав громадян під час правоохоронної діяльності є, по-перше, право на ознайомлення з поліцейськими файлами зацікавлених осіб, по-друге, право на виправлення неточних даних, по-третє, право на оскарження неправомірних дій. Ці питання регламентуються в *шостому принципі*.

Не вимагає додаткових пояснень твердження, що збирання, систематизація й аналіз відомостей про осіб, які готують або вчинили злочини, так само як і про осіб, життя, здоров’я або майно яких стали об’єктом посягань, є ключовими елементами правоохоронної діяльності. В той же час, у інтересах правоохоронної діяльності – не повідомляти осіб про негласне збирання персоніфікованої інформації, тримати одержані відомості про особу недоступними для громадськості, оскільки розголошення може зашкодити слідству, унеможливити досягнення результату оперативно-розшукових заходів і слідчих дій взагалі. Таємний характер обробки відомостей про особу в цілях боротьби із злочинністю входить у протиріччя з принципом прозорості, який є суттєвим для ефективної реалізації права людини на приватність персоніфікованої інформації. Не маючи уявлення про збирання персональних даних, зацікавлена особа не може захистити свої права.

Отже, потрібне вироблення правового механізму, який дозволить врахувати інтереси особи, чиї права обмежуються у ході негласного збирання і обробки

персональних даних. Зокрема, у цьому принципі йдеться про контроль з боку громадськості через орган нагляду за обробкою персональних даних, яка здійснюється правоохоронними органами. Тобто, не повинно існувати таємних файлів або баз даних, про які не знає громадськість. Усі вони повинні бути легалізованими, а їх використання врегульовано у законодавстві, доступному для громадськості.

Право на доступ до персональних даних, що містяться у поліцейських файлах, повинно гарантуватися. Однак межі здійснення цього права залежатимуть від наслідків, які буде мати розголошення відповідної інформації. Якщо розголошення тієї чи іншої інформації, одержаної як гласними, так і негласними засобами, може зашкодити слідству, – остання не повинна повідомлятися. В інших випадках, як в інтересах громадян, так і в інтересах правоохоронних органів надавати зацікавленій особі доступ до відомостей з правом їх виправлення або доповнення достовірних даних. При цьому персональні дані, які були зібрані з порушенням закону, повинні бути знищені на вимогу суб'єкта даних.

Національне законодавство повинно передбачати процедуру контролю за дотриманням законності у випадку відмови у доступі до поліцейських файлів. Цю функцію повинен виконувати незалежний орган держави, будь-то наглядова інстанція чи суд.

Принцип 7 Рекомендацій передбачає, що персональні дані, які збиралися з певною метою, після досягнення цієї мети або неможливості чи недоцільності її досягнення, повинні знищуватися. Такими підставами можуть бути відмова у порушені кримінальної справи, засудження особи, реабілітація, амністія чи інші аналогічні випадки. Національне законодавство повинно визначати терміни зберігання тих чи інших даних залежно від мети їх збирання чи характеру самих даних.

Останній, *восьмий принцип* покликаний забезпечити цілісність даних шляхом адекватних технічних та організаційних заходів для унеможливлення, запобігання чи припинення несанкціонованого доступу, передачі, перетворення або знищення персональних даних і від будь-якої іншої незаконної обробки як внаслідок необережності, так і навмисних дій третіх осіб.

Отже, впровадження вищезазначених приписів у законодавство, що регулює правоохоронну діяльність, дозволяє збалансувати суб'єктивні інтереси осіб, яких стосується персоніфікована інформація, а також інтереси суспільства у безпеці. Тим самим гарантуватиметься дотримання принципу пропорційності застосування обмежень і законність. До питання встановлення правових рамок здійснення права на приватність в контексті правоохоронної діяльності ми ще повернемося на прикладі функціонування "простору свободи, безпеки і правосуддя" в Європейському Союзі.

Як видно з проведеного нами аналізу спеціальних міжнародних норм і принципів захисту приватності персоніфікованої інформації у сфері правоохоронної діяльності, вони базуються на загально-інституційних нормах і принципах і закріплюються у формі пристосованій до особливостей відносин щодо використання персоніфікованої інформації у тих чи інших сферах суспільного життя.

Окрім рекомендацій, експерти Проектної Групи Ради Європи здійснили у 1991 році дослідження питань, що виникають під час застосування персональних ідентифікаційних номерів [193]. Представниками Консультативного Комітету за активної участі експертів ЄС і Міжнародної Торгової Палати розроблено "Модельний контракт на забезпечення еквівалентного захисту персональних даних у контексті питання транскордонних потоків даних" 1992 року. Положення модельного контракту спрямовані на регулювання умов передачі даних до країн, в яких рівень захисту даних не відповідає стандартам Ради Європи [194].

Консультативним Комітетом підготовлено проект додаткового протоколу до Конвенції (відкритий для підписання 8 листопада 2001 року), метою прийняття якого є запровадження інституту наглядової інстанції у питаннях захисту персональних даних. В цьому ж протоколі запропоновано встановити правило, що принципово змінює підхід до регулювання питань транскордонної передачі даних. Так, стаття 12 Конвенції за старою редакцією встановлює правило, згідно з яким забороняється застосування обмежень на експорт даних до іншої держави, яка надає еквівалентний захист. Тобто, тут не передбачається позитивна вимога до країн-членів Конвенції обмежувати експорт персональних даних; вирішення цього питання залишається на розсуд держав. У той же час, стаття 2 додаткового протоколу встановлює правило,

згідно з яким передача персональних даних одержувачу, який перебуває під юрисдикцією держави, яка не є учасницею Конвенції, дозволяється лише за умови, що ця держава забезпечує адекватний рівень захисту для запропонованої передачі даних. Такий підхід у регулюванні транскордонних потоків даних аналогічний тому, що був обраний Європейським Союзом, і свідчить про прагнення європейських країн запровадити загальноєвропейські стандарти у галузі захисту персональних даних на основі Конвенції Ради Європи № 108.

Цим пояснюється зацікавленість Європейського Союзу у приєднані до Конвенції № 108. 22 липня 1997 року Рада ЄС своїм рішенням уповноважила Комісію ЄС почати процес переговорів з метою приєднання Європейських Співтовариств до Конвенції № 108. У листі, датованому 22 жовтня 1997 року, Генеральний Секретар Європейської Комісії повідомив Генеральному Секретарю Ради Європи про таке прагнення Європейських Співтовариств. Воно було реалізовано шляхом внесення відповідних змін до Конвенції у 2000 році.

Слід звернути увагу на те, що Конвенція № 108 не є “європейською” у вузькому розумінні, що відрізняє її від інших конвенцій Ради Європи. У цьому розумінні стаття 23 несе в собі важливий елемент, оскільки дозволяє вступ до Конвенції державам, які не є членами Ради Європи. Крім того, у статті 18 передбачається можливість участі у роботі Комітету на правах спостерігачів представників держав-членів Ради Європи, які не є сторонами Конвенції № 108. За одностайним рішенням Консультативного комітету така можливість може надаватися й іншим країнам, які навіть не є членами Ради Європи. Це зроблено для того, щоб закласти фундамент для досягнення міжнародного консенсусу в питаннях захисту персональних даних, особливо з третіми, неєвропейськими країнами. Однак жодна країна - не член Ради Європи ще не скористалася такою можливістю стати учасницею Конвенції, що вимагає активізації діяльності конвенційних органів у цьому напрямку.

Проведений аналіз положень Конвенції № 108 дозволяє дійти висновку, що мінімальні стандарти захисту приватності персоніфікованої інформації, що містяться в ній, а також діючий механізм конвенційного співробітництва можуть бути успішно використані для досягнення консенсусу між країнами з різними правовими

традиціями і розробки на його основі універсальних міжнародно-правових стандартів у цій сфері.

Не менш цікавою є діяльність іншої впливової міжнародної організації на процес уніфікації правил поводження з персональними даними. Організація Економічної Співпраці і Розвитку почала дослідження питань, пов'язаних із транскордонними потоками даних, у 1969 році. Група з питань застосування комп'ютерів, а пізніше Комісія з питань баз даних, проаналізувала та підготувала доповіді з різних аспектів, що стосуються питань приватності персональних даних, зокрема, цифрового формату інформації, транскордонних потоків даних, управління інформаційною діяльністю.

У 1977 році Комісія ОЕСР з питань баз даних спільно з Комітетом експертів Ради Європи у Відні провела міжнародний симпозіум, де відбувся обмін думками та досвідом людей, що представляли різні інтереси, включаючи представників політичних і бізнесових кіл, користувачів міжнародних мереж та зацікавлених міжнародних організацій. Під час його проведення було вироблено спільну позицію щодо необхідності встановлення на міжнародному рівні основоположних принципів для регулювання міжнародного обміну інформацією, що стосується осіб.

На початку 1978 року була сформована нова Група експертів з питань транскордонних потоків та захисту приватності на чолі з головою Австралійського Комітету з правової реформи, суддею Верховного Суду М.Д. Кербі. Група підготувала низку доповідей щодо ключових проблем обміну персональними даними і проаналізувала різні підходи, які обрали країни – члени ОЕСР у законодавчому регулюванні цих питань.

Серед членів ОЕСР на час ухвалення Керівних принципів деякі країни вже прийняли нормативні акти, які передбачали відповідне регулювання питань захисту інформаційної приватності. Так, наприклад, Австрія, Канада, Данія, Франція, Люксембург, Норвегія, Швеція та Сполучені Штати вже мали відповідні закони, а Бельгія, Ісландія, Нідерланди, Іспанія та Швейцарія тільки підготували законопроекти.

Наявні розбіжності між країнами торкалися питань сфери законодавчого регулювання, уваги до певних елементів захисту та контрольного механізму. Зокрема,

не було узгодженості в питаннях запровадження ліцензування і функціонування контрольного механізму – спеціального уповноваженого наглядового органу, категорій “вразливих даних”, розуміння принципу прозорості та індивідуальної участі суб’єкта даних у процесах обробки даних. До цього ж додавалися традиційні розбіжності між правовими системами, з яких випливали різні підходи до закріплення правил поводження з даними на регулятивному рівні. Зазначені обставини обумовили характер прийнятого документа.

“Керівні принципи, що регулюють захист приватності і транскордонні потоки персональних даних” ОЕСР, які були ухвалені у вигляді рекомендації, встановлюють узагальнені правила поводження з персональними даними. “Керівні принципи, що регулюють захист приватності і транскордонні потоки персональних даних” вступили в дію 23 вересня 1980 року після їх ухвалення Рекомендацією Ради ОЕСР на 523-у засіданні [195].

Вони є мінімальними стандартами, що створені в результаті пошуку консенсусу між позиціями країн-членів ОЕСР в цьому питанні. Документ складається з п’яти частин. Перша частина містить низку визначень та окреслює сферу застосування Керівних принципів. Друга частина вміщує вісім основних положень (пункти 7-14), які становлять стрижень Керівних принципів: 1) обмеження ціллю; 2) якості даних; 3) визначення цілі; 4) обмеження використання; 5) гарантії безпеки; 6) відкритості; 7) індивідуальної участі; 8) відповідальності.

Частина 3 подає принципи міжнародного застосування, що пов’язані зі взаємовідносинами країн-членів ОЕСР в цьому питанні, які в тексті документа позначаються як “вільний потік і законні обмеження”.

“Керівні принципи” покладають на держави-члени зобов’язання вжити усіх розумних і відповідних заходів для забезпечення безперешкодності й безпечності транскордонних потоків персональних даних, включаючи транзит через територію держави-члена ОЕСР. З цією метою держави повинні утримуватися від обмежень транскордонного обміну персональними даними з іншою державою-членом, окрім випадків, коли остання ще не достатньою мірою дотримується цих “Керівників принципів” або коли реекспорт таких даних порушує її внутрішнє законодавство з

захисту приватності персоніфікованої інформації. Як і Конвенція Ради Європи № 108, “Керівні принципи” передбачають можливість застосування обмежень передачі даних стосовно певних категорій персональних даних, які мають спеціальний національний правовий режим.

Питання імплементації основних принципів викладені у четвертій частині. Тут же конкретизується, що принципи повинні застосовуватися на недискримінаційній основі. Упровадження принципів у національну правову систему вимагає встановлення законодавчих, адміністративних або інших процедур чи інституцій. Згідно з “Керівними принципами” ОЕСР від держав вимагається: 1) прийняття відповідного внутрішнього законодавства; 2) заохочення й підтримка саморегуляції; 3) забезпечення реалізації індивідами своїх прав; 4) запровадження санкцій (заходів відповідальності) за порушення викладених принципів.

П’ята частина присвячується питанням співпраці країн-членів, яка здійснюється через обмін інформацією, уникнення несумісних національних процедур для захисту персональних даних. Рекомендація не покладає на країни-члени ОЕСР таких зобов’язань як Конвенція Ради Європи № 108 на її учасників. Слід відмітити, що членами ОЕСР є 19 держав-членів Конвенції Ради Європи № 108 (членами ОЕСР є 20 країн-засновників організації з Західної Європи і Північної Америки, а також прийняті пізніше Японія, Австралія, Нова Зеландія і Фінляндія та щойно прийняті Мексика, Чеська Республіка, Угорщина, Польща, Корея і Словацька Республіка). Разом з тим, Керівні принципи обмежують можливість застосування винятків зі встановлених у них правил, що певним чином посилює цей документ. До того ж Керівні принципи поширюють свою дію не лише на автоматизовані файли даних, як Конвенція Ради Європи, а й на дані, обробка яких несе загрозу приватності та індивідуальним свободам незалежно від методів і засобів поводження з ними. Група експертів аргументувала такий підхід намаганням уникнути можливих прогалин у регулюванні, причиною яких є проблема розмежування на технічному рівні процесів автоматизованої і неавтоматизованої обробки даних, зокрема, у “змішаних” системах.

Крім того, Керівні принципи більш конкретно визначають права суб’єкта даних. Так, принцип 13 регламентує “індивідуальну участь” суб’єкта даних в процесі

доступу і містить право на отримання даних, що його стосуються. Суб'єкту даних дається право оскаржити будь-яку відмову в надані такої інформації та отримати обґрунтування такої відмови.

Низку міжнародно-правових документів було прийнято ОЕСР у розвиток проголошених принципів і їх адаптації до вимог часу. Питання вільної передачі даних отримало свій подальший розвиток в Декларації про транскордонні потоки даних, яка була підготовлена Комітетом з інформації, комп'ютерів та комунікацій у березні й затверджена міністрами країн-членів у квітні 1985 року [196]. Приймаючи Декларацію, країни-члени ОЕСР підтвердили своє прагнення забезпечити вільний обмін інформацією та розробити спільні політичні підходи до питань транскордонної передачі даних, зокрема, щодо передачі інформації у торговельній сфері, внутрішньо-корпоративного обміну даними, комп'ютеризованих інформаційних послуг, наукового та технологічного обміну.

У листопаді 1992 року Рада ОЕСР ухвалила Рекомендацію про Керівні принципи щодо безпеки інформаційних систем [197]. Цей документ передбачає прийняття країнами національних положень для забезпечення цілісності й конфіденційності інформаційних систем та інформації, що в них обробляється, через вжиття комплексу організаційних і технічних захисних заходів.

Питанням гармонізації політики країн-членів ОЕСР у сфері застосування криптографічного захисту інформації присвячена Рекомендація про Керівні принципи щодо політики у галузі криптографії, ухвалена в березні 1997 року [198]. Документ встановлює принципи, спрямовані на регламентування прав користувачів щодо вибору криптографічних методів, вільного проектування таких методів і засобів, можливість взаємодії інформаційних мереж, їх значення для захисту персональних даних та усунення бар'єрів у міжнародній торгівлі.

У жовтні 1998 року в Отаві (Канада) на засіданні міністрів 29 країн-членів ОЕСР, присвяченому електронній комерції, розглядалося питання захисту приватності в глобальних інформаційних мережах. Серед його результатів, зокрема, прийняття Декларації про захист приватності в глобальних мережах. В Декларації наголошується на необхідності захисту приватності в глобальних інформаційних

мережах для забезпечення поваги до основних прав, побудови довіри й запобігання встановленню зайвих обмежень для транскордонної передачі даних [199]. В Декларації відзначається важливість прийняття на національному рівні комплексної програми заходів для забезпечення приватності, зокрема, попередження користувачів мереж щодо проблеми приватності в інформаційному просторі, їх навчання, сприяння розвитку технологій, що гарантують приватність інформаційного обміну.

Розвиток інформаційних технологій і глобалізація інформаційних потоків вимагає перегляду раніше встановлених принципів з метою їх адаптації до вимог часу. Перед ОЕСР постає необхідність переглянути раніше досягнутий між країнами-членами консенсус з цього питання. Це непросте завдання ускладнюється існуючими розбіжностями в стандартах між європейськими і неєвропейськими країнами-членами ОЕСР, насамперед між Європейським Союзом і США.

Слід відзначити, що питанням уніфікації правил поводження з персональними даними, присвятила увагу також Генеральна Асамблея ООН, яка 14 грудня 1990 року ухвалила "Керівні принципи стосовно комп'ютеризованих файлів персональних даних" [200], що розраховані на їх впровадження в національне законодавство, а також на застосування міжурядовими організаціями.

"Керівні принципи" ООН відтворюють основні загальновизнані принципи захисту приватності: принцип дотримання законності та справедливості під час обробки; принцип "акуратності" (перевірки відповідності і точності); принцип "специфікації" цілі обробки; принцип доступу до персональних даних, включаючи право на заперечення проти обробки, внесення змін до персональних даних і поновлення порушених прав; принцип недискримінації і захист приватності, так званих, "вразливих" даних; повноваження робити винятки в інтересах національної безпеки, громадського порядку, здоров'я або моралі, а також захисту прав і свобод інших осіб; принцип безпеки; принцип нагляду і санкцій зобов'язує кожну державу призначити незалежну наглядову інстанцію, яка буде контролювати дотримання зазначених принципів, а також передбачати відповідальність за їх порушення; принцип безперешкодної передачі даних через кордони між країнами, які пропонують рівноцінні гарантії. Наведені принципи, як це вказується в тексті документа, повинні

поширюватися на всі публічні й приватні комп’ютеризовані файли, а також можуть застосовуватися до “мануальних” файлів, тобто персональних даних, які обробляються вручну. В “Керівних принципах” зазначається, що всі ці принципи або деякі з них можуть застосовуватися також до юридичних осіб.

Однак “Керівні принципи” ООН не визнаються міжнародною спільнотою як універсальні міжнародні стандарти, оскільки є занадто загальними і розраховані здебільше на внутрішнє застосування міжнародними органами самої Організації Об’єднаних Націй, а не для регулювання питань транскордонної передачі даних. Отже питання розробки універсальних міжнародних домовленостей у цій сфері постає вкрай актуально.

Приклад успішної гармонізації національного законодавства у сфері захисту приватності персоніфікованої інформації на основі спільних правових стандартів, що відбивають загальноєвропейське розуміння проблеми й шляхів її вирішення, демонструє Європейський Союз.

2.2. Регулювання обробки й транскордонної передачі персоніфікованої інформації в праві Європейського Союзу

Дбаючи про розвиток такого напрямку співробітництва країн Європейського Союзу, як створення простору свободи, безпеки і співробітництва, Європейський Парламент і Рада у 2000 році ухвалили Хартію основних прав громадян ЄС [201]. Захисту права на повагу до приватного життя і захисту персональних даних присвячено дві статті цієї Хартії. Стаття 7 "Повага до приватного та сімейного життя", яка є другою за порядком в другому розділі Хартії, майже тотожна за змістом частині першій статті 8 Європейської Конвенції про захист прав людини і основних свобод. А наступна, восьма стаття Хартії, містить квінтесенцію принципів захисту приватності персональних даних:

"Стаття 8. Захист персональних даних

1. Кожен має право на захист персональних даних стосовно своєї особи.

2. Такі дані можуть збиратися виключно для спеціально визначених цілей і на підставі попередньої згоди зацікавленої особи або на іншій законній підставі, передбаченій законодавством. Кожен має право вільного доступу до даних, які були зібрані щодо його особи, та право на виправлення таких даних.

3. *Дотримання цих правил має контролюватися незалежним органом"* [202, *181*][1)].

Повага до прав людини є одним з ключових елементів концепції створення простору свободи в Європі. Стаття 6 (1) Договору про створення Європейського Союзу передбачає, що він ґрунтується на принципах свободи, демократії, поваги до прав людини і фундаментальних свобод, на верховенстві (правлінні) права. У рамках

[1] [181] Шевчук С., Кравчук І Ніццький договір та розширення ЄС / Центр порівняльного права / С. Шевчук (наук.ред.), А. Пендак (пер.). — К.: Логос, 2001. — 195с.

дослідження доцільно проаналізувати розвиток законодавства Європейського Союзу у цій сфері.

Європейське Економічне Співтовариство в перший раз згадує про захист даних у доповіді 1973 року, що була продовжена дебатами у Європейському Парламенті в 1974-75 роках. Про необхідність узгодження політики країн Європейських Співтовариств з цього питання йдеться у Резолюції, що була ухвалена Радою ЄС у липні 1974 року [203].

У червні 1979 року Парламент ухвалив підготовлену експертами Комітету з правових питань Резолюцію "Про захист прав індивідів стосовно технічного розвитку і обробки даних", в якій робиться акцент на створенні спільного ринку в обробці даних. У Резолюції, зокрема, зазначається, що національні положення в галузі захисту приватності мають безпосередній вплив на такий спільний ринок, а саме, здатні "деформувати умови конкуренції".

У Рекомендації від 29 липня 1981 року № 81/679/ЕЕС, яка присвячується затвердженню Радою Європи Конвенції № 108, вказується про її прийнятність для створення однакового рівня захисту інформаційної приватності в Європі [204].

Фактором, що активізував розробку документа, стала не вирішена повною мірою проблема транскордонної передачі даних як всередині Європи, так і при передачі даних за межі континенту. Випадок, який отримав значний резонанс, стався у 1991 році, коли Французьке агентство з питань захисту персональних даних заборонило компанії "Фіат" електронну передачу інформації про французьких працівників компанії до її головного офісу в Італії, доки "Фіат" не погодиться бути пов'язаною вимогами законодавства Франції про захист даних. Інший випадок стався у 1992 році. Німецький банк відмовився надати своєму підрозділу у Гонконгу доступ до інформації про клієнтів банку, громадян Німеччини.

Європейська Комісія подала проект директиви у вересні 1990 році після низки запитів Європейського Парламенту щодо необхідності вжиття заходів у цій галузі. С численними зауваженнями Європейського Парламенту проект подали на друге читання у жовтні 1992 року. У лютому 1994 року держави-члени дійшли політичної угоди стосовно основних положень директиви; і лише рік потому Рада Міністрів

ухвалила “спільну позицію”, що була підтверджена Парламентом у червні 1995 року. Директива № 95/46 СЕ Європейського Парламенту і Ради “Про захист фізичних осіб стосовно автоматизованої обробки персональних даних та безперешкодного руху цих даних” набула чинності 24 жовтня 1995 року [205].

Процес проходження Директиви супроводжувався протидією з боку бізнесових кіл, як європейських, так і американських. Запропоновані Директивою правила вимагали, щоб індивіди надавали свою “повідомлену згоду” на вторинне, у тому числі при зміні цілі, використання персональних даних. Це положення було включено до тексту директиви з метою заборонити комерційним структурам продаж та обмін інформацією про осіб без сповіщення і згоди суб’єкта даних.

На практиці це означає, що суб’єкт даних має виявити бажання на будь-яке подальше використання за, так званою, формулою “опт-ін” (**англ.** *opt in*). Але для комерційних структур більш зручною є “пасивна” форма, коли особу повідомляють про можливість вторинного використання і їй надається можливість заперечувати такому використанню чи обміну, що відповідає формулі “опт-аут” (**англ.** *opt out*),. До речі, саме така процедура передбачена за законодавством Сполучених Штатів Америки [206].

Принципи інформаційної приватності, що їх містить друга частина документа, відповідають за своєю спрямованістю принципам ОЕСР та Ради Європи, бо й спираються на них. Положення Директиви уточнюють і розширюють принципи, які містить Конвенція Ради Європи від 28 січня 1981 року “Про захист осіб стосовно автоматичної обробки персональних даних”. Разом з тим, запозичивши національні розробки країн Європейського Союзу, Директива розширила коло прав суб’єктів даних, що дозволяє віднести її до наступного покоління міжнародних інструментів у галузі інформаційної приватності.

Так, стаття 11 встановлює, що у разі отримання персональних даних не від самого суб’єкта даних, а з інших джерел, суб’єкт даних має бути сповіщеним про цілі збору і обробки, її одержувачів, наявність права доступу та виправлення даних. Стаття 12 передбачає право суб’єкта даних вимагати повідомлення третім особам про зміну, знищення чи блокування інформації, повідомленої до цього. А стаття 14 надає особі

право заперечувати обробці персональних даних за певних обставин та забороняти використання даних у цілях рекламної діяльності чи ринкових досліджень.

Крім того, Директива встановлює нові правила, які до цього не містилися ні в Конвенції Ради Європи, ні в Керівних принципах ОЕСР. Ідеться про рішення, що їх приймають автоматизовані системи під час оцінки якостей людини на основі аналізу інформації, що стосується цієї особи. Директива надає особам право ознайомитися з логічною формулою, що її використовує така система (стаття 12), і право оскаржити автоматично прийняте рішення (стаття 15). Ці положення були запозичені з законодавства Франції про захист приватності, що відбиває ідею захисту людини від рішень "бездушної" машиною.

Директивою запроваджується процедура сповіщення контролером про обробку наглядовій інстанцій. Відповідні відомості вносяться до реєстру, який веде наглядовий орган. Така процедура має на меті забезпечити гласність цілей обробок і основних умов її здійснення для перевірки на їх відповідність положенням національного законодавства. Запроваджено також процедуру попереднього контролю, за якою держави мають встановлювати, які обробки здатні становити специфічний ризик для прав осіб, щоб проводити їх перевірки до початку обробки даних (стаття 20). Крім того, передбачено механізм внутрішнього контролю за обробкою. З цією метою, обробник зобов'язаний призначити службовця, який буде контролювати додержання правил обробки. Це нововведення прийшло до тексту Директиви з відповідних положень законодавства Німеччини.

Спеціальні вимоги сформульовано щодо "вразливих даних": дані, які за своєю природою здатні завдати шкоди основним свободам або приватності, за загальним правилом не повинні піддаватися вільній обробці. Стаття 8 містить загальну заборону на обробку даних, що розкривають расове або етнічне походження, політичні погляди, релігійні або філософські переконання, членство у профспілках, а також даних стосовно стану здоров'я або статевого життя суб'єкта даних. Винятки з цього правила мають передбачатися на підставі закону у визначених випадках, деякі з яких перелічуються у вступній частині Директиви: в цілях забезпечення діяльності об'єднань громадян, метою яких є сприяння реалізації на практиці прав і свобод

індивідів, а також у галузі охорони здоров'я і соціального захисту для забезпечення якості й рентабельності послуг.

Якщо обробка звукових та зображуваних даних виконується в журналістських цілях або з метою літературного чи мистецького відображення, зокрема, в аудіовізуальному секторі, то принципи Директиви повинні застосовуватися в обмеженому вигляді. Стаття 9 вказує, що винятки повинні встановлюватися в обсязі, який необхідний для узгодження права на приватність з положеннями, що регулюють свободу виявлення поглядів, яка захищається статтею 10 Європейської Конвенції про захист прав людини і основних свобод.

Директива визначає роль наглядової інстанції як ключову для забезпечення дієвості національних положень про захист приватності персональних даних. Така інстанція повинна діяти у повній незалежності і мати низку наглядових повноважень. Стаття 28 Директиви передбачає, що думка наглядових органів враховується при розробці підзаконних нормативних актів щодо захисту прав і свобод осіб стосовно обробки персональних даних. Наглядовий орган наділяється такими повноваженнями: розслідування як з власної ініціативи, так і за зверненням суб'єкта даних, що забезпечується правами доступу до даних, на збір будь-якої інформації, необхідної для виконання наглядової функції; доступу для блокування, знищення даних, заборони обробки, попередження контролера тощо; оскарження у разі порушення національних положень або передачі справи для прийняття рішення судом. На наглядовий орган покладається також функція інформування громадськості і зацікавлених органів держави про свою діяльність шляхом подання періодичної доповіді.

Крім того, наглядовий орган може виконувати й певну регулятивну функцію. Розділ 5 Директиви передбачає, що держави-члени повинні заохочувати розробку кодексів поведінки, покликаних сприяти правильному застосуванню національних положень, враховуючи галузеві особливості. Такі кодекси можуть представлятися на розгляд наглядовому органу, який повинен вирішувати, з-поміж іншого, чи відповідають представлені йому на розгляд проекти національним положенням (стаття 27).

Іншим, не менш принциповим, є положення Директиви про заборону передачі даних до третіх країн, що не забезпечують адекватного рівня захисту. Цим, зокрема, встановлюється, що для транскордонних потоків даних з країн ЄС від одержувача даних у третій країні вимагається надання достатніх гарантій щодо дотримання ним вимог Директиви ЄС. Розділ IV Директиви за назвою "Передача персональних даних до третіх країн" присвячується саме цьому питанню. Стаття 25 встановлює принципи, які застосовуються для передачі персональних даних до третіх країн, а стаття 26 містить винятки з цих правил.

Стаття 25 вказує на критерії для оцінки адекватності рівня захисту приватності персоніфікованої інформації у третій країні. Серед них – характер даних, ціль і тривалість обробки, країна походження і країна кінцевого призначення, стан законності і дотримання норм права – як загальних (загальний рівень законності), так і галузевих (у галузі захисту приватності), – що діють у третій країні, а також професійні норми і заходи безпеки, що застосовуються у цій країні.

Однак можливість передачі персональних даних до третіх країн, які не надають адекватного рівня захисту приватності, все-таки існує. Стаття 26 перелічує ці випадки: суб'єкт даних надав свою чітку згоду; передача є необхідною для укладення або виконання контракту між суб'єктом даних і контролером чи між контролером і третьою стороною в інтересах суб'єкта даних; передача є необхідною для забезпечення важливого державного інтересу або суб'єктивного права під час судочинства; передача є необхідною для захисту життєвих інтересів суб'єкта даних; передача здійснюється з доступного для громадськості джерела (реєстру). Крім цього, за окремим дозволом уповноваженого органу (мається на увазі, насамперед, наглядова інстанція), можлива передача або низка передач персональних даних до третьої країни, яка не гарантує адекватного захисту, якщо контролер доведе адекватність гарантій щодо захисту права на приватність, основних прав і свобод осіб, а також стосовно реалізації відповідних прав; ці гарантії можуть випливати, зокрема, з відповідних договірних положень.

Запропонований підхід до регулювання транскордонної передачі даних було піддано критиці з боку Міжнародної Торгової Палати під час законодавчого

проходження Директиви, яка відстоювала позицію, що гармонізація міжнародного права у галузі захисту приватності персональних даних повинна, швидше за все, відбуватися на основі моделі Керівних Принципів ОЕСР та Конвенції Ради Європи № 108, а ніж на стандартах, запропонованих Європейським Союзом.

Незважаючи на лобіювання, відповідне положення залишилося у тексті Директиви, що пояснюється намаганням країн ЄС встановити вищий рівень захисту приватності порівняно зі стандартами Ради Європи і створити, так званий, "європейський простір вільного руху інформації". Досягнення такої мети передбачається завдяки зусиллям, спрямованим на зближення національних законів через імплементацію Директиви у внутрішнє право країн ЄС. Це запровадження мало відбутися впродовж трирічного терміну з дати набуття Директивою чинності, тобто до 24 жовтня 1998 року. Однак не всі країни ЄС впоралися з цим завданням у відведений час, що стало приводом для прийняття Робочою групою відповідної рекомендації у лютому 2000 року, в якій вказується на необхідність негайного виправлення ситуації [207].

Робоча група, створена на підставі статті 29 Директиви, має консультативний статус і діє незалежно. Вона складається з представників національних наглядових органів держав-членів, представника органів, створених установами та органами Європейського Співтовариства (Союзу) і представника Європейської Комісії.

Робоча група виконує дослідницьку, експертну і консультативну функції. Згідно зі статтею 30 Директиви, вона досліджує питання щодо застосування національних положень, надає висновки про рівень захисту приватності як всередині Європейського Союзу, так і в третіх країнах, а також про відповідність кодексів поведінки, прийнятих на рівні ЄС, вимогам Директиви. Робоча група надає також консультації Комісії щодо подальших змін цієї Директиви та можливих додаткових чи спеціальних заходів для забезпечення прав і свобод осіб стосовно обробки персональних даних.

З метою галузевого застосування принципів, що їх проголосила Директива 1995 року, Європейський Парламент ухвалив 15 грудня 1997 року Директиву № 97/66/ЕС стосовно обробки персональних даних і захисту приватності у телекомунікаційному

секторі [208]. Директива № 97/66/ЕС доповнює і конкретизує положення основної Директиви 1995 року. Положення цієї Директиви зобов'язують країни ЄС забезпечити через національне регулювання приватність інформаційних потоків у сфері загальнодоступних телекомунікаційних мереж та загальнодоступних телекомунікаційних послуг. Ці зобов'язання, зокрема, стосуються приватності операційних даних, тобто інформації, яка збирається операторами під час надання телекомунікаційних послуг.

Забезпеченню приватності у телекомунікаційному секторі присвячені також рекомендації Робочої групи, ухвалені 23 лютого [209] і 3 травня 1999 року [210], а питанню вдосконалення принципів основної Директиви 1995 року і приведення їх у відповідність до сучасного стану розвитку телекомунікаційних і мультимедійних технологій – висновок Робочої групи від 3 лютого 2000 року [211].

Увага, яку Європейські інституції приділяють цьому питанню, пояснюється важливістю захисту прав людини і права на приватність інформаційного обміну, зокрема, для повноцінного користування громадянами ЄС перевагами новітніх інформаційних технологій для розбудови інформаційного суспільства в Європі. Ця причина зумовила прийняття в липні 2002 року Директиви про захист приватності у секторі електронних комунікацій, яка замінила собою Директиву 97/66/ЕС [212].

Узгодження положень національного законодавства з питань захисту приватності персоніфікованої інформації в контексті транскордонної передачі, яка здійснюється в цілях боротьби із злочинністю, постає надзвичайно актуальним з огляду на транснаціоналізацію злочинності і необхідність ефективного співробітництва національних правоохоронних структур на регіональному й міжнародному рівнях.

Це питання розглядається як необхідний елемент загальноєвропейської політики, спрямованої на створення, так званого, "простору свободи, безпеки і правосуддя" в Європі. Амстердамський Договір змінив підхід до співробітництва європейських країн у галузі правосуддя і внутрішніх справ, визначивши простір свободи, безпеки і правосуддя програмно і чітко. Постановивши за мету забезпечення вільного пересування по Європейському Союзу як громадян, так і не громадян, цей документ

наголосив на необхідності гарантування безпеки шляхом боротьби з усіма формами організованої злочинності та тероризмом.

Слід зазначити, що в українській правовій науці ці питання залишаються мало дослідженими. Можна назвати лічені публікації з цього актуального питання, з-поміж яких видання автора цієї роботи [1)]. Проблемам функціонування Шенгенської інформаційної системи, впливу візового режиму на пересування громадян України по Європі присвячене також інформаційно-аналітичне видання Центру миру, конверсії та зовнішньої політики України [213]. Ці актуальні питання були предметом уваги здебільше зарубіжних дослідників. В контексті правоохоронної діяльності питання захисту приватності персоніфікованої діяльності на європейському рівні в рамках Шенгенської Конвенції аналізують Дж. Дюмортьє [214], Г. Салберіні [215], Л. Коррадо [216]. Питанням реалізації принципів захисту приватності персоніфікованої інформації у діяльності Європейської Поліцейської Установи (Європол) приділяє увагу іспанський науковець Дж.Д. Торренс [217]. Схожою за тематикою, але більш розгорнутою з точки зору досліджуваного матеріалу є праця Т. Зердік, в якій вивчається співвідношення нормативних приписів, що містяться в документах із питань європейської інтеграції, зокрема, у сфері правоохоронної діяльності, і Конвенції Ради Європи №108 про захист фізичних осіб стосовно автоматизованої обробки персональних даних [218]. Теоретичні й практичні питання захисту приватності в контексті правоохоронної діяльності більш докладно досліджуються у спеціальному виданні Європейської Комісії за програмою “Фалконе” [219].

Зростання рівня злочинності і її транснаціоналізація є причиною, що підштовхує розвиток співробітництва європейських країни в галузі правосуддя і внутрішніх справ. Реалізація ідеї свободи пересування, незважаючи на кордони, для всіх – громадян і не громадян – вимагає адекватного вдосконалення співробітництва поліцейських установ у галузі контролю за перетинанням кордонів.

---

1) [147] Пазюк А.В. Захист прав громадян у зв’язку з обробкою персональних даних у правоохоронній діяльності: європейські стандарти і Україні. — К.: МГО Прайвесі Юкрейн, 2001. — 258 с.

Питання захисту приватності персональних даних у зв'язку з їх обробкою поліцейськими установами набуває особливої важливості для Європейського Союзу після ліквідації митних кордонів між країнами-членами Шенгенської Конвенції.

Перша домовленість "Про поступове скасування перевірок на спільних кордонах" об'єднала групу з п'яти Європейських країн (Францію, Німеччину, Бельгію, Люксембург і Нідерланди). Підписана 14 червня 1985 року, вона заклала фундамент для подальшого співробітництва європейських країн у галузі створення території без внутрішніх кордонів. Ця домовленість одержала назву Шенгенської Угоди від назви міста у Великому Герцогстві Люксембург, де відбулося її підписання.

Процес ліквідації внутрішніх кордонів і створення спільних правил паспортного контролю був продовжений підписанням Конвенції 19 червня 1990 року "Про застосування Шенгенської Угоди від 14 червня 1985 року про поступове скасування перевірок на спільних кордонах", яка вступила в силу лише у 1995 році.

Шенгенський простір поширився майже на усі країни-члени Європейського Союзу, і вже в 1997 році включав 13 країн ЄС, за винятком Великої Британії та Ірландської Республіки. З 25 березня 2001 року до Шенгенської Угоди долучаються ще дві країни Північного (Скандинавського) Паспортного Союзу, які не є членами ЄС, – Ісландія та Норвегія. Цей факт, однак, не заважає Європейським інституціям вживати заходів для поступового включення Шенгенської структури до складу "третьої колони", на якій "тримається" Європейський Союз, а саме регулювання співробітництва між національними правоохоронними і судовими органами країн ЄС.

Запроваджений Амстердамським Договором простір свободи, безпеки і правосуддя дозволив включити Шенгенську Угоду до структури Європейського Союзу. Цим же Договором, що набув чинності 1 травня 1999 року, повноваження Виконавчого Комітету Шенгенської Конвенції були передані Раді Європейського Союзу.

З метою сприяння діяльності правоохоронних органів особливо з огляду на труднощі, які виникають через надання громадянам європейських і неєвропейських країн свободи вільного пересування в Шенгенському просторі, було створено комплексну інформаційну систему для обміну відомостями про осіб, а також про

вкрадені або загублені речі. Інформаційна система складається з мережі, до якої підключені національні підрозділи, інформаційного центру, а також операційної системи задоволення запитів національних підрозділів під назвою "СІРЕН" (**фр.** *Supplément d'Information Requis a l'Entrée Nationale*).

Цю операційну систему з вересня 2001 року замінено на нову – "СІСНЕТ", в якій додатково обробляються відомості про імміграцію. Функції технічної підтримки цієї системи забезпечує Французька Республіка; служби технічного забезпечення розташовуються в Страсбурзі.

Ліквідація контролю під час перетинання внутрішніх кордонів усередині Шенгенської зони компенсується спільним контролем за перетином її зовнішніх меж, який здійснюється національними підрозділами в загальному порядку визначеному Шенгенською Конвенцією. Під час такого контролю перевіряються як громадяни країн Шенгенського простору, так і громадяни інших країн. Він включає перевірку ідентифікуючих особу документів, а для громадян інших країн – ще й додатково наявність офіційного дозволу на в'їзд та відсутність підстав для затримання цієї особи у будь-якій Шенгенській країні. Інформація, необхідна для проведення контролю, надається згаданою інформаційною системою, в якій містяться відомості про всі ордери на затримання, видані в Шенгенських країнах, а також відмови на в'їзд негромадянам. Інформація в системі утримується в стані постійного оновлення в режимі реального часу.

У разі відсутності дозволу на в'їзд негромадянин позбавляється доступу на територію Шенгенського простору. За наявності підстав для затримання, передбачених Шенгенською Конвенцією, особа підлягає затриманню на кордоні. Такими підставами можуть бути: судовий ордер на арешт або на екстрадицію цієї особи під юрисдикцію іншої Шенгенської країни (стаття 95); відомості про зникнення особи або про необхідність надання їй спеціального захисту (стаття 97); відомості про необхідність дачі цією особою свідчень у суді або відбуття покарання у вигляді позбавлення волі (стаття 98).

Шенгенська інформаційна система містить такі вхідні дані, що стосуються осіб (стаття 94): прізвище, ім'я, а також інші імена (псевдоніми, прізвиська), якими

користується особа і які можуть бути зареєстровані; особливості зовнішнього вигляду, його сталі характеристики; першу літеру імені по батькові; дату і місце народження; стать; національність; наявність зброї; агресивність (готовність до вчинення насильства); підстави для внесення відомостей до системи; заходи, яких належить вживати стосовно осіб у випадку її ідентифікації під час контролю.

До інформаційної системи заносяться відомості про іноземців, щодо яких зроблено інформаційний запит з метою відмови у допуску. Шенгенські країни вирішують питання щодо запиту на підставі своїх національних положень з додержанням відповідних процесуальних норм. Стаття 96 Конвенції доволі розпливчасто визначає підстави для прийняття таких рішень, залишаючи це на розсуд країнам. Такими підставами є: загроза громадському порядку чи національній безпеці та спокою, що може спричинитися через перебування іноземця на території країни; іноземець є об'єктом депортації, примусового повернення чи вислання, дія яких не відмінена і не зупинена, внаслідок недодержання національних правил про в'їзд і перебування іноземців.

Уведена інформація використовується для здійснення негласного стеження чи спеціального контролю, коли на це є наступні підстави: наявна об'єктивна інформація про підготовку до вчинення або скоєння злочину цією особою; загальна оцінка цієї особи, здійснена на підставі її попередніх злочинів, свідчить про вірогідність повторення особливо небезпечних злочинів; одержання відомостей необхідно для відвернення серйозної загрози внутрішній і зовнішній безпеці держави.

В рамках негласного стеження для органу, що надіслав інформаційний запит, може збиратися і передаватися інформація, зібрана національними правоохоронними органами під час вжиття профілактичних і запобіжних заходів всередині країни. Негласно одержана інформація може включати наступні відомості: про факт виявлення особи або транспортного засобу, щодо яких направлено інформаційний запит; місце, час і підстави вжитих заходів; маршрут та місце призначення поїздки; супроводжуючих осіб або пасажирів транспортного засобу; транспортний засіб, що використовується; предмети, що перевозяться; обставини, за яких було виявлено особу чи транспортний засіб.

За процедурою спеціального контролю, особи, транспортні засоби та предмети, що перевозяться, можуть бути піддані обшуку у відповідності з національними процесуальними нормами для одержання зазначено інформації.

Питанням контролю за безпекою персональних даних і дотримання прав осіб, щодо яких здійснюється їх обробка в Шенгенській інформаційній системі, присвячується третя глава в Розділі IV Конвенції (статті 102-118), а також окремий Розділ VI під назвою "Захист персональних даних" (статті 126-130).

Принципи правомірності обробки персональних даних, проголошені Конвенцією Ради Європи "Про захист осіб стосовно автоматизованої обробки персональних даних" 1981 року № 108, а також в Рекомендації № R (87)15 Комітету Міністрів Ради Європи, інкорпоровані до Шенгенської Конвенції. Зокрема, стаття 126 Шенгенської Конвенції вимагає від кожної з країн-членів прийняття національних положень з захисту персональних даних, які мають гарантувати рівень правового захисту не нижчий, ніж стандарти, впроваджені Конвенцією Ради Європи № 108. Ця ж стаття забороняє будь-яку передачу персональних даних до країн, рівень захисту в яких не відповідає вимогам Конвенції Ради Європи №108. Крім того, на сторону, яка одержує дані, покладається зобов'язання використовувати їх лише у цілях, передбачених Конвенцією. При цьому такі дані можуть використовуватися лише судовими органами. Перед передачею даних повинна бути здійснена перевірка їх точності. Неточні дані підлягають уточненню або знищенню, про що повідомляються всі їх одержувачі.

Особи, яких стосується інформація введена до інформаційної системи, можуть здійснювати своє право на доступ до таких відомостей у кожній Шенгенській країні відповідно до положень національного законодавства за місцем звернення. У разі оскарження факту занесення персональних даних до вказаної системи або звернення щодо внесення уточнення чи знищення персональних даних, рішення приймається національним наглядовим органом після одержання пояснення від компетентного органу держави, відповідальної за внесення даних. Таке рішення має обов'язковий характер на території всіх Шенгенських країн.

Якщо повідомленням недостовірних або частково неточних даних було порушено права суб'єктів даних, завдано збитки тощо, компенсація заподіяної зацікавленим особам шкоди у повному обсязі здійснюється згідно з національними положеннями країн-членів. Кінцеву відповідальність у порядку регресу несе сторона, яка повідомила недостовірні дані, що призвело до заподіяння шкоди особам.

З метою здійснення внутрішнього контролю будь-яке направлення або одержання персональних даних підлягає реєстрації в базі даних (національній складовій інформаційної системи). Такі ж самі правила поширюються на неавтоматизовану (ручну) обробку і передачу персональних даних.

Гарантувати дотримання правил поводження з персональними даними і, відповідно, прав суб'єктів даних повинні національні органи, які уповноважені здійснювати незалежний нагляд. У разі відсутності такої гарантії передача даних до такої країни забороняється. Персональні дані, внесені до Шенгенської інформаційної системи, використовуються не лише в цілях контролю під час перетинання кордонів Шенгенського простору, але й у правоохоронній діяльності поліцейських установ і судових органів Європейських країн.

Співпраця поліцейських установ Європейського Союзу набула певних інституційних форм із створенням Європейської Поліцейської Установи, скорочена назва якої – Європол. Перша офіційне посилання на Європол міститься в Маастрихтському Договорі 1992 року, в статті К. 1.9 якої країни-члени ЄС зобов'язуються вважати об'єктом спільного інтересу такі сфери: співпрацю поліції з метою запобігання і приборкання тероризму, незаконного обігу наркотиків та інших серйозних форм міжнародної злочинності, включаючи за необхідності аспекти співпраці митних установ, – з огляду на організацію загальноєвропейської системи обміну інформацією через Європейську Поліцейську Установу (Європол).

Після підписання Конвенції Європол у липні 1995 року знадобилось ще три роки, щоб парламенти всіх країн-членів ЄС її ратифікували. Вступивши в силу 1 жовтня 1998 року, Конвенція дозволила Європол розпочати свою діяльність з 1 липня 1999 року.

Сферами, на які поширюється компетенція Європол (до них долучаються нові) є: запобігання і приборкання тероризму; незаконного обігу наркотиків; торгівлі людьми (в тому числі виробництво і поширення дитячої порнографії); злочинів, пов'язаних з нелегальною імміграцією; протизаконного обігу радіоактивних і ядерних речовин; торгівлі викраденими автомобілями; підробки грошей і засобі платежу; відмивання грошей, здобутих злочинним шляхом, які пов'язані з міжнародною злочинністю.

Європол має такі основні завдання: покращити обмін інформацією між поліцейськими установами країн-членів Європейського Союзу; одержувати, класифікувати і аналізувати інформацію й відомості; повідомляти без затримки компетентним установам країн-членів ЄС інформацію, що їх стосується, а також про будь-які зв'язки, встановлені між кримінальними вчинками; надавати допомогу у розслідуваннях, які здійснюються національними поліцейськими підрозділами; підтримувати комп'ютеризовані системи зібраної інформації тощо.

Однією з унікальних характеристик Європол є те, що в рамках цієї установи постійно підтримується зв'язок з національними підрозділами через офіцерів зв'язку, призначених країнами-членами для роботи у складі центрального апарату Європол. Крім того, досягається певна централізація правоохоронної діяльності на Європейському рівні, завдяки організації підрозділів-представництв Європол, які служать проміжними ланками для обміну інформацією з національними поліцейськими органами.

Для виконання своїх завдань Європол утримує інформаційну систему, в якій збираються, сортируються й аналізуються відомості, що можуть бути використані для розслідування злочинів. Основна перевага наявності спільної інформаційної системи полягає в тому, що одержані від національних підрозділів розрізнені дані після їх опрацювання в системі дозволяють на ранніх стадіях розслідування виявляти зв'язки, які не могли б бути встановлені під час їх первинного аналізу національними підрозділами.

Інформаційна система Європол, зокрема, містить наступні види персональних даних (стаття 9): прізвище, дівоче прізвище, а також інші імена (псевдоніми,

прізвиська); дата і місце народження; національність; стать; особливості зовнішнього вигляду, його сталі характеристики.

Крім того, інформаційна система Європол використовується для обробки додаткової інформації стосовно обставин скоєння чи підготовки до вчинення злочинів; засобів вчинення злочинів; підрозділів, що здійснювали розслідування, а також матеріалів розслідування; підозрюване членство в злочинній групі; пред'явленні звинувачення.

Уведені дані повинні стосуватися лише осіб, які готуються вчинити злочин, підозрюються у вчиненні або причетності до злочину, на який поширюється компетенція Європол, а також звинувачених у такому злочині (стаття 8).

Персональні дані, які збираються і накопичуються в інформаційній системі, передаються до неї національними підрозділами держав-членів Конвенції, третіми державами чи міжнародними організаціями і органами як за власною ініціативою, так і на запит Європол.

Розділ IV Конвенції Європол містить положення, які регулюють обробку персональних даних, у тому числі принципи захисту приватності. Стаття 14 покладає на держави-члени зобов'язання узгодити національне законодавство із стандартами захисту приватності персональних даних у галузі правоохоронної діяльності, зокрема тими, що запроваджуються в Конвенції Ради Європи № 108, а також Рекомендації № R (87)15 Комітету Міністрів Ради Європи. Невиконання цієї умови матиме наслідком заборону на передачу персональних даних.

Відповідальність за дотримання правил поводження з персональними даними покладається на державу-члена Конвенції, яка уводить або передає дані, а також на Європол, якщо дані одержані від третіх сторін, заносяться до інформаційної системи безпосередньо офіцерами Європол чи отримані в результаті проведеного офіцерами Європол аналізу. Оскільки передбачається розмежування відповідальності між суб'єктами обробки, інформаційна система повинна забезпечувати можливість їх розпізнавання.

Стаття 16 Конвенції Європол передбачає механізм внутрішнього контролю за дотриманням законності під час обробки персональних даних в інформаційній

системі Європол. Один з десяти випадків використання персональних даних, а також кожне їх виправлення підлягають перевірці з точки зору їх відповідності вимогам Конвенції, про що складається звіт.

Загальним правилом поводження з даними, одержаними з інформаційної системи Європол, є обмеження їх використання уповноваженими органами держав-членів Конвенції випадками, що підпадають під компетенцію Європол. Однак вони також можуть бути ними використані для боротьби з іншими серйозними видами злочинів, що виходять за межі компетенції Європол. При цьому будь-яка повідомляюча держава-член Конвенції або третя сторона (держава чи міжнародний орган) вправі обумовити застереження щодо подальшого використання персональних даних. У цих випадках користувач даних (Європол чи держава-член Конвенції) повинен узгодити зі стороною, що передає, умови використання даних у кожному конкретному випадку.

Стаття 18 Конвенції Європол закладає основи для співробітництва з третіми державами та організаціями, передбачаючи правила передачі персональних даних, що містяться в інформаційній системі Європол, сторонам, які не є членами Конвенції. Це питання є важливим для України з огляду на потреби розширення співробітництва з Європейським Союзом у галузі правоохоронної діяльності.

Передача персональних даних третім державам та організаціям дозволяється, коли це необхідно, в окремих випадках в цілях запобігання чи боротьби із злочинами, які входять до компетенції Європол. При цьому третя держава чи організація повинні забезпечувати адекватний рівень захисту приватності персональних даних.

Це положення запозичене зі статті 25 Директиви № 95/46 СЕ Європейського Парламенту і Ради “Про захист фізичних осіб стосовно автоматизованої обробки персональних даних та безперешкодного руху цих даних”. Для оцінки адекватності рівня захисту до уваги братимуться такі умови, як характер даних, ціль запропонованої обробки, її тривалість, а також які положення законодавства застосовуються до передачі персональних даних. Необхідною умовою для передачі даних на вказаних вище підставах є наявність у третій державі чи організації

механізму нагляду за дотримання законності використання персональних даних, який здійснюється уповноваженим органом.

Питання передачі персональних даних до третіх держав чи організацій деталізуються в Акті Ради Європейського Союзу від 12 березня 1999 року. Загальною підставою для передачі персональних даних є відповідна угода між керівним органом Європол та третьою державою чи організацією. Рішення про укладення угоди з третьою державою чи організацією приймається одноголосно Радою Європейського Союзу на підставі оцінки можливості дотримання правил обробки персональних даних третьою державою чи організацією. В угоді з третьою державою чи організацією зазначаються одержувачі даних (відповідальний орган держави чи організації), характер даних, цілі передачі та використання. Кожний запит на передачу даних також повинен містити вказівку на вказані умови одержання і використання даних.

Передачі даних третій державі або організації передує одержання згоди тієї держави-члена Конвенції Європол, яка занесла дані до інформаційної системи. Про передачу персональних даних, які уведені до інформаційної системи безпосередньо службовцями Європол, рішення також приймає Європол. Від одержувача даних (третьої держави чи організації) вимагається запевнення, що заявленої цілі використання персональних даних буде дотримано. За відсутності угоди між Європол і третьою державою чи організацією, як виняток, дозволяється санкціонована директором Європол передача, якщо це необхідно для захисту важливих інтересів держав-членів Конвенції або для відвернення навислої небезпеки, пов’язаної зі злочином. Про таку передачу негайно повідомляються правління та спільний наглядовий орган Європол.

Виключно під санкцію директора Європол можуть передаватися “вразливі дані”, які розкривають расове походження, політичні погляди, релігійні чи інші переконання, дані про здоров’я, сексуальне життя. Цим, зокрема, забезпечується вимога статті 6 Конвенції Ради Європи № 108 щодо надання додаткових гарантій стосовно обробки персональних даних, що можуть з огляду на їх характер нести підвищений ризик для безпеки прав і свобод особи.

Як зазначалося вище, право зацікавлених осіб на доступ до своїх персональних даних є важливою гарантією законності, оскільки при цьому особа здатна оскаржити можливі неправомірні дії з персональними даними. Стаття 19 Конвенції Європол регламентує порядок доступу осіб до персональних даних, що знаходяться в інформаційній системі Європол. Звернення громадян повинні адресуватися національним компетентним органам відповідно до вимог національного права. У доступі до даних може бути відмовлено, якщо це необхідно для забезпечення належного виконання Європол своїх функцій, для захисту безпеки та громадського порядку чи запобігання злочину, а також для захисту прав і свобод інших осіб.

Враховуючи міжнародний характер діяльності Європол і наявність різних джерел інформації, що потрапляє до інформаційної системи, в цій статті передбачається процедура узгодження позицій різних суб'єктів щодо вирішення питання про надання доступу. Зокрема, враховується думка держав-членів Конвенції, третіх держав і організацій, які надали персональні дані чи зацікавлені у надані чи ненадані їх для ознайомлення. При цьому, достатньо лише одного заперечення будь-якої з зацікавлених сторін, щоб персональні дані не були повідомлені.

Зацікавлена особа, прохання якої щодо доступу чи перевірки даних не буде задоволено, вправі звернутися з апеляцією до спільного наглядового органу. Цей орган приймає своє рішення після одержання висновку національного наглядового органу, який повинен здійснити перевірку дотримання національного законодавства під час розгляду звернення національним підрозділом поліції. Якщо дані уведені до інформаційної системи безпосередньо офіцерами Європол, необхідні перевірки здійснюються також Європол.

У випадку, коли персональні дані є неточними або уведені до інформаційної системи чи обробляються з порушенням вимог правил обробки, передбачених Конвенцією Європол чи національним правом, вони виправляються чи знищуються. Про це повідомляються усі одержувачі даних, держави чи організації, які їх утримують, а також суб'єкт даних, який звернувся з проханням про виправлення своїх персональних даних. Стаття 22 Конвенції Європол містить важливу гарантію запобігання приховуванню порушення прав суб'єктів даних під час процедури

знищення персональних даних, а також перешкоджання реалізації ним своїх законних інтересів. Якщо існують підстави вважати, що законні інтереси суб'єкта даних можуть бути не збереженими у разі знищення неточних даних, файли не знищуються, а маркуються спеціальними позначеннями, щоб їх не могли використати. Це ж саме правило застосовується також у випадках можливого знищення даних у зв'язку з закінченням терміну зберігання.

Стаття 21 Конвенції Європол регламентує строк зберігання і знищення персональних даних. За загальним правилом, дані зберігаються стільки, скільки це потрібно для виконання Європол своїх завдань. Перший строк обмежується трьома роками, після чого дані переглядаються на предмет можливості їх тривалішого зберігання. Держави-члени повідомляються за три місяці про наближення терміну перегляду даних. Дані, щодо яких рішення про продовження строку зберігання не прийнято, автоматично знищуються. Держава-член повідомляє Європол про знищення даних, які були раніше уведені нею до інформаційної системи. У разі необхідності Європол може не знищувати такі дані, якщо він має потребу у їх подальшому зберіганні. Про таке рішення повідомляється зацікавленій державі-члену.

Національні наглядові органи контролюють усі операції, що здійснюються національними поліцейськими підрозділами з персональними даними, а також розглядають звернення зацікавлених осіб щодо перевірки правомірності дій з персональними даними, а також у разі відмови зацікавленим особам у наданні доступу до персональних даних. Стаття 23 Конвенції передбачає, що такий наглядовий орган має діяти цілком незалежно.

Положення стаття 25 Конвенції Європол, що стосуються технічного і організаційного захисту (безпеки) даних, майже тотожні за своїм змістом відповідним положенням статті 118 Шенгенської Конвенції. Зокрема, в обох документах передбачається контроль за: доступом до обладнання, носіями і змістом даних, доступом до інформаційної системи, контроль за використанням, передачею, введенням та транспортуванням. Однак, на додаток до передбачених у Шенгенській Конвенції заходів з безпеки Конвенція Європол вказує на необхідність забезпечення

негайного полагодження систем, які вийшли з ладу, а також невідкладного повідомлення про помилкові операції. Вимагається також гарантування цілісності персональних даних у разі неправильного функціонування систем автоматизованої обробки.

Положення про технічний і організаційний захист (безпеки) персональних даних далі по тексту Конвенції Європол доповнюються в статтях 31 і 32. Крім того, Актом Ради Європейського Союзу від 3 листопада 1998 року затверджено правила про конфіденційність інформації Європол. Передбачається, що б рівень технічного і організаційного захисту (безпеки) персональних даних на території держав-членів Конвенції, був не нижчий за рівень захисту, запроваджений Конвенцією Європол, зазначеними правилами про конфіденційність інформації Європол, а також у "Керівних принципах з безпеки".

Для інформації, що знаходиться у розпорядженні Європол, крім тієї, що явно відноситься до відкритої для громадськості, за загальним правилом встановлюється основний рівень захисту. Інформація, що за своїм характером вимагає додаткових заходів з безпеки, класифікується за рівнями безпеки на три категорії: "Європол 1" , "Європол 2" та "Європол 3".

Запровадження такої системи маркування інформації не означає, що громадськість позбавлена можливості контролювати діяльність Європол. Будь-яка зацікавлена особа також має право на доступ не лише до своїх персональних даних, але й до інформації про діяльність Європол як і будь-якої іншої інституції Європейського Союзу. Це право закріплюється в Акті Ради ЄС від 20 грудня 1993 року "По доступ громадськості до документів Ради" , який прийнятий для забезпечення прозорості у роботі органів ЄС. Винятковими легітимними підставами для відмови у надані інформації для ознайомлення є захист: суспільних інтересів (державна безпека, міжнародні відносини, монетарна стабільність, розслідування злочинів, перевірка та дослідження); осіб, їх права на приватність; комерційної та виробничої таємниці; фінансових інтересів Європейських Співтовариств; конфіденційності, про що просить фізична чи юридична особа, що надала інформацію; конфіденційності роботи Ради ЄС тощо. Отже, у громадян ЄС, а також громадян третіх держав є можливість

скористатися своїм правом на доступ до інформації, що стосується діяльності Європол, якщо це не зашкоджуватиме законним інтересам суспільства, інших осіб тощо.

Безперечно, що укладення як Шенгенської Конвенції, так і Конвенції Європол позитивно вплинуло на врегулювання питань обробки персональних даних у правоохоронній діяльності на Європейському рівні. Однак відсутність міжнародних стандартів із захисту приватності персональних даних у контексті правоохоронної діяльності, які б мали обов'язковий характер для держав-учасниць відповідного міжнародного договору, залишає багато невирішених питань, що негативно позначається на правах і свободах людини.

Положення про захист приватності персональних даних, які містяться в Шенгенській Конвенції і Конвенції Європол, справедливо критикуються за їх фрагментарність і наявність прогалин. Зокрема, в Шенгенській Конвенції підстави для внесення даних до інформаційної системи сформульовані досить широко і дозволяють використовувати її, серед іншого, в політичних цілях для заборони в'їзду небажаних для влади осіб. Один з таких випадків трапився у 1998 році, коли активістці "Грінпісу" з Нової Зеландії було відмовлено у в'їзді до Нідерландів, оскільки її прізвище було внесено Францією до Шенгенської інформаційної системи як небажану особу з огляду на інтереси національної безпеки. Її "злочин" полягав у тому, що вона брала участь у демонстрації проти випробувань ядерної зброї, які проводила Франція.

В цих же цілях інформаційна система може використовуватися для стеження за профспілковими та екологічними активістами, правозахисниками. Саме з використанням Шенгенської інформаційної системи були здійснені масові арешти учасників демонстрацій в Амстердамі під час підписання Амстердамського Договору у 1997 році [220].

Також підлягає удосконаленню механізм контролю за доступом до персональних даних, що містяться в Шенгенській інформаційній системі. Станом на 2000 рік налічувалось близько 48000 комп'ютерів, підключених до Шенгенської інформаційної мережі. Про порушення режиму конфіденційності в системі свідчить

кримінальна справа, порушена у 1997 році проти двох офіцерів з Бельгії, які підозрювалися у наданні інформації з Шенгенської інформаційної системи для осіб, задіяних в організованому злочинному угрупуванні.

Конвенція Європол також не достатньо конкретно визначила питання дотримання правил обробки персональних даних одержувачами даних. Принцип невідхилення від заявленої цілі використання персональних даних чітко не прописаний у тексті цієї Конвенції.

Ці та інші недоліки чинного правового регулювання питань обробки персональних даних у правоохоронній діяльності на загальноєвропейському рівні були предметом уваги міжнародного семінару, проведеного у грудні 1999 року Радою Європи. За його результатами були запропоновані рекомендації для покращення правового регулювання як на національному, так і міжнародному рівнях [221]. Зокрема, на національному рівні рекомендовано, щоб законодавство з питань захисту приватності персональних даних у правоохоронній діяльності ґрунтувалося як на загальному законі про захист (приватності) персональних даних, так і на спеціальних нормативно-правових актах з питань обробки персональних даних різними ланками правоохоронних (поліцейських) установ.

З огляду на зростаючий обсяг транскордонної передачі персональних даних під час співробітництва у галузі правоохоронної діяльності рекомендується, щоб перед початком передачі якість даних ретельно оцінювалася; здійснювався ефективний нагляд за законністю обробки; суб'єкти даних одержували ефективну допомогу навіть за межами національних кордонів. Також наголошується на необхідності вдосконалення регулювання передачі даних до країн, які не забезпечують адекватного захисту приватності персональних даних, посиливши відповідні вимоги до одержувачів.

Захист прав громадян у зв'язку з обробкою персоніфікованої інформації в діяльності органів правосуддя також знаходиться на порядку денному інституцій Європейського Союзу. Зокрема, нещодавно прийнята Конвенція про взаємну допомогу в кримінальних справах країн-членів Європейського Союзу передбачає обмін персональними даними в рамках такого співробітництва [222]. Для цього

створюється інформаційна мережа, управління якою здійснюватиме спеціальний підрозділ з питань судового співробітництва Євроджаст (Eurojust) [223]. У грудні 2000 року тимчасовий склад Євроджаст був призначений із суддів, прокурорів і магістратів з країн-членів ЄС, які координують правові питання проведення транскордонних розслідувань, включаючи тероризм, комп'ютерну злочинність, відмивання грошей та екологічні правопорушення [224].

Між тим, питання впровадження принципів захисту приватності персональних даних у механізм відправлення правосуддя недостатньо розроблене на сьогоднішній день на теоретичному рівні та призводить до порушення прав людини на практиці. Про це свідчать результати дослідження, проведеного Європейською Комісією, в рамках реалізації проекту "Фалконе". Вирішення цього питання можливе шляхом розробки спеціальних правил захисту приватності персональних даних, які були б адаптовані до вимог кримінального і цивільного процесуального права, враховували б особливий статус учасників процесу, а також незалежний статус суддів.

Відсутність гарантій поваги до приватного життя або їх недотримання під час провадження судочинства нерідко спричиняються до порушення прав учасників судових процесів, а також інших причетних до цього осіб. Один з таких випадків був предметом розгляду Європейського Суду з прав людини.

У рішенні по справі *"Z проти Фінляндії"*, датованому 25 лютого 1997 року, Європейський Суд з прав людини встановив порушення гарантованого статтею 8 Європейської Конвенції про захист прав людини і основних свобод права на повагу до приватного життя через обмеження строку зберігання вироку суду, яке містить медичні дані про зараження заявниці ВІЛ-інфекцією, 10-а роками, а також розкриття особи заявниці та факту її зараження у тексті вироку апеляційного суду, що став доступним для преси. Європейський Суд наголосив на необхідності ретельної оцінки судами можливих наслідків втручання у приватне життя і встановлення справедливого балансу між інтересами гласності судових процесів, з одного боку, та інтересами якоїсь сторони чи третьої особи у збереженні конфіденційності таких даних, з другого боку. При цьому, означення лінії розрізнення залежить від таких факторів, як характер і серйозність цих інтересів та міра втручання [225].

Вироблені й застосовані в практиці Європейського Суду з прав людини критерії для узгодження інтересів окремої людини і суспільства служать орієнтиром для розробки законодавства Європейського Союзу про захист приватності персональних даних у галузі правосуддя. Такий позитивний приклад варто запозичити і вітчизняним законодавцям.

Підсумовуючи вищевказане, слід відзначити, що питання регулювання обробки персональних даних у правоохоронній діяльності на Європейському рівні залишається відкритим. Його вирішення великою мірою залежатиме від успіху подальшої співпраці країн ЄС у галузі створення простору свободи, безпеки і правосуддя на території Європейського Союзу. Питання захисту приватності персональних даних певним чином торкається трьох взаємопов'язаних складових цього простору. З огляду на це, Європейський Союз розпочав роботу з об'єднання цих складових у "третій колоні" з поширенням на неї вимог захисту приватності персональних даних. Про це свідчить, зокрема, Рішення Ради Європейського Союзу від 17 жовтня 2000 року, яким запроваджений об'єднаний секретаріат спільних органів нагляду за дотриманням законності під час обробки персональних даних, створений Конвенцією Європол, Конвенцією про використання інформаційних технологій для митних цілей та Шенгенською Конвенцією [226]. Секретаріат з захисту даних виконує функції, які розрізнено виконували відповідні секретаріати спільних наглядових органів цих Конвенцій Європейського Союзу.

Безперечно, що це сприятиме покращенню ефективності нагляду за додержанням законності в діяльності правоохоронних структур Європейського Союзу під час обробки й передачі персоніфікованої інформації, у тому числі за межі ЄС.

2.3. Міжнародно-правові засоби розв'язання проблеми захисту приватності в контексті транскордонної передачі персоніфікованої інформації

Той вибір, який зробили країни ЄС запровадив доволі жорсткі вимоги до правил поводження з персоніфікованою інформацією, підштовхує інші країни до перегляду власних підходів у пошуку компромісу в контексті її транскордонної передачі. Це ще більшою мірою вимагає міжнародного діалогу й розв'язання існуючих проблем за допомогою міжнародно-правових засобів. Як вже зазначалось, зусилля міжнародних організацій спрямовуються на уніфікацію міжнародно-правових стандартів і вироблення механізмів усунення перешкод для вільного обігу персоніфікованої інформації через кордони.

До процесу вироблення уніфікованих міжнародних правил у галузі захисту приватності і безперешкодного руху персоніфікованої інформації через кордони залучаються й міжнародні організації економічної орієнтації. Так, Світова Організація Торгівлі (СОТ) забороняє державам-учасницям накладати обмеження на транскордонну передачу даних, хоча й передбачає можливість застосування винятків в інтересах захисту приватності, але забороняє вдаватися до дискримінаційних дій проти інших її учасників. Це положення забезпечується можливістю розгляду СОТ заяв про застосування обмежень щодо передачі персональних даних і застосування санкцій.

Серед претендентів на роль, так би мовити, уніфікатора міжнародних стандартів захисту приватності розглядається й Міжнародна Організація Стандартизації (ISO). Вперше офіційно таку ініціативу висунув Комітет Асоціацій споживачів (COPOLCO) у травні 1994 року, прийнявши резолюцію щодо створення робочої групи для вивчення питання, чи потрібно починати на міжнародному рівні роботу стосовно захисту персональних даних і приватності, і взяти за основу в цій роботі проект стандарту Канадської Асоціації Стандартизації. Робоча група, виконавши це завдання, рекомендувала у квітні 1996 року Комітету Асоціацій споживачів

поставити перед МОС питання про доцільність початку такої роботи. Генеральна Рада МОС у вересні 1996 року на щорічній нараді у Лондоні схвалила ініціативу щодо вивчення питання про розробку міжнародних стандартів захисту приватності і поклала це завдання на Технічну Колегію МОС. Однак створена у червні 1998 року робоча група дійшла висновку, що вироблення нових міжнародних стандартів є передчасним.

Професор з Канади К. Беннетт, досліджуючи необхідність запровадження міжнародних стандартів захисту приватності саме в рамках Міжнародної Організації Стандартизації, пропонує такі інструментальні функції майбутніх стандартів [227]:

1) зменшення стурбованості споживачів (Модельний Кодекс МСО потенційно більш ефективний шлях для споживачів при з'ясуванні, яка компанія надає більш адекватний захист приватності);

2) демонстрації адекватного захисту приватності (стосується неєвропейських обробників персональних даних, які зможуть довести адекватність захисту для своїх партнерів з ЄС);

3) задоволення експортера даних (існуючі моделі регулювання транскордонних потоків даних покладають на експортера даних відповідальність за дотримання кожним здобувачем даних принципів захисту приватності; експортер даних зацікавлений у посиленні гарантій, що принципів буде дотримано здобувачами);

4) сприяння більшій міжнаціональній і між-секторній узгодженості (деякі компанії через нечесну практику щодо інформації про споживачів набувають певних конкурентних переваг; компанії, які дотримуються принципів приватності, потребують більш безпечних і надійних засобів для демонстрації ними чесної інформаційної практики, що буде заохочувати споживачів);

5) допоміжної регуляції (стандарти МСО можуть впроваджуватися в закони і кодекси, включатися до контрактів про надання послуг з обробки персональних даних);

6) сприяння поширенню чесної інформаційної практики в Інтернет (міжнародні стандарти можуть становити єдиний засіб “виміру” для оцінки “дружелюбності” певних веб-сторінок і сприяти глобалізації електронної комерції);

7) стандартизації регулювання використання криптографічних ключів для кодування (розвиток засобів кодування і їх використання в електронній комерції для посвідчення угод, наприклад, за допомогою “цифрового” підпису, може розглядатися лише в контексті більш широких стандартів, які включають, серед іншого, принципи чесної інформаційної практики).

На нашу думку, механізм сертифікації рівня захисту приватності як складової інформаційної практики організацій має право на існування. Зокрема, існуючий стандарт підтвердження якості ISO 9000 може бути використаний для розробки окремого стандарту інформаційної приватності або, завдяки своїй універсальності, - доповнений вимогами щодо якості інформаційної практики щодо персональних даних.

Одним з перших прикладів успішного застосування стандартизації у галузі захисту приватності є досвід Британської Поштової Служби, яка через стандарт ISO 9000 зареєструвала свої операції з обробки персональних даних. На національному рівні це вперше зробила Канадська Асоціація Стандартизації, прийнявши у 1996 році Модельний Кодекс захисту персональної інформації [228].

Вирішення питання захисту приватності в глобальних, наднаціональних мережах за наявності розбіжностей в регулятивних нормах на національному і міжнародному рівнях залишається проблематичним. Професор Дж. Райденберг як один з можливих шляхів подолання проблеми пропонує запровадження міжнародних технічних стандартів, які діють на рівні мережі і можуть бути незалежні від національних кордонів [229].

Необхідність втілення правил поводження з персоніфікованою інформацією в технічні стандарти визнається експертами Європейського Союзу як важливий крок для узгодження розбіжностей між національними законодавствами [230]. Відповідні розробки ведуться й на європейському рівні. Створена Європейською Організацією Стандартизації група під назвою “Ініціатива зі Стандартизації Приватності в Європі”

підготувала доповідь з актуальних питань стандартизації у галузі захисту персоніфікованої інформації [231], яку високо оцінили експерти ЄС [232].

Над виробленням способів вирішення неузгоджених питань захисту приватності під час транскордонної передачі даних працюють на міжнародному рівні незалежні групи експертів, які часто створюються після обговорення тих чи інших актуальних питань на міжнародних конференціях, присвячених захисту приватності з урахуванням розвитку інформаційних технологій. Уже традиційною є міжнародна конференція представників наглядових органів з захисту приватності. Двічі на рік проводяться наради "Міжнародної Робочої Групи з захисту приватності в телекомунікаціях", на яких обговорюється розвиток національних положень, а також актуальні питання захисту приватності у зв'язку з появою нових різновидів електронних комунікацій і мультимедійних технологій.

Однак досягти компромісу між різними стандартами захисту приватності, впроваджених у національні правові системи, неможливо без міжнародного обговорення із залученням представників усіх зацікавлених сторін, міжнародних організацій, урядів країн, приватного сектору, організацій стандартизації, громадських організацій, організацій споживачів тощо. Такі представницькі наради проводяться, зокрема, в рамках Організації Економічної Співпраці і Розвитку. Прикладом успішного обміну думками між приватним сектором, науковими експертами, адвокатами-правозахисниками і урядами може бути проведений ОЕСР у лютому 1998 року семінар "Захист приватності у глобальному інформаційному суспільстві" [233]. Хоча ця організація приділяє більше уваги економічним аспектам захисту приватності в контексті захисту прав "користувачів" і "споживачів", а не "громадян" чи "індивідів". Це пояснюється впливом ліберального (ринкового) підходу, який лежить в основі позиції Сполучених Штатів щодо регулювання питань обробки персональних даних. Саме ця обставина унеможливлює досягнення компромісу в цьому питанні на принципах, запроваджених Радою Європи в Конвенції № 108, які базуються на соціально-захисному підході, пріоритетом якого є повага до прав людини, а не ринкові чинники.

У 1997 році в Монреалі (Канада) на Міжнародній конференції з питань захисту приватності, з вуст її організаторів пролунала пропозиція створити нову міжнародну організацію, яка б займалася питаннями координації міжнародних зусиль у вирішенні питання узгодження національних підходів до захисту приватності [234].

За іншою пропозицією, потрібно створити нову міжурядову організацію за зразком Генеральної Угоди про Торгівлю Товарами. Діяльність запропонованої договірної структури, Генеральної Угоди про Інформаційну Приватність, мала б зосередитися на питаннях забезпечення співіснування різних режимів, а через деякий час, на гармонізації діючих стандартів інформаційної приватності. Автор цієї концепції, професор Дж. Райденберг пропонує укладення Генеральної Угоди про Інформаційну Приватність у рамках СОТ, у якій є для цього необхідний інституційний механізм. Однак при цьому зазначає, що існує ризик "комерціалізації" питань захисту приватності з огляду на прихильність цієї організації до ліберальних, ринкових норм, що створює проблеми для впровадження соціально-захисного підходу.

Наскільки успішно ініціативи щодо розробки нових міжнародних стандартів будуть втілені у життя, покаже час. Однак проблема ліквідації бар'єрів для транскордонної передачі персоніфікованої інформації залишається дуже актуальною. В даний момент часу, коли існуючі міжнародні стандарти не гармонізовані, вихід зі складної ситуації нормативної неузгодженості в питанні транскордонної передачі даних можливий, серед іншого, за допомогою договірної моделі захисту приватності, що розглядається нижче.

Як уже зазначалось, існують кілька основних національних моделей правового захисту приватності персоніфікованої інформації. Насамперед, це модель комплексного законодавчого регулювання і модель саморегуляції. Однак питання надання "еквівалентного" чи "адекватного" у європейському розумінні рівня захисту під час передачі персональних даних за межі юрисдикції тієї чи іншої держави, як того вимагають міжнародні стандарти у цій галузі, не вирішується лише на підставі оцінки обраної моделі національного регулювання у третій країні. Разом з тим, використання договірної моделі розглядається як один з можливих способів

запобігання нетарифним обмеженням економічного співробітництва між країнами з різним рівнем захисту права на приватність персоніфікованої інформації.

Контрактні положення повинні забезпечити належний захист і гарантувати безперешкодну передачу персональних даних через кордони. Використання контрактів для уникнення можливих непорозумінь під час транскордонних потоків даних бере свій початок ще у 80-х роках двадцятого століття. Саме в цей період міжнародні організації почали розробку відповідних положень, які б стали стандартами при застосуванні контрактної форми.

Під час обговорення поняття "еквівалентний захист", Консультативний Комітет, до складу якого входять представники країн-сторін Конвенції Ради Європи 1980 року № 108, відмічав досвід деяких країн щодо використання контрактної моделі для забезпечення захисту приватності в контексті транскордонних потоків даних як у публічному, так і приватному секторах. Досвід цих країн надав поштовху процесу розробки модельного міжнародного контракту.

Про можливість використання контрактної форми для транскордонного обміну даними йдеться також у деяких галузевих рекомендаціях з питань захисту приватності, прийнятих Комітетом Міністрів Ради Європи. Зокрема, принцип 8.2 вищезгаданої Рекомендації № R (86) 1 "Про захист персональних даних, які використовуються у соціальному страхуванні" звертає увагу на необхідність закріплення у контрактах додаткових гарантій у разі передавання таких даних до країн, в яких не існує законодавства про захист даних.

У свою чергу, параграф 69 пояснювальної записки до Рекомендації Комітету Міністрів № R (87) 15 "Про використання персональних даних у поліцейському секторі" вказує: якщо правоохоронний орган сторони-відправника встановлює умови використання даних у країні, де перебуває одержувач (наприклад, щодо тривалості зберігання даних), то такі умови повинні поважатися.

Параграф 63 пояснювальної записки до Рекомендації Комітету Міністрів № R (89) 2 "Про захист персональних даних, що використовуються з метою найму працівників" пропонує укладення контракту, який зобов'язує одержувача даних у

країні, де не існує законодавства про захист даних, поважати принципи, викладені у вказаній рекомендації.

Як показує практика, об'єднання спільних зусиль міжнародних організацій для підготовки уніфікованих модельних правил транскордонної передачі даних має значення не лише для узгодження позицій представників таких міжнародних організацій з тих чи інших питань, а й для зближення самих стандартів захисту приватності. Це, зокрема, підтверджується запропонованими змінами до Конвенції Ради Європи № 108 у зв'язку із прийняттям Директиви ЄС 1995 року.

"Модельний Контракт для забезпечення еквівалентного захисту даних щодо транскордонних потоків даних", – таку назву має документ Ради Європи, підготовлений у 1992 році як результат спільного проекту Ради Європи, Комісії ЄС і Міжнародної Торгової Палати [235]. Модельний Контракт містить низку модельних положень, покликаних забезпечити еквівалентний захист для транскордонної передачі даних, базуючись на положеннях Конвенції Ради Європи № 108.

Згідно з Модельним Контрактом, ліцензіар (сторона, яка надсилає дані за межі юрисдикції держави) гарантує, що дані були одержані й зберігалися у відповідності з вимогами національного законодавства країни, в якій здійснюється діяльність. Зокрема, це стосується принципів, які містяться у статті 5 Конвенції Ради Європи № 108 щодо підстав правомірності і законності обробки, обмеження ціллю збору, адекватності і не надмірності даних, точності та санкціонованого часу зберігання.

Ліцензіат – сторона, яка одержує дані, – у свою чергу, зобов'язується дотримуватися цих принципів, які застосовуються до ліцензіара у його країні. Ліцензіат також погоджується використовувати дані лише з ціллю, яка визначається у контракті, і зобов'язується захищати вразливі дані у спосіб, який вимагається за законодавством країни ліцензіара, не поширювати дані іншим сторонам, крім випадків, обумовлених контрактом, а також знищувати чи вносити зміни до даних на вимогу ліцензіара.

Інші положення Модельного Контракту присвячені питанням відповідальності за втрату даних їх одержувачем, правам суб'єкта даних, вирішенню спорів і розірванню контракту. Пропонується механізм вирішення спорів шляхом залучення арбітрів.

Сторонам дається право самим визначити, право якої країни буде застосовуватися до контракту.

Модельний Контракт Ради Європи 1992 заклав фундамент для подальших розробок у галузі договірного врегулювання питань транскордонної передачі даних за схемою "бізнес до бізнесу" (*B2B*), тобто коли сторонами такого контракту є лише відправник і одержувач персональних даних, а сам суб'єкт даних є потенційним набувачем відповідних прав за контрактом. Зокрема, це стосується права на одержання компенсації у разі порушення передбачених таким контрактом правил поводження з персоніфікованою інформацією.

Така модель врегулювання транскордонної передачі персональних даних зараз широко використовується на практиці. Одним з найбільш відомих випадків, який, на думку фахівців, може бути прикладом успішного вирішення проблеми транскордонної передачі персональних даних до країни, рівень захисту інформаційної приватності в якій нижчий порівняно з країною відправлення, є реалізований у 1996 році німецькою державної корпорацією "Німецька залізниця" проект впровадження електронних карток для подорожування залізничним транспортом. За цим проектом, "Німецька залізниця" уклала угоду з відомим банком "Сітібанк" про запровадження комбінованих карток для проїзду, які також могли використовуватися їх власниками для безготівкового розрахунку за товари і послуги як звичайні кредитні картки.

Персоніфікована інформація, яка міститься на такій картці, проходить доволі великий шлях під час "життєвого" циклу самої картки. Персональні дані потенційного клієнта збираються на одній зі станцій або одним з агентів залізниці і направляються до підрозділу банку в Німеччині. Після перевірки вони кодуються і надсилаються до дочірньої фірми банку у Південну Дакоту (США). Ця фірма організовує виготовлення карток за допомогою іншої дочірньої компанії банку у Неваді (США), після чого картки запаковані у конверти, надсилаються до Нідерландів, а звідси – до одержувачів у Німеччині. Використання голландської компанії для пересилки пояснюється тим, що в Нідерландах поштові послуги коштують дешевше, ніж в Німеччині.

Запропонований контракт про врегулювання передачі персональних даних за проектом “Німецької залізниці” з’явився після того, як німецькі споживачі почали активно вимагати від компанії гарантування захисту їхньої інформаційної приватності під час передачі і обробки персональних даних у США. Ці вимоги були підтримані наглядовими інстанціями у галузі захисту приватності ФРН.

“Міжтериторіальна угода”, а саме таку назву одержав цей контракт між дочірніми компаніями банку в Німеччині і США, передбачає наступні важливі положення:

1. До відносин, які регулюються цим контрактом, застосовується законодавство ФРН, оскільки споживачами є громадяни Німеччини.
2. Обробка даних у США дозволяється лише з метою виготовлення карток.
3. Дочірні компанії банку в Німеччині і США не мають права передавати персональні дані третім особам у комерційних цілях за винятком, що персональні дані власників кредитних карток можуть передаватися лише підрозділам цього банку для надання фінансових послуг, а дані про володарів звичайних карток – для рекламування кращих карток з платіжною функцією.
4. Технічний захист даних розписаний детально відповідно до вимог законодавства ФРН.
5. Американська дочірня компанія банку зобов’язується призначити посадову особу для внутрішнього контролю за дотриманням правил поводження з персональними даними, слідуючи вимогам законодавства ФРН.
6. Німецький споживач – володар картки має всі індивідуальні права проти американської компанії, які передбачені законодавством ФРН. Він може вимагати перевірки, пред’являти свої вимоги щодо знищення, виправлення або блокування даних, компенсації завданої шкоди як проти “Німецької залізниці”, так і проти німецької чи американської дочірніх компаній банку.
7. Дочірня компанія банку в США буде сприяти проведенню аудиту на місці наглядовою інстанцією з захисту приватності ФРН чи призначеним нею агентом, у тому числі будь-якою найманою американською аудиторською або консалтинговою фірмою.

При цьому відповідний уповноважений орган з німецької сторони здійснює нагляд за виконанням цієї угоди [236]. На думку доктора права з Німеччини, А. Дікса, такий контракт витримує тест на адекватність рівня захисту, оскільки містить усі необхідні гарантії і механізми захисту приватності, як того вимагає відповідна Директива ЄС № 95/46/ЕС [237].

Ініціативи щодо подальшого розвитку договірної моделі транскордонної передачі персональних даних висувають і бізнесові міжнародні організації. У вересні 1998 року Рада Міжнародної Торгової Палати затвердила нову редакцію Модельних положень (попередня версія була розроблена у співробітництві з Радою Європи і Європейськими Співтовариствами). Перегляд Модельних положень 1993 року відбувся з огляду на зміни у діловій практиці і на нові правові вимоги, зокрема, у зв'язку із прийняттям Директиви Європейського Союзу у 1995 році. Оновлені модельні положення були підготовлені Робочою Групою з приватності і захисту даних Комісії з питань телекомунікацій і інформаційних технологій Міжнародної Торгової Палати.

Модельні положення передбачають, що експортер даних повинен мати певні повноваження і права для забезпечення додержання імпортером даних взятих зобов'язань, і вимагають від експортера даних, який має для цього більші можливості, домагатися контрактного відшкодування від його бізнес-партнерів у випадку порушення законодавства про захист приватності у країні експорту. Крім того, ці положення вимагають:

- представлення імпортером для верифікації або аудиту його технічних можливостей для обробки і зберігання інформації і надання суб'єкту даних тих самих прав стосовно експортера даних, які він мав перед тим, як дані були експортовані;
- поновлення порушених прав суб'єкта даних шляхом повернення даних, їх знищення, а також компенсації за порушення положень контракту.

У разі виникнення спору між імпортером та експортером даних стосовно будь-яких можливих порушень вказаних положень, то згідно зі статтею 5 Модельних

положень він передається Міжнародній Торговій Палаті для кінцевого вирішення на підставі Правил арбітражу.

Серед наступних розробок у галузі транскордонної передачі даних слід назвати Робочий документ "Попередній погляд на застосування договірних положень у контексті передачі персональних даних до третіх країн", прийнятий 22 квітня 1998 року Робочою Групою експертів, яка була створена на підставі статті 29 Директиви Європейського Союзу 95/46 [238].

В цьому документі, зокрема, наголошується, що оцінювати ефективність контрактної форми захисту приватності слід за такими критеріями: 1) досягнення належного рівня дотримання встановлених правил; 2) надання підтримки і допомоги суб'єктам даних у реалізації їх прав; 3) забезпечення відповідного відшкодування і поновлення прав у разі їх порушення.

З метою посилення відповідних контрактних положень щодо надання відшкодування і поновлення прав суб'єктів даних експертами Робочої групи "Статті 29 Директиви" пропонується укладення додаткової окремої угоди між відправником даних і суб'єктом даних під час одержання даних безпосередньо від суб'єкта даних про покладення на відправника відповідальності за можливі порушення прав суб'єкта даних подальшими одержувачами персоніфікованої інформації. В цьому випадку суб'єкт даних одержує від відправника відшкодування за можливі порушення одержувача, а відправник, у свою чергу, може вимагати в подальшому відповідної компенсації за збитки від одержувача персональних даних. У такий спосіб пропонується доповнити схему "B2B" новим елементом, після чого вона буде мати вигляд "C2B" – "B2B" (споживач – до бізнесу, бізнес – до бізнесу).

Така схема має право на існування, однак піддається критиці за її непрактичність через складність договірного механізму. У той же час, в деяких країнах питання транскордонної передачі персональних даних можуть вирішуватися набагато простіше. Зокрема, виконавчий член Австрійської Комісії з захисту даних, доктор права Вальтраут Котші зазначає, що на підставі цивільного законодавства Австрії можна встановити прямий зв'язок прав і обов'язків між суб'єктом даних і імпортером

на підставі односторонньої угоди (**австр**. *Auslobung)*, і це буде більш природним і логічним шляхом поширення правил захисту даних на імпортера даних [239].

Питання прямих договірних стосунків між суб'єктом даних і одержувачем в третій країні за схемою "C2B" детально розглядається Організацією Економічної Співпраці і Розвитку у документі, підготовленому Робочою Групою з питань інформаційної безпеки і приватності у вересні 2000 року за назвою "Контрактна форма транскордонного обміну даними у загальному підході до механізму захисту приватності в глобальних мережах" [240].

У цьому документі зазначається, що схема "C2B" значною мірою відрізняється від схеми "B2B". Якщо передача персональних даних між партнерами по бізнесу у багатьох випадках відбувається на постійній основі, як, скажімо, передача даних авіакомпаніями про маршрути пасажирів, то ситуація передачі персональних даних споживачем комерційній структурі частіше за все не має передісторії договірних стосунків. Це має безпосереднє відношення до контактів, які здійснюються за допомогою електронних комунікацій, зокрема, через веб-сторінки тієї чи іншої компанії.

Іншою проблемою є сам механізм укладення контракту за схемою "C2B". Якщо сторони знаходяться на території різних країн, укласти прямі контракти у традиційний спосіб є доволі складне завдання. У той же час, використовуючи електронні комунікації, це можна зробити простіше шляхом акцепту пропозиції, яка розміщена в Інтернет. При цьому, однак, існує проблема розбіжностей у законодавчому регулюванні питань укладення контрактів у різних країнах, пов'язана з неоднаковим розумінням, що саме можна вважати за пропозицію тощо. Питання врегулювання процедури укладення контрактів про транскордонну передачу даних за допомогою електронних засобів вимагає уніфікації на міжнародному рівні.

Підготовлений експертами Європейського Союзу проект "Стандартних контрактних положень для передачі персональних даних до третіх країн згідно зі статтями 26(4) Директиви 95/46/ЕС у редакції від 27 березня 2001 року передбачає додаткові гарантії для суб'єктів даних під час транскордонної передачі даних [241]. При цьому ключова роль відноситься національній наглядовій інстанції щодо

забезпечення додержання адекватного захисту персональних даних після їх передачі. Так, стаття 3 проекту вказує, що національний наглядовий орган залишає за собою право заборонити чи відкласти передачу або серію передач, якщо дійде висновку, що при цьому не забезпечується адекватний захист прав людини.

Стандартні контрактні положення повинні передбачити механізм правового захисту не тільки організацій, які є сторонами за контрактом (схема “B2B”), а й суб’єкта даних, зокрема, у випадку, якщо його буде заподіяно шкоду внаслідок порушення контракту. Для зменшення практичних проблем, з якими можуть зіткнутися суб’єкт даних під час застосування механізму захисту прав за цими контрактними положеннями, пропонується солідарна та індивідуальна відповідальність як імпортера, так і експортера даних за порушення прав суб’єкта даних. При цьому обидві сторони можуть бути звільнені від застосування санкцій, якщо доведуть, що порушення сталося не з їх вини.

За наявності спору між сторонами і суб’єктом даних, який не може бути вирішений шляхом переговорів, і при цьому задіяні положення контракту, що передбачають відповідні права суб’єкта даних, сторони домовляються надати суб’єктові даних вибір засобів правового захисту, як це передбачає стаття 7 Стандартних контрактних положень. Суб’єкт даних може на свій розсуд обирати, а сторони зобов’язані погодитися з його вибором: а) звернутися до третьої сторони для посередництва, включаючи національну наглядову інстанцію, якщо це передбачається законодавством; б) передати спір на вирішення до суду у країні, де заснований чи знаходиться експортер даних (у одній з країн Європейського Союзу). Стандартні контрактні положення передбачають, що право, застосоване до контракту, повинно бути правом країни-члена Європейського Союзу, де заснований експортер даних, надаючи цим додаткові гарантії захисту прав суб’єкта даних за контрактом.

Змішаний механізм, який поєднує саморегуляцію і договірну модель регулювання транскордонної передачі даних, знайшов своє втілення у розробленій Департаментом торгівлі США моделі, що покликана розв'язати проблему передачі персональних даних громадян Європейського Союзу до США.

Зважаючи на можливість застосування обмежень під час транскордонної передачі персональних даних громадян Європейського Союзу до Сполучених Штатів, Департаментом торгівлі США була запропонована модель за назвою “Рятувальна Гавань”.

Остаточна версія цієї моделі, яка одержала схвалення Європейської Комісії, дозволяє американським компаніям на добровільній основі приєднатися до принципів захисту приватності персональних даних, які ухвалені Департаментом торгівлі США [242].

Оскільки компанії, які виявили таке бажання, беруть на себе зобов'язання дотримуватися зазначених принципів порушення правил поводження з персональними даними громадян Європейського Союзу буде підпадати під юрисдикцію органів США, що здійснюють нагляд за комерційною практикою у відповідній галузі. Такими органами визначено Федеральну торгову комісію і Департамент транспорту США.

Розроблена модель орієнтована лише на компанії, діяльність яких підпадає під юрисдикцію цих органів. За Законом про Федеральну торгову комісію (ФТК), юрисдикція ФТК не поширюється на банки, ощадні і кредитні спілки, телекомунікації, на внутрішніх транспортних перевізників, авіаперевізників, пакувальників і операторів складів, а також на страхові компанії тих штатів, у яких існує своє регулювання їх діяльності. Юрисдикція Департаменту транспорту відповідно до підрозділу 49 Секції 41712 Кодексу Сполучених Штатів поширюється на авіаперевезення. Департамент може порушувати справи, що базуються на власних розслідуваннях, або за заявами осіб, агенцій з подорожей, авіакомпаній, урядових установ США та інших країн.

Американські компанії, які виявили згоду приєднатися до цієї моделі, включаються до загальнодоступного списку, ведення якого покладено на Департамент торгівлі США. На компанії, які здійснюють діяльність в інших секторах економіки США, дія вказаної моделі не поширюється.

Згідно з домовленістю між США і Європейським Союзом, національні компетентні органи країн-членів ЄС, маються на увазі наглядові органи у галузі

захисту приватності, мають право здійснювати свої повноваження щодо блокування передачі даних до американських компаній, які пройшли самосертифікацію і взяли зобов'язання додержуватися принципів "Рятувальної Гавані", з метою захисту прав своїх громадян у двох випадках: 1) якщо урядовий орган США (Федеральна Торгова Комісія або Департамент транспорту) встановлять факт порушення такою компанією запроваджених принципів приватності; або 2) існує значна вірогідність, що принципи будуть порушені; є підстави вважати, що механізм забезпечення не вживає адекватних і своєчасних заходів для вирішення справи; продовження передачі створить неминучий ризик завдання шкоди суб'єктові даних; і компетентний орган в країні-члені ЄС вчинив необхідні у конкретному випадку дії для повідомлення компанії і надав можливість відповісти.

Блокування транскордонної передачі повинно бути знято як тільки забезпечиться додержання принципів і зацікавлені компетентні органи в ЄС будуть поінформовані. Країна-член ЄС зобов'язана інформувати Комісію у випадках, коли органи США, відповідальні за забезпечення принципів приватності, не виконують своїх функцій. У разі підтвердження цього факту Комісія зобов'язана повідомити Департамент торгівлі США і, за необхідністю, подати у відповідності до процедури, встановленої в статті 31 Директиви ЄС, проект заходів для перегляду або припинення дії вказаної моделі регулювання транскордонних потоків даних між Європейським Союзом і США.

Передача персональних даних громадян ЄС до компаній США, які не визнали принципи "Рятувальної Гавані", все ж таки залишається можливою, однак лише у випадках, які передбачені в частині першій статті 26 Директиви ЄС. Слід зазначити, що запропонована модель розроблена виключно для передачі персональних даних громадян Європейського Союзу до США, розрахована саме на особливості національного регулювання окремих секторів економіки США, а тому не може бути автоматично застосована до інших країн, які не надають адекватного рівня захисту права людини на приватність.

Висновки до розділу 2

Аналіз чинних міжнародно-правових стандартів та законодавства Європейського Союзу у галузі захисту права на приватність персоніфікованої інформації, а також вивчення правових проблем забезпечення транскордонної передачі персоніфікованої інформації між країнами з різним рівнем правового захисту дозволяє зробити підсумок проведеного у другому розділі дослідження у формі наступних висновків:

Міжнародно-правові стандарти, що втілені в Конвенції Ради Європи "Про захист осіб стосовно автоматизованої обробки персональних даних" 1981 року і Директиві № 95/46 СЕ Європейського Парламенту і Ради "Про захист фізичних осіб стосовно автоматизованої обробки персональних даних та безперешкодного руху цих даних" 1995 року, відбивають загальноєвропейський, соціально-захисний підхід до регулювання обробки і транскордонної передачі персональних даних. "Керівні принципи, що регулюють захист приватності і транскордонні потоки персональних даних" Організації Економічного Співробітництва і Розвитку 1980 року, а також "Керівні принципи стосовно комп'ютеризованих файлів персональних даних" ООН 1990 року виникли внаслідок досягнення міжнародного консенсусу між країнами з різними правовими традиціями і базуються на ліберальному, орієнтованому на ринкові відносини підході до регулювання захисту приватності.

Країни Європейського Союзу гармонізують своє законодавство у галузі використання персоніфікованої інформації в правоохоронній діяльності на основі принципів, закладених у Директиві ЄС 95/46, а також Конвенції Ради Європи № 108 і Рекомендації Комітету Міністрів Ради Європи № R (87)15. Інкорпорація зазначених принципів у Шенгенську Конвенцію і Конвенцію Європол позитивно

вплинула на врегулювання питань обробки персональних даних у правоохоронній діяльності на європейському рівні.

Договірна модель визнається в теорії і на практиці як один з можливих засобів поширення дії національного адекватного (еквівалентного) захисту приватності на відносини з передачі персональних даних до третіх країн. Правові питання укладення таких договорів ще не врегульовані належним чином; а тому відмічається наявність розбіжностей у підходах на національному і міжнародному рівнях. Модель забезпечення безперешкодної передачі даних між країнами з різним рівнем захисту персоніфікованої інформації під назвою “Рятувальна Гавань”, яка ґрунтується на домовленості між Європейським Союзом і Сполученими Штатами, має обмежений характер, оскільки поширюється лише на окремі сегменти приватного сектора економіки США і пристосована до особливостей національного механізму публічно-правового нагляду за комерційною практикою.

РОЗДІЛ 3
МІЖНАРОДНІ СТАНДАРТИ ЗАХИСТУ ПРАВА НА ПРИВАТНІСТЬ ПЕРСОНІФІКОВАНОЇ ІНФОРМАЦІЇ І НАЦІОНАЛЬНЕ ЗАКОНОДАВСТВО

Розглянуті у попередньому розділі питання уніфікації міжнародно-правового регулювання обробки та транскордонної передачі персоніфікованої інформації викликані здебільше розбіжностями у національних правових системах. Без вивчення особливостей законодавства і досвіду окремих країн, позиція яких на міжнародній арені є ключовою, вкрай ускладнюється розуміння сучасних проблем міжнародно-правового захисту права на приватність персоніфікованої інформації. Безперечно, цікавим є цей досвід для нашої держави, оскільки перед Україною тільки постає питання про вибір тієї чи іншої регулятивної моделі для упровадження міжнародно-правових стандартів захисту права на приватність персоніфікованої інформації у національне законодавство.

Це питання постає надзвичайно актуально з огляду на необхідність проведення реформи національного законодавства України не тільки для забезпечення прав і свобод людини, приведення його у відповідність до міжнародних, зокрема, європейських стандартів, а й для досягнення відповідності приписів національного законодавства положенням законодавства Європейського Союзу з врахуванням національної правової практики держав-членів ЄС.

У цьому розділі досліджуються особливості національних регулятивних підходів окремих країн Європи, Сполучених Штатів Америки та інших демократичних держав, які мають розвинуте законодавство і багаторічний досвід захисту права на приватність персоніфікованої інформації (підрозділ 3.1); аналізується стан розвитку законодавства України у цій сфері (підрозділ 3.2), а також вивчаються можливі шляхи його удосконалення з метою наближення до міжнародних, зокрема, європейських стандартів у цій сфері (підрозділ 3.3).

3.1. Національно-правові моделі захисту приватності персоніфікованої інформації

Національні правові традиції, а також особливості способів правового регулювання зумовили формування різних моделей захисту приватності персоніфікованої інформації в національних правових системах різних країн. Найбільш поширеною у світі є модель базового регулювання, згідно з якою в країні приймається один чи декілька основних нормативних актів, які створюють відповідний правовий механізм захисту приватності персональних даних. Ключовим елементом регуляторної моделі країн Західної і Центральної Європи, Австралії, Нової Зеландії, Гонконгу і Канади є наглядовий орган з захисту даних. На нього покладається низка повноважень щодо виконання наглядової, охоронної і регулятивної функцій у цій галузі.

Наглядова інстанція з питань захисту приватності персональних даних наявна у національних правових системах більшості розвинутих країн світу. Для дослідження компетенції і повноважень наглядового органу доцільно розглянути процес його становлення і розвитку в деяких європейських країнах. Наглядовий орган з'явився разом з появою перших правил поводження з персональними даними. Його повноваження зазнавали змін, відображаючи еволюцію законодавчого регулювання цього питання.

Перші закони, серед яких закон Землі Гессен (ФРН) 1970 року [243], Землі Райнланд-Фальц (ФРН) 1974 року [244], Шведський закон 1973 року [245], були спрямовані на адміністрування баз даних у деяких публічних секторах і здебільшого регулювали лише організаційні та технічні питання. Суб'єкту даних надається лише право доступу і виправлення даних, якщо вони були неточними. Роль наглядового органу зводилася до реєстрації баз даних і загального нагляду за дотриманням правил і процедур обробки даних органами державної влади і публічними організаціями.

У своєму ґрунтовному досліджені розвитку законодавчого регулювання обробки персоніфікованої інформації в європейських країнах Майор-Шонбергер простежує тенденцію поширення технократичного підходу в першому поколінні нормативних актів [39]. Ця особливість перших нормативних актів являється і в термінології, яка в них використовується. Зокрема, в них відсутні такі терміни як «приватність», «інформація» чи «захист приватного життя»; натомість застосовуються технічні терміни – «дані», «банк даних», «файл даних» тощо.

Розширення прав осіб, яких стосуються дані, у законах Франції [246], Австрії [247], Данії [248] і Норвегії [249], прийнятих 1978 року, та впровадження права індивіда визначати, які дані і з якою метою можуть використовуватися, додали кілька важливих контрольних повноважень наглядовій інстанції. Перш за все, це стосується права вимагати від державних органів дотримання правил захисту даних і ліквідації допущених порушень.

Подальший розвиток національних положень знаменується доповненням прав суб'єкта даних правом на «інформаційне самовизначення». Під цим розуміється право людини контролювати поводження з персональними даними на всіх стадіях обробки, починаючи від збору й кінчаючи знищенням.

Ця доктрина вперше була сформульована у 1983 році Федеративним Конституційним судом ФРН, який зазначив, що свобода особи планувати і здійснювати свої вчинки значною мірою обмежується, якщо вона не має достатньої впевненості у тому, яку персоніфіковану інформацію мають у своєму розпорядженні її співбесідники. А тому для захисту прав осіб необхідно їй надати повноваження визначати, яким чином персональні дані розкриваються і використовуються [250].

Доктрина права на інформаційне самовизначення була впроваджена у Федеративному законі ФРН про захист даних у 1990 році [251], Законі Фінляндії про реєстрацію громадян у 1987 році [252]. На цьому етапі повноваження наглядового органу зазнають суттєвих змін. Зокрема, на нього покладається охоронна функція, яка реалізується ним через повноваження звертатися до судових органів для захисту порушених прав людини стосовно її персональних даних. Він стає більш схожим на традиційного уповноваженого з прав людини. Не випадково, що найбільш

поширеними назвами цієї інституції стають “Уповноважений з питань захисту приватності” чи “Уповноважений із захисту даних”.

З огляду на те, що права особи стосовно поводження з її даними не є абсолютними чи виключними та що існують інші інтереси, які мають бути враховані в інтересах суспільства, перед Уповноваженим постає складне завдання балансування між інтересами суб'єкта даних і публічними інтересами. Необхідність встановлення справедливого балансу між такими конкуруючими правами, як право на приватність і право на свободу інформації, є, зокрема, однією з причин, яка зумовила покладання на Уповноваженого із захисту даних Канади і Угорщини функції нагляду за дотриманням права на вільний доступ до інформації, що становить публічний інтерес.

Принцип балансування між інтересами особи та публічними інтересами є одним із ключових у діяльності наглядового органу. Складність вирішення цього питання у комплексі і динаміці обставин була сформульована Реєстратором із захисту даних Великої Британії, який відзначив, що точка балансу є різною для різних індивідів, чиї законні інтереси зважуються у конкретних обставинах [253]

Відомий спеціаліст у цій галузі, професор Единбурзького університету Ч. Рааб, досліджуючи тенденції розвитку інституту наглядової інстанції, запропонував концепцію «ручного управління» (**англ**. *steering*) у галузі захисту приватності персональних даних. Згідно з нею, подальший розвиток інституту наглядової інстанції має відбуватися у напрямку надання йому більших повноважень для ручного управління балансом між інтересами особи і публічними інтересами відповідно до обставин конкретної справи [254].

Серед чинників, які мають бути враховані під час встановлення такого балансу, сучасне покоління нормативних актів із захисту приватності персональних даних визнає потенційну шкоду для суб'єкта даних від обробки певної категорії «вразливих» даних. Згідно з Декретом про вразливі дані 1993 року, в Нідерландах встановлено детальні вимоги стосовно правил поводження з кожним окремим видом «вразливих» даних, які стосуються релігійних чи філософських переконань (ст. 2), расового походження (ст. 3), політичних поглядів (ст. 4), інтимних аспектів

приватного життя і стану здоров'я (ст. 5), кримінальних вчинків (ст. 6), адміністративних порушень (ст. 7) тощо.

Для врахування особливостей секторів, у яких запроваджується регулювання операцій з даними, наглядовий орган деяких країн наділяється регулятивною функцією. На нього покладаються повноваження щодо затвердження відповідних кодексів «чесної інформаційної практики», сертифікації запропонованих ними правил на їх відповідність до вимог національного законодавства про захист приватності персональних даних. Зокрема, Комісія із захисту даних Нідерландів може декларувати, що правила, які містяться у такому кодексі, належним чином впроваджують правові положення щодо обробки персональних даних.

Уповноважений Гонконгу, наприклад, відповідно до положень Закону Гонконгу "Про захист даних" 1995 року ухвалив два Кодекси: «Про практику стосовно номерів посвідчення особи» (1997 р.) і «Про дані стосовно кредитоспроможності споживачів» (1998 р.).

Крім того, більшість національних положень надають наглядовому органу право у той чи інший спосіб впливати на процес підготовки регулятивних актів шляхом подання пропозиції або зауважень стосовно проектів нормативних актів.

Важливість існування дієвого наглядового органу в механізмі захисту приватності персоніфікованої інформації зумовила вироблення відповідних пропозицій щодо доповнення Конвенції Ради Європи про захист осіб стосовно автоматизованої обробки персональних даних 1981 року положеннями про таку інституцію. На 16-й нараді Консультативного Комітету Конвенції, що відбувалася з 6 по 8 липня 2000 року у Страсбурзі, був ухвалений проект додаткового протоколу до Конвенції. Протокол містить положення, що вимагають від держав-учасниць Конвенції впровадження наглядового органу з питань захисту приватності персональних даних і надання йому необхідних повноважень для виконання наглядової й охоронної функцій. Зокрема, друга частина статті 1 проекту додаткового протоколу встановлює, що вказаний орган повинен мати, крім інших, повноваження щодо розслідування і втручання, а також повноваження вступати у юридичний процес або подавати на розгляд судовій владі порушення положень національного законодавства [255].

У деяких європейських країнах створено спеціальну інстанцію для розгляду такої категорії справ. За Законом Швейцарії 1992 року [256] на Федерального Уповноваженого із захисту даних покладаються функції ведення реєстру баз даних, нагляду за дотриманням правил поводження з даними, захисту прав суб'єктів даних. У разі встановлення порушень він ухвалює відповідні рекомендації. Однак у разі їх невиконання Уповноважений може звернутися до Федеральної Комісії з захисту персональних даних, яка виносить рішення, що має силу судового. Крім того, Федеральна Комісія розглядає апеляції на рішення органів влади федерації і кантонів у галузі захисту приватності персональних даних.

Уповноважений із захисту даних Фінляндії за законом 1987 року здійснює контроль за дотриманням правил поводження з персональними даними і розслідування за заявами осіб. А колегія із захисту даних Фінляндії вирішує суперечки і має право визначати, коли персональні дані можуть передаватися за кордон країни.

Наглядовий орган з питань захисту приватності персональних даних для ефективного виконання своїх функцій має діяти цілком незалежно. Цей принцип закріплений у більшості європейських законів із захисту персональних даних. Він проголошується і в проекті додаткового протоколу до Конвенції Ради Європи про захист осіб стосовно автоматизованої обробки персональних даних. Так само визнаним є й принцип підконтрольності наглядового органу судовій владі. Зокрема, частина четверта вказаного протоколу передбачає, що рішення наглядового органу, які призвели до подання скарг, можуть бути оскаржені до суду.

Для сучасного стану моделі базового (статутного) регулювання принциповим є поширення як правил правового захисту приватності персоніфікованої інформації, так і наглядових повноважень не тільки на публічні, але й рівною мірою на приватноправові відносини. Це є яскравим прикладом нормативного відтворення поширеної в Європі доктрини горизонтальної дії конституційних норм з прав людини у відносинах між приватними особами *(***нім**. *Drittwirkung).*

Інший підхід до законодавчого регулювання питань поводження з даними був обраний Сполученими Штатами Америки, які уникали ухвалення загального закону

із захисту даних, поширюючи відповідні правила лише на певні сектори. Так званий, ліберальний підхід, оснований на концепції невтручання держави у відносини між приватними особами, обумовлює особливості національного режиму захисту приватності персональних даних у приватному секторі США та інших країн. Як відмічає американський правозахисник, професор Марк Ротенберг, Закони США з захисту даних, як правило виникали як реакція на питання, що залишалися неврегульованими судовими прецедентами чи як спроба кодифікувати правові стандарти для їх застосування під час комерційних операцій з використанням нових технологій [257].

До першої категорії можна віднести такі закони: “Про право на фінансову приватність” (захист приватності інформації фінансового характеру) 1978 року [258], “Про захист приватності” (захист від неправомірного збору інформації під час обшуку і виїмки) 1980 року [259] і певною мірою “Про приватність електронних комунікацій” (захист від несанкціонованого зняття інформації з каналів зв'язку) 1986 року [260]. Ці закони були прийнятті внаслідок того, що Верховний Суд Сполучених Штатів у своїй практиці не визнав відповідні права на приватність.

До другої категорії відносяться такі закони: “Про приватність” (право на доступ до персональних даних у публічних реєстрах) 1974 року [261], “Про захист приватності під час відео-зйомки” (захист від стеження) 1988 року [262], “Про захист споживачів телефонних послуг” 1991 року [263]. Перелічені закони з'явилися з упровадженням нових технологій, які викликали відповідну зацікавленість громадськості у захисті приватності.

Забезпечення додержання правил поводження з даними за цією моделлю покладається на низку органів, серед яких суди, прокуратура, Федеральна торгова комісія, Департамент транспорту та інші органи, які здійснюють загальний нагляд за виконанням умов ліцензій на певні види діяльності тощо.

За цим підходом виникає проблема у разі появи нової технології, яка вимагає окремого законодавчого регулювання питань захисту приватності. Наприклад, у США відсутній закон про захист приватності генетичних даних. Унаслідок такої

правової прогалини на цю категорію персональних медичних даних не поширюється режим приватності.

Крім того, галузева юрисдикція наглядових органів у США дозволяє порушникам права на приватність в певних випадках уникати відповідальності. Так, юрисдикція Федеральної торгової комісії в цьому питанні поширюється на нечесну чи обманну діяльність або практику лише тоді, коли вони здійснюються на комерційній основі або впливають на комерцію. З іншого боку, якщо особи чи організації неправомірно збирають інформацію без комерційної мети, це виходить за межі юрисдикції Федеральної торгової комісії.

До того ж, нечесною визнається практика, яка може заподіяти чи заподіяла значну шкоду споживачам, якщо її не можна уникнути і вона не переважується користю від цього для споживачів або конкуренції (§45, Секція 5 Закону США "Про Федеральну торгову комісію") [264]. Однак поширеною, зокрема, серед постачальників інформаційного продукту, є практика надання споживачам безоплатного товару в обмін на повідомлення персональних даних. В таких випадках, за законодавством США, відповідальність настає лише у разі обману покупців, які надали інформацію про себе, а взамін нічого не отримали.

Під час розгляду однієї з таких справ у 1999 році Федеральна торгова комісія встановила таке порушення з боку компанії "Ліберті Файненшл Компаніс". Ця компанія через свою веб-сторінку, яка була орієнтована на дитячу і юнацьку аудиторію, пропонувала відвідувачам надати персональну інформацію про фінансовий стан їх родини в обмін на безоплатну розсилку фінансових новин. Компанія також обіцяла, що повідомлені дані будуть триматися в анонімній формі. Насправді персональні дані зберігалися у формі, що дозволяла ідентифікувати суб'єктів даних, а фінансові новини так і не надходили до передплатників.

Федеральна торгова комісія заборонила компанії вдаватися до таких дій у майбутньому і наказала розмістити на веб-сторінці повідомлення про практику щодо персональних даних, які збираються компанією, а також зобов'язала одержувати попередню згоду батьків на збір інформації від дітей [265].

За європейською моделлю, галузевий підхід не замінює, а доповнює базове законодавство з захисту даних. Крім того, з метою сприяння правильному застосуванню загальних положень, враховуючи галузеві особливості, європейські стандарти передбачають можливість створення професійними організаціями чи іншими представницькими органами кодексів поведінки стосовно поводження з персональними даними.

Теоретично механізм саморегуляції може забезпечити прийнятний рівень захисту приватності персональних даних. За цією моделлю, споживачеві певної послуги дається право вибирати серед постачальників, зважаючи на запропонований ними рівень захисту приватності. За ідеальних умов умов рівності всіх учасників ринку певної послуги конкурентні переваги буде мати той постачальник, який пропонує найбільш оптимальний для споживачів рівень захисту. А отже, це повинно спонукати постачальників приєднуватися до галузевих кодексів "чесної інформаційної практики".

Передача персоніфікованої інформації від споживача до постачальника послуг, який знаходиться в іншій країні, несе ризик втрати контролю за операціями з персональними даними, оскільки фактично дуже складно проконтролювати додержання постачальником правил, встановлених у контракті або у внутрішніх правилах захисту приватності, які демонструє постачальник споживачам через свою веб-сторінку. В електронному середовищі доволі поширеними стали схеми сертифікації дотримання компаніями проголошеної корпоративної політики щодо поводження з персональними даними у формі маркування чи поставлення сертифікаційних печаток, ярликів на веб-сторінках постачальників, які мають посвідчувати факт дотримання ними зобов’язань про захист приватності.

Слід відзначити такі системи посвідчення приватності, які покликані запропонувати нові можливості для посилення захисту приватності в електронному середовищі: “Електронна печатка кращої ділової практики щодо приватності”, “Електронна Довіра” і “Японська Система маркування захисту приватності”. Відповідні позначення сертифікації даються за результатами проведення аудиту додержання запропонованих стандартів захисту приватності в електронному

середовищі. Така сертифікація є одним із способів саморегуляції приватного сектора шляхом встановлення галузевих стандартів і забезпечення їх додержання за допомогою як фінансових санкцій, так і позбавлення статусу сертифікованого постачальника зняттям позначки про сертифікацію з його веб-сторінки.

Модель саморегуляції, однак, не може розглядатися як альтернативна до законодавчого регулювання. Низький рівень захисту і неможливість забезпечення проголошених професійних стандартів є слабкими місцями цієї регулятивної моделі. У документі, який був підготовлений Робочою Групою статті 29 Директиви ЄС 95/46 ЕС за назвою "Судячи індустріальну саморегуляцію", експерти ЄС дійшли висновку, що інструмент саморегуляції може розглядатися як дієва складова "адекватного захисту" за умов, що він буде: обов'язковим до виконання для всіх членів, яким дані передаються, і забезпечувати адекватні гарантії у разі передачі даних не членам; прозорим і містити основний зміст принципів захисту даних; мати механізм для забезпечення достатнього рівня його додержання в цілому через систему превентивних санкцій і покарання, а також обов'язковий безсторонній аудит; надавати підтримку і допомогу суб'єктам даних, які зіткнулися з проблемами; мати легкодоступний, неупереджений і незалежний орган для розгляду заяв суб'єктів даних і прийняття рішень у разі порушень кодексу; гарантувати у випадках його порушення відповідну компенсацію для суб'єкта даних [266].

Зрозуміло, що забезпечити виконання цих вимог лише інструментами саморегуляції проблематично. Разом з тим, у поєднані з механізмом державного регулювання така модель має право на існування.

Слід відзначити, що європейські стандарти захисту приватності, які базуються на соціально-захисному підході, одержують все більше визнання у світі, що можна спостерігати на прикладі таких традиційно ліберально-ринкових країн як Канада і Австралія.

Чинне федеральне законодавство Канади про захист приватності у публічному секторі діє з 1983 року. Закон Канади “Про персональну інформацію і електронні документи”, що набрав чинності 13 квітня 2000 року, поширюється на організації приватного сектора, які збирають, використовують і поширюють персональну

інформацію під час комерційної діяльності. Він вступає в дію у три етапи: 1) з 1 січня 2001 року Закон застосовується до будь-якої організації, яка здійснює діяльність за федеральним законодавством у секторах авіаперевезень, банківської справи, телебачення, радіомовлення, між-провінційних перевезень і телекомунікації, а також до будь-яких організацій, які передають дані за межі провінції чи Канади; 2) з 1 січня 2002 року – до медичної персоніфікованої інформації, яка обробляється задіяними на першому етапі організаціями; 3) з 1 січня 2004 року – до всіх організацій, які збирають, використовують і поширюють персональну інформацію під час комерційної діяльності на території провінції, незалежно від того, поширюється на таку організацію федеральний статус чи ні [267].

Однак, на думку експертів Робочої Групи Європейського Союзу, законодавство Канади все ж таки ще не надає адекватного рівня захисту, оскільки має прогалини, зокрема, не поширюється на неприбуткові організації, не передбачає спеціальних гарантій щодо обробки вразливих даних і передачі даних до третіх країн [268].

Австралія ухвалила федеральний закон про захист приватності у 1998 році. Закон встановлює детальні “Принципи Інформаційної Приватності”, які ґрунтуються на Керівних принципах ОЕСР 1980 року. Законом, що набрав чинності 21 грудня 2000 року, внесені зміни до закону 1998 року, розраховані на їх застосування до організацій приватного сектора. Він вступає в дію з 21 грудня 2001 року. Закон впроваджує так звані “Національні Принципи Приватності”, які базуються на принципах, розроблених Федеральним Комісаром з приватності у 1998 році і узгоджених з позицією представників приватного сектора економіки Австралії [269].

Подібно до канадського, законодавство Австралії не містить заборону на обробку вразливих даних, не передбачає правил щодо обробки даних у цілях “прямого продажу” товарів і послуг, що відзначається у висновку Робочої Групи ЄС [270].

Отже, можна стверджувати, що переважає тенденція поширення європейського, соціально-захисного підходу регулювання обробки персоніфікованої інформації до країн, які є традиційно ліберальними у їх ставленні до відносин між публічним і приватним секторами. Це ще раз доводить необхідність вибору саме європейської моделі захисту права на приватність для упровадження в України.

3.2. Правове забезпечення реалізації і захисту права на приватність в законодавстві Україні

У цьому підрозділі аналізується чинне законодавство України з точки зору відповідності європейським стандартам у галузі захисту приватності і безперешкодності транскордонної передачі персоніфікованої інформації, а також досліджується найбільш оптимальний шлях для втілення європейських мінімальних стандартів у правову систему нашої держави з метою забезпечення адекватного, у європейському розумінні, рівня правового захисту приватності персоніфікованої інформації.

Досвід пострадянських країн показує, що реформування інформаційних відносин є вирішальним завданням, які вони мають виконати, ставши на шлях демократії. У зв'язку з цим актуальним є не лише питання запровадження нових регулятивних моделей, а й проблема докорінної зміни свідомості громадян. Упродовж тривалого часу, з покоління в покоління, вона була під впливом пропаганди ідеї "зовнішніх і внутрішніх ворогів", від яких треба було оберігати "святині", до яких належала також державна таємниця. При цьому, більшість громадян не мала уявлення, що саме підпадає під цю категорію. А тому утаємничувалась мало не вся інформація, пов'язана з діяльністю органів державної влади, недотримання чого загрожувало звинуваченням у державній зраді.

Західна ідея приватного життя як певної автономії людини у суспільстві ("мій дім – моя фортеця"), зовсім по-іншому сприймається людьми, свідомість яких зазнала впливу ідеології тоталітарного режиму за часів Радянського Союзу. Оскільки приватна власність вважалася "злом", яке треба викорчувати із суспільних відносин і свідомості громадян, то для прийняття ідеї приватного життя не було ґрунту у радянському суспільстві. Не випадково, що термін "приватне життя", який сприймався як антитеза "громадському життю", був підмінений у законодавстві

терміном “особисте життя”, що значною мірою звузило нормативне наповнення права на приватність.

Концепція засекречування була поширена й на інформацію про громадян, що збиралася органами державної влади, у тому числі й органами безпеки, яка часто використовувалась як підстава для застосування репресій. Зрозуміло, що про доступ до цієї інформації не можна було й мріяти, оскільки вона належала державі як і сама людина.

Як уже зазначалося, Конституція України визнає за правом на приватність статус конституційного права людини. Слід визнати, що право на приватність зазнало певного розвитку у вітчизняному конституційному праві. Стаття 32 Конституції України, яка проголошує право на приватність, набагато змістовніша порівняно зі статтею 54 Конституції Української Радянської Соціалістичної Республіки 1978 року. За редакцією Статті 54 Конституції УРСР, право на приватність несло у собі лише “негативний” правовий припис, – забороняло втручання в особисте життя громадян:

“Особисте життя громадян, таємниця листування, телефонних розмов і телеграфних повідомлень охороняються законом” [271, *319*].

Слід відзначити, що використане формулювання майже тотожне за змістом статті 31 чинної Конституції України, яка гарантує таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції, охороняючи комунікаційну приватність (Див. стор. 18-19 дисертації). Право на приватність за редакцією Статті 32 чинної Конституції України доповнено позитивними правами, що надає додаткові гарантії для ефективного захисту права на приватність:

“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.

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" [272].

Як видно з тексту статті 32, право на приватність персоніфікованої інформації знайшло своє закріплення в Конституції України в переліку певних прав. З одного боку, ці права захищають конфіденційність або, іншими словами, обмежують доступ до такої інформації, а з іншого, – надають особі право на доступ до власної персоніфікованої інформації, що знаходиться у розпорядженні органів влади, установах і організаціях, право спростовувати недостовірну інформацію і вимагати її вилучення.

Основні закони третьої та четвертої хвиль світової конституційної нормотворчості, а саме так називають конституції нових держав Європи та Азії, у своїй більшості закріплюють право людини на доступ до персоніфікованої інформації в окремих статтях конституцій, відокремлюючи його від права на недоторканність приватного життя. Як правило, в текстах конституцій статті, що проголошують недоторканність приватного життя, передують статтям, що присвячені праву на доступ до персоніфікованої інформації. Зокрема, ці права закріплені у статтях 26 і 44 Конституції Естонської Республіки 1992 року, статтях 22 і 25 Конституції Литовської Республіки 1992 року, статтях 28 і 34 Конституції Республіки Білорусь 1994 року, статтях 32 і 41 Конституції Республіки Болгарія 1991 року, статтях 28 і 34 Конституції Республіки Молдова 1994 року, статтях 23 і 24 Конституції Російської Федерації 1993 року. Причому, право на доступ до персоніфікованої інформації розглядається як складова загального права на доступ до інформації, тобто в цих же статтях проголошується і право на доступ до публічної інформації [273].

Інший підхід у конституційному закріпленні права на доступ до персоніфікованої інформації було обрано Республікою Угорщина й Україною. Це право закріплено як складова частина права на захист недоторканності приватного життя в статі 59 Конституції Угорщини й статті 32 Конституції України. До речі, цей підхід відповідає

позиції, яку обрав Європейський Суд з прав людини під час розгляду справи “Гаскін проти Сполученого Королівства”. Погоджуючись з висновком Європейської Комісії з прав людини, у рішенні, датованому 7 липня 1989 року, Суд відзначив, що інтерес позивача в отриманні дозволу на доступ до інформації, якою володіє місцева влада, про його перебування у державному дитячому виховному закладі торкається аспектів особистого і сімейного життя, а не загального інтересу в доступі до інформації, що знаходиться у розпорядженні публічної влади, а тому відсутність доступу до такої інформації порушує статтю 8 Європейської Конвенції про захист прав людини і основних свобод [274].

В статті 32 Конституції України передбачається можливість обмежування права на приватність персоніфікованої інформації, адже воно не є абсолютним або виключним. Тому будь-яке обмеження права на приватність, у тому числі і з метою захисту свободи слова, розглядається з точки зору дотримання певних вимог, вироблених у практиці європейських конвенційних органів – Європейської Комісії і Суду з прав людини. Такі обмеження права на приватність повинні відповідати наступним вимогам: 1) запроваджуватися на підставі закону, 2) мати легітимну ціль, 3) бути необхідними у демократичному суспільстві.

Цей принцип визнається і творцями Європейської Конвенції про захист прав людини і основних свобод. Між тим, перелік можливих обмежень права на приватність персоніфікованої інформації за Конституцією України менший, ніж у Конвенції.

Стаття 8 Конвенції вказує на такі інтереси, що конкурують із правом особи на приватність:

- інтереси національної та громадської безпеки;
- економічного добробуту країни;
- запобігання заворушенням і злочинам;
- захисту здоров’я або моралі;
- захисту прав і свобод інших людей.

Стаття 32 Конституції України вказує лише на інтереси національної безпеки, економічного добробуту та прав людини як можливу підставу для обмеження права

на приватність персоніфікованої інформації. Поясненням цьому може бути той факт, що право на повагу до приватного життя, як ширше за правовим змістом, цілком закономірно може зазнавати більших обмежень, ніж право на приватність персоніфікованої інформації.

Це підтверджується, зокрема, положеннями спеціальних міжнародно-правових документів, присвячених захисту права на приватність персоніфікованої інформації. Стаття 9 вищевказаної Конвенції Ради Європи 1981 року № 108 передбачає, що відступ від положень, що гарантують права суб'єкта даних, дозволяється в інтересах державної безпеки та громадського спокою, грошових інтересів держави або для боротьби із кримінальними злочинами та для захисту прав і свобод інших осіб. А стаття 13 Директиви ЄС № 95/46/ЕС 1995 року передбачає, що обмеження можуть застосовуватися, якщо це є необхідним заходом для забезпечення: державної безпеки, оборони, громадського порядку, в інтересах слідства, важливого економічного або фінансового інтересу, захисту суб'єкта даних або прав і свобод інших осіб. Як видно, цьому переліку обмежень майже тотожні за змістом відповідні положення статті 32 Конституції України.

Поряд із цими позитивними зрушеннями на конституційно-правовому рівні залишається низка недоліків у визначені правового режиму персоніфікованої інформації в законах та підзаконних актах нашої держави. За відсутності правової традиції захисту прав людини стосовно відомостей про особу і взагалі правового терміну для позначення режиму регулювання відносин, пов'язаних з персоніфікованою інформацією, законодавчі акти України з інформаційних питань визначають її правовий режим досить розпливчасто. До того ж, чинному законодавству бракує термінологічної узгодженості, що створює складнощі під час реалізації відповідних правових норм на практиці.

Досить прогресивний на час свого прийняття, а це всього рік потому після проголошення Україною незалежності, Закон України "Про інформацію" 1992 року містить низку положень, присвячених захисту персоніфікованої інформації, яка визначається у ньому як "інформація про особу" [275]. Так, стаття 23 Закону витлумачує поняття "інформація про особу" як сукупність документованих або

публічно оголошених відомостей про особу. Основними даними про особу (персональними даними) визначено: національність, освіта, сімейний стан, релігійність, стан здоров'я, а також адреса, дата і місце народження. Джерелами документованих відомостей про особу Закон визнає видані на її ім'я документи, підписані нею документи, а також відомості про особу, зібрані державними органами влади та органами місцевого і регіонального самоврядування в межах своїх повноважень.

Стаття 31 вказаного Закону гарантує громадянам доступ до інформації про них шляхом визначення обов'язку державних органів і організацій, органів місцевого і регіонального самоврядування надавати її безперешкодно і безкоштовно на вимогу осіб, яких вона стосується, а також гарантує право на оскарження у суді відмови у доступі до такої інформації, приховуванні її, незаконному збирані, використанні, зберіганні чи поширенні.

Закон України "Про інформацію" закріпив принцип розрізнення інформації за ступенем відкритості доступу до неї громадськості. Згідно зі статтею 28 Закону режим доступу до інформації – це передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації. Відповідно до режиму доступу, Закон диференціює відкриту інформацію та ту, що має обмежений доступ. Інформація з обмеженим доступом, у свою чергу, поділяється на конфіденційну і таємну. Конфіденційна – це така інформація, яка є у *володінні* фізичних і юридичних осіб і поширюється ними на власний розсуд. До таємної інформації відноситься державна та інша таємниця, яка охороняється законом.

Тобто визначальним для класифікації інформації за режимом доступу було застосовано критерій належності інформації тому чи іншому суб'єкту на праві власності. Це створило проблему щодо визначення правового режиму персоніфікованої інформації, оскільки право людини на приватність є немайновим правом. Саме тому, у цьому Законі не було визначено, до якої категорії слід відносити інформацію про особу, конфіденційної чи таємної. Не випадково Закон України "Про інформацію" серед видів таємниці, яка охороняється законами, називає: таємницю усиновлення (удочеріння), таємницю кореспонденції, лікарську таємницю,

таємницю грошових вкладів і прибутків від підприємницької діяльності – тобто, відносить до таємних окремі категорії відомостей про фізичних осіб.

У чинному законодавстві України не дається чіткого визначення персоніфікованої інформації і правового режиму її використання. Зокрема, Законом України "Про свободу совісті та релігійні організації" захищається таємниця сповіді [276]. Закон України "Про адвокатуру" захищає адвокатську таємницю – питання, з яких громадянин або юридична особа зверталися до адвоката, суть консультацій, порад, роз'яснень та інших відомостей, одержаних адвокатом при здійсненні своїх професійних обов'язків (ст. 9) [277].

Законом України "Про захист інформації в автоматизованих системах" захищається інформація в автоматизованих системах, тобто сукупність усіх даних і програм, які використовуються в автоматизованих системах незалежно від засобу їх фізичного та логічного представлення [278].

Закон України "Про оперативно-розшукову діяльність" забороняє передавати і розголошувати відомості, що можуть зашкодити слідству або інтересам людини (ч. 10 ст. 9), а також зобов'язує правоохоронні органи знищувати отримані в результаті оперативно-розшукової діяльності відомості, що стосуються особистого життя, честі і гідності людини, якщо вони не містять інформації про вчинення заборонених законом дій (ч. 12 ст. 9) [279]. А Закон України "Про розвідувальні органи України" у статті 5 визначає, що не підлягає розголошенню інформація, що стосується особистого життя, честі та гідності громадян, яка стала відома розвідувальним органам у процесі їх роботи, крім випадків, передбачених законом [280].

Стаття 8 Закону України "Про рекламу" забороняє вміщувати зображення фізичної особи або використовувати її ім'я без згоди останньої [281].

Закон України "Основи законодавства України про охорону здоров'я" гарантує захист лікарської таємниці, забороняючи медичним працівникам та іншим особам, яким у зв'язку з виконанням професійних або службових обов'язків стало відомо про хворобу, медичне обстеження, огляд та їх результати, інтимну і сімейну сторони життя громадянина, розголошувати ці відомості, крім передбачених законодавчими актами випадків. У разі використання інформації, що становить лікарську таємницю,

в навчальному процесі, науково-дослідній роботі, у тому числі у випадках її публікації у спеціальній літературі, повинна бути забезпечена анонімність пацієнта [282]. У новому Цивільному кодексі України, який набрав чинності з 1 січня 2004 року, право на приватність медичних даних конкретизується у двох статтях, які гарантують право доступу пацієнта до власних медичних даних, а також таємницю цих даних для сторонніх осіб. Так, стаття 285 і гарантує повнолітній фізичній особі право на достовірну і повну інформацію про стан свого здоров'я, у тому числі на ознайомлення з відповідними медичними документами, що стосуються її здоров'я. А стаття 286 надає фізичній особі право на таємницю про стан свого здоров'я, факт звернення за медичною допомогою, діагноз, а також про відомості, одержані при її медичному обстеженні.

Слід відзначити, що запропоноване Цивільним кодексом розгалуження і конкретизації особистих немайнових прав фізичної особи, зокрема, тих, що стосуються приватної сфери життя людини, як-то, право на ім'я, його зміну та використання (статті 294-296), право на повагу до гідності та честі (стаття 297), ділової репутації (стаття 298), право на індивідуальність (стаття 300), на особисте життя та його таємницю (301), на таємницю кореспонденції (стаття 306), - безперечно, позитивно вплине на реалізації і захист прав і свобод людини. Гарантоване статтею 32 Конституції України право на приватність в частині, що стосується заборони певний дій з конфіденційною інформацією про особу, знайшло своє відображення в Цивільному кодексу у частині другій статті 302, хоча й в дещо обмеженому вигляді.

Зокрема, в цій статті йдеться про цивільно-правовий захист права на заборону збирання, зберігання, використання і поширення інформацію про особисте життя, тобто вузького кола приватних відносин, насамперед, інтимного характеру. У той же час, як вже зазначалось у попередніх розділах цієї роботи, за європейським підходом, правового захисту потребують не лише ці аспекти приватного життя, а комплекс правових відносин, що виникають і реалізуються у зв'язку з обробкою персональних даних у різних сферах соціального буття, навіть й тих, які безпосередньо відносяться до публічної сфери життя людини, без чого неможливо забезпечити реалізацію права

на повагу до приватного життя, гарантованого статтею 8 Європейської Конвенції про захист прав людини та основних свобод. Це вимагає внесення відповідних змін до Цивільного кодексу з метою розширення відповідних суб'єктивних прав, яким надається цивільно-правовий захист.

Прогресивною є, на нашу думку, редакція статті 37 Закону України "Про телебачення і радіомовлення" [283], в якій законодавець запровадив оціночний критерій для врівноваження індивідуальних і суспільних інтересів, як того вимагає стаття 8 Європейської Конвенції про захист прав людини і основних свобод. Так, телерадіоорганізація зобов'язана не розголошувати інформацію про приватне життя громадянина без його згоди, якщо ця інформація не є суспільно необхідною. Це має враховуватися судом, зокрема, під час розгляду справ за позовами до телерадіокомпаній про відшкодування матеріальної та моральної шкоди.

Низка підзаконних нормативних актів у різних галузях законодавства також містить положення про обмеження доступу до інформації про особу, які відзначаються неконкретністю формулювання на зразок: "розголошення відомостей без згоди особи забороняється" (Постанова Кабінету Міністрів України від 04.06.1998 року № 794 "Про персоніфікований облік у системі пенсійного забезпечення" [284]) або "забезпечити конфіденційність інформації про особу" (Положення про порядок проведення медичного обстеження на ВІЛ засуджених до позбавлення волі, затверджене спільним наказом МВС, Міністерства охорони здоров'я, Комітету про запобіганню захворюванням на СНІД від 18 травня 1997 року [285]).

Успадкована Україною з тоталітарного режиму схильність до засекречування є гальмом на шляху до демократії. Залишки цієї негативної практики ще й досі пронизують правову систему України. Вітчизняні правознавці Ю. Тодика і В. Серьогін відзначають таку ситуацію як потенційно загрозливу, оскільки переважна більшість відомчих актів, які визначають перелік відомостей, що становлять інформацію з обмеженим доступом, самі не підлягають друку, що унеможливлює аналіз підстав засекречування [286].

Такому негативному явищу як обмеження доступу громадян до інформації, що є у розпорядженні органів державної влади, сприяє неадекватне законодавство, численні

прогалини в ньому, а також низький рівень правової свідомості державних службовців, які відповідають за правову регламентацію інформаційних відносин. Віднесення всієї інформації, що є у розпорядженні органів державної влади, до конфіденційної з наступним позначенням її грифом "ДСК" ("для службового користування") одразу обмежує права людини на свободу інформації і на приватність персоніфікованої інформації, складовим елементом якого є право людини на доступ до інформації про себе.

Використання нечіткого терміна "конфіденційна інформація про особу" в Конституції України також сприяє термінологічній плутанині. Конституція забороняє збирання, зберігання, використання та поширення конфіденційних відомостей про особу без її згоди з певними винятками з загального правила. Таке формулювання не чітке, оскільки залишається незрозумілим, вся чи лише частина відомостей про особу є конфіденційною. Скоріше за все, термін "конфіденційна інформація про особу" в Конституції застосовується для розрізнення правового режиму персоніфікованої інформації, яка дається особою під певні зобов'язання її подальшого нерозголошення одержувачем, та інформації про особу, яка є загальнодоступною, відкритою для доступу громадськості без застережень щодо подальшого її поширення, у тому числі публічного оголошення.

Частина 3 статті 32 Конституції України надає громадянам право на доступ до відомостей, що стосуються їх особисто, які не є державною або іншою захищеною законом таємницею. Цим фактично визнається, що персоніфікована інформація може бути віднесена до державної або іншої захищеної законом таємниці, що практично позбавляє громадян права на доступ до інформації про себе в окремих випадках.

Невизначеність правового режиму персоніфікованої інформації – віднесення її до відкритої чи конфіденційної або таємної у чинному законодавстві України – стала однією з причин розгляду Конституційним Судом України справи щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України "Про інформацію" та статті 12 Закону України "Про прокуратуру" (справа К.Г. Устименка) [287].

Заявник по справі, К.Г. Устименко, за клопотанням адміністрації спеціального навчального закладу у 1998 році був поставлений на консультативний психіатричний

облік за місцем проживання, а дізнався про це лише два роки потому. Він звернувся до головного лікаря психоневрологічного диспансеру з вимогою надання відомостей з питань постановки і зняття його з обліку, про можливі випадки повідомлення про це іншим особам, а також про застосовані до нього обмеження щодо працевлаштування за висновками психіатрів.

Посилаючись на лікарську таємницю, головний лікар диспансеру відмовив заявнику у надані такої інформації. Звернення до прокуратури також не дало бажаного результату, оскільки посадові особи органів прокуратури, посилаючись на статтю 37 закону України “Про інформацію”, відмовили прохачеві у наданні інформації про стан його здоров’я. Суди загальної юрисдикції різних ланок неодноразово і неоднозначно розглядали скарги заявника, задовольнивши його вимоги частково. Заявник одержав копію диспансерної картки і деяку іншу інформація, що не задовольнило його в повній мірі. Отже, в цій ситуації посадові особи державних органів, використовуючи хибні положення законодавства, зокрема, Законів України “Про інформацію” і “Основи законодавства України про охорону здоров’я”, неправомірно відмовляли громадянину в доступі до персоніфікованої інформації, посилаючись на лікарську таємницю.

Конституційний Суд України встановив наявність у нормативно-правовій базі в частині інформаційних правовідносин нечітко визначених, колізійних положень і прогалин, що негативно впливає на забезпечення конституційних прав і свобод людини і громадянина: не повністю визначено режим збирання, зберігання, використання та поширення інформації, зокрема, щодо психічного стану людини, її примусового огляду та лікування; не створено процедуру захисту прав особи від протизаконного втручання в її особисте життя психіатричних служб; належним чином не розроблено механізм реалізації права на доступ до персоніфікованої інформації.

Конституційний Суд України дав офіційне тлумачення лише частинам четвертій і п’ятій статті 23 та статті 48 Закону України “Про інформацію”, не знайшовши невизначеності в статтях 3, 31 , 47, як і в частині першій, другій, третій і шостій статті 23 Закону України “Про інформацію”, які вимагали б офіційного тлумачення у

контексті справи заявника. Так, Конституційний Суд України розтлумачив, що забороняється не лише збирання, а й зберігання, використання та поширення конфіденційної інформації про особу без її попередньої згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту, прав та свобод людини. Таким чином, Суд повторив відповідні положення статті 32 Конституції України.

Крім того, Конституційний Суд України здійснив офіційне тлумачення поняття "конфіденційна інформація". Суд відніс до конфіденційної інформації такі відомості про особу: освіта, сімейний стан, релігійність, стан здоров'я, дата і місце народження, майновий стан та інші персональні дані. При цьому Конституційний Суд не зазначив будь-яких застережень щодо джерел одержання персоніфікованої інформації, що, за нашим переконанням, є неправильним, бо, по-перше, особа сама вправі зробити свої персональні дані відкритими, а, по-друге, доступ до відомостей, що становлять легітимний суспільний інтерес, не може бути обмежений у цілях захисту інтересів суб'єкта даних.

Крім того, даючи тлумачення частини п'ятої статті 23 Закону України "Про інформацію", Конституційний Суд України через відсутність адекватного законодавчого регулювання питань доступу до інформації, яка містить таємницю, що охороняється законом, спробував прояснити, що саме відноситься до лікарської таємниці, а що до медичної інформації.

На думку Суду, лікарська таємниця – інформація про пацієнта, а медична інформація – інформація для пацієнта. До медичної належать "свідчення про стан здоров'я людини, історію її хвороби, про мету запропонованих досліджень і лікувальних заходів, прогноз можливого розвитку захворювання, в тому числі і про наявність ризику для життя і здоров'я". Проте стаття 40 Закону України "Основи законодавства України про охорону здоров'я", навпаки, відносить вказані відомості до лікарської таємниці. Як видно з переліку відомостей, які Суд відокремив від лікарської таємниці і відніс до медичної інформації, визнавши за ними статус конфіденційної інформації, вони також є відомостями про пацієнта.

Слід зауважити, що термін “конфіденційність” (*confidentia* – довір’я, **лат**.) означає довірчий, секретний, той, що не підлягає розголошенню, публікації [288, *359*]. Тобто, конфіденційна інформація з огляду на довірливий характер її повідомлення не повинна бути в подальшому розголошена. Цей термін може застосовуватися до будь-якого виду інформації, не обов’язково про особу. Отже, захист конфіденційності – це захист відносин довіри між тим, хто надає інформацію, і тим, хто її одержує, під зобов’язання уникати її розголошення.

Таким чином, режим конфіденційності не може бути поширений на персоніфіковану інформацію, яка є загальнодоступною, зокрема, через її публічне оголошення, а також на інформацію, яку особа бажає залишити таємною і не повідомляти нікому, чи яка віднесена до державної таємниці. Саме з цих позицій виходили розробники модельного закону “Про персональні дані”, який був підготовлений Постійною комісією з питань оборони і безпеки Міжпарламентською Асамблеєю держав-учасниць Співдружності Незалежних Держав (СНД) і прийнятий на її чотирнадцятому пленарному засіданні 16 жовтня 1999 року [289].

Зокрема, стаття 4 модельного закону проголошує:

“...2. Персональні дані, що знаходяться у віданні утримувача, належать до конфіденційної інформації, крім випадків, визначених чинним Законом.

3. Режим конфіденційності персональних даних знімається у випадках знеособлення персональних даних; вимог суб’єкта щодо своїх персональних даних, які не суперечать національному законодавству; включення персональних даних до загальнодоступних баз даних.

4. За бажанням суб’єкта для його персональних даних може бути встановлений режим загальнодоступної інформації (бібліографічні довідники, телефонні книги, адресні книги, приватні об’яви тощо)...”

Отже, право на приватність дозволяє особі на власний розсуд визначати режим доступу до її персональних даних з винятками в певних випадках, передбачених законами, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Одним з таких легітимних випадків обмеження права людини визначати режим доступу до своїх персональних даних і самому суб'єкту даних мати доступ до негласно зібраної персоніфікованої інформації є оперативно-розшукова діяльність правоохоронних органів.

Законом України від 18 січня 2001 року № 2246 внесено суттєві зміни, які ліквідують чимало недоліків Закону України "Про оперативно-розшукову діяльність" [290] і сприятимуть зміцненню законності в діяльності правоохоронних органів:

- посилені вимоги щодо підстав для проведення оперативно-розшукової діяльності, що вимагає від правоохоронних органів детального обґрунтування необхідності проведення цих заходів. Згідно з частиною першою статті 6 Закону такою підставою є наявність достатньої інформації, одержаної в установленому законом порядку, що потребує перевірки за допомогою оперативно-розшукових заходів і засобів;
- обмежується втручання інших осіб у діяльність оперативних підрозділів і підкреслюється обмежений характер оперативних заходів. Якщо за попередньою редакцією пункту 1 статті 7 оперативні підрозділи були зобов'язані виконувати письмові доручення слідчого, вказівки прокурора та ухвали суду і запити повноважних державних органів, установ та організацій про проведення оперативно-розшукових заходів, то за новою редакцією вони повинні у межах своїх повноважень *відповідно до законів*, що становлять правову основу оперативно-розшукової діяльності, вживати *необхідних* оперативно-розшукових заходів;
- конкретизуються випадки застосування технічних засобів для одержання інформації, процедура судового і прокурорського контролю (нагляду) за законністю цих дій, а також використання здобутої інформації у кримінальному судочинстві. Зокрема, передбачається, що застосування цих заходів проводиться виключно з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншим способом одержати інформацію неможливо. Рішення про надання або відмову в наданні дозволу на вжиття оперативних заходів і засобів приймає суд за поданням керівника відповідного оперативного підрозділу або його заступника, про що повідомляється прокуророві протягом доби. При цьому, за

результатами здійснення зазначених оперативно-розшукових заходів складається протокол з відповідними додатками, який підлягає використанню як джерело доказів у кримінальному судочинстві;

- внесенні до статті 9 зміни надають додаткові гарантії забезпечення прав людини під час оперативно-розшукової діяльності. Зокрема, якщо раніше Закон однозначно не зобов'язував оперативні органи заводити оперативно-розшукову справу у кожному випадку проведення заходів, то за новою редакцією без заведення оперативно-розшукової справи проведення оперативно-розшукових заходів, крім випадку, передбаченого частиною четвертою цієї статті, забороняється. Про заведення справи виноситься постанова, яка затверджується керівником або заступником керівника правоохоронного органу. Постанова повинна містити підстави і мету заведення оперативно-розшукової справи, що покращує можливості для відомчого контролю за здійсненням оперативної діяльності;
- доповнення Закону України "Про оперативно-розшукову діяльність" статтями 9-1 "Строки ведення оперативно-розшукових справ" і 9-2 "Закриття оперативно-розшукових справ" запроваджує процесуальні правила, які гарантують додержання терміну провадження оперативно-розшукової діяльності, а значить і відповідних обмежень прав людини у часі.

Разом з цими позитивними змінами в регулюванні оперативно-розшукової діяльності в Україні слід, однак, відзначити й недоліки, які залишились у відповідному законодавстві і можуть спричинитися до порушення права людини на приватність персоніфікованої інформації. Один з них стосується питання доступу до інформації, яка збирається про особу під час оперативно-розшукової діяльності. Зокрема, частина 9 статті Закону України "Про оперативно-розшукову діяльність" надає громадянам України та іншим особам право у встановленому законом порядку одержати від органів, на які покладено здійснення оперативно-розшукової діяльності, письмове пояснення з приводу обмеження їх прав і свобод та оскаржити ці дії до суду". Отже, одержати можна пояснення щодо застосування передбачених Законом України "Про оперативно-розшукову діяльність" заходів, а не самі відомості, що були одержані в ході такої діяльності. Крім того, сам факт негласного збирання і

використання відомостей про особу законодавством не визнається як обмеження права.

На нашу думку, будь-яке збирання, зберігання, використання і поширення персоніфікованої інформації без згоди особи (негласно) є обмеженням її прав незалежно від способів, методів і засобів виконання цих дій. Оперативно-розшукова діяльність, під час якої збирається інформація про особу таємно від неї, з самого початку, тобто з моменту заведення оперативно-розшукової справи, є обмеженням прав і свобод людини.

Частина 10 цієї статті Закону забороняє передачу і розголошення відомостей про нерозкриті злочини або такі, що можуть зашкодити слідству чи інтересам людини, безпеці України тощо. Частиною 13 цієї статті в попередній редакції передбачалось, що не підлягають передачі і розголошенню результати оперативно-розшукової діяльності, які відповідно до законодавства України становлять державну, військову і службову таємницю, а також відомості, що стосуються особистого життя, честі, гідності людини. Внаслідок змін, внесених Законом України від 18 січня 2001 року, слова "військову і службову" було виключено з тексту статті, що є позитивним прикладом позбавлення від ураженості "вірусом" засекречування з правових норм, що регулюють інформаційні питання.

Указана частина статті 9 Закону України проголошує, що не підлягають передачі та розголошенню результати оперативно-розшукової діяльності, які становлять державну таємницю. Затверджений наказом Голови Служби безпеки України від 1 березня 2001 року № 52 Звід відомостей, що становлять державну таємницю [291], відносить до державної таємниці у сфері державної безпеки і охорони правопорядку інформацію про факт підготовки та проведення, а також результати негласних оперативно-розшукових заходів із застосуванням оперативно-технічних засобів стосовно осіб, які готують або вчинили особливо небезпечні злочини проти держави (п. 4.18), а також ті самі відомості стосовно осіб, які готують або вчинили інші тяжкі злочини (п. 4.18.1). До останнього пункту є примітка, що у разі використання отриманої інформації як доказ у кримінальному процесі, зниження її ступеня секретності чи розсекречення здійснюється згідно з чинним законодавством України.

Таким чином, незалежно від підтвердження чи не підтвердження фактів причетності людини до підготовки або вчинення особливо небезпечного злочину проти держави, незважаючи на використання чи невикористання цих відомостей у кримінальному судочинстві, доступ до першої з указаних категорій відомостей зі ступнем секретності "цілком таємно" громадян, яких стосується інформація, заборонений.

Доступ до другої категорії відомостей із ступнем секретності "таємно", незалежно від підтвердження чи не підтвердження фатів причетності людини до підготовки або вчинення іншого тяжкого злочину проти держави, можливий лише після прийняття рішення про зниження ступеня її секретності чи розсекречення і лише у випадку використання отриманої інформації як доказ в кримінальному процесі.

Однак доступ людини до персоніфікованої інформації, яку одержали оперативні органи в інших випадках, також практично неможливий. Частина 12 статті 9 Закону "Про оперативно-розшукову діяльність" забороняє зберігання і зобов'язує відповідальних осіб оперативних органів знищувати одержані внаслідок оперативно-розшукової діяльності відомості, що стосуються особистого життя, честі, гідності людини, якщо вони не містять інформацію про вчинення заборонених законом дій.

Разом з тим, Закон не окреслює поняття "відомості, що стосуються особистого життя, честі, гідності людини", а воно може тлумачитись як завгодно широко чи вузько. На практиці, громадянин може ніколи не дізнатися, яку саме інформацію про нього було зібрано, використано і знищено. Отже, позитивні напрацювання, впроваджені в Закон України "Про оперативно-розшукову діяльність", потребують свого подальшого розвитку шляхом розширення гарантій забезпечення права людини на приватність персоніфікованої інформації.

Не менш важливим, але також неадекватно врегульованим є питання застосування відповідальності за порушення законодавства України про персоніфіковану інформацію. Стаття 47 Закону України "Про інформацію" передбачає, що порушення законодавства про інформацію тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність згідно з законодавством України.

При цьому частина друга статті 47 містить перелік можливих порушень, за які передбачається відповідальність: необґрунтована відмова від надання відповідної інформації; несвоєчасне надання інформації; навмисне приховування інформації; примушення до поширення або перешкоджання поширенню чи безпідставна відмова від поширення певної інформації; використання і поширення інформації стосовно особистого життя громадянина без його згоди особою, яка є власником відповідної інформації внаслідок виконання своїх службових обов'язків; розголошення державної або іншої таємниці, що охороняється законом, особою, яка повинна охороняти цю таємницю; порушення порядку зберігання інформації; навмисне знищення інформації; необґрунтоване віднесення окремих видів інформації до категорії відомостей з обмеженим доступом тощо.

Як видно з цього переліку, всі зазначені порушення можуть стосуватися персоніфікованої інформації. Однак наскільки повно цим переліком охоплюються можливі порушення стосовно інформації про особу, слід розглянути більш докладно.

Виходячи з того, що порушення законодавства у більшості випадків спричиняється до якихось негативних наслідків для носія певних прав, суб'єкта персональних даних, то й перелічені порушення можна класифікувати шляхом зіставлення з відповідними правами людини, які складають право на приватність персоніфікованої інформації.

Зокрема, право громадянина на самовизначення стосовно підстав, умов і обсягу операцій з обробки персональних даних передбачає відповідні обов'язки інших суб'єктів не перешкоджати протиправними діями чи бездіяльністю суб'єкту даних, тобто особі, якої стосується інформація, їх реалізовувати. До цих протиправних діянь можна віднести такі правопорушення, перелічені в статті 47 Закону України "Про інформацію": 1) примушення до поширення або перешкоджання поширенню чи безпідставна відмова від поширення інформації про особу; 2) використання і поширення інформації стосовно особистого життя громадянина без його згоди особою, яка є власником відповідної інформації внаслідок виконання своїх службових обов'язків; 3) розголошення державної або іншої таємниці, що

охороняється законом, особою, яка повинна охороняти цю таємницю; 4) порушення порядку зберігання інформації; 5) навмисне знищення інформації тощо.

Однак, поза сферою регулювання статті 47 Закону України “Про інформацію” залишилася низка протиправних дій, які порушують право людини на самовизначення стосовно підстав, умов і обсягу операцій з обробки персональних даних. З урахуванням офіційного тлумачення Конституційним Судом України частини четвертої статті 23 Закону України “Про інформацію” протиправним є не лише збирання, а й інші операції з персональними даними, які здійснюються без згоди суб’єкта даних за винятком тих, що передбачені законом. За Конституцією України це також такі дії, як зберігання, використання та поширення, хоча цілком логічним є включення до них і інших протиправних дій з персоніфікованою інформацією, які порушують право на інформаційне самовизначення, тобто які здійснюються без згоди суб’єкта даних. Це стосується таких операцій як накопичення (як ширше за змістом, ніж просто зберігання, включає також охоплення і запис інформації на матеріальний носій), передача (надання для ознайомлення третім особам, у тому числі шляхом публічного поширення інформації), знеособлення (перетворення, що унеможливлює подальше ототожнення з суб’єктом даних) і знищення персональних даних без згоди суб’єкта даних та за відсутності законних підстав для цього.

Іншою важливою складовою частиною права на приватність персоніфікованої інформації є право контролювати операції з персональними даними, яке покликано забезпечити сталість правового зв’язку між суб’єктом даних і персоніфікованою інформацією під час усіх операцій з ними. Сприяти суб’єктові даних у підтриманні цього правового зв’язку повинні особи, які здійснюють обробку інформації. Зокрема, суб’єкт даних має право знати, які операції з даними будуть здійснюватися в подальшому, а відповідальна за обробку особа повинна його про це повідомити до початку їх здійснення. Отже, право на контроль є необхідною гарантією реалізації права на інформаційне самовизначення на подальших операціях з персональними даними, у тому числі під час їх “вторинної” передачі або використання.

Неповідомлення або приховування операцій із “вторинної” обробки чи створення перешкод у реалізації суб’єктом даних права на контроль за здійсненням обробки повинно кваліфікуватися як порушення права на приватність персоніфікованої інформації.

Нарешті, право на доступ, внесення змін, знищення і заперечення проти обробки персональних даних у випадках і в порядку, визначеному законами України, є дієвою гарантією запобігання або припинення порушень прав суб’єкта даних. А створення перешкод суб’єктові даних у реалізації цих прав або невиконання його законних вимог також повинно розглядатися як порушення права на приватність інформації про особу. На жаль, чинне законодавство не вбачає в таких діях або бездіяльності складу порушення права на приватність.

На окрему увагу заслуговує питання щодо порушення законодавства про персоніфіковану інформацію внаслідок дій, які спрямовані проти встановленого порядку державного управління в галузі регулювання обробки персональних даних. Однак, про це можна буде вести мову лише тоді, коли такий порядок буде визначений законом (ідеться про порядок реєстрації масивів (баз) персональних даних, ліцензування транскордонної передачі даних, діяльність органу нагляду в галузі обробки персональних даних тощо).

Частина перша статті 47 закону України “Про інформацію” вказує на можливість застосування різних видів відповідальності за порушення законодавства України про інформацію, використовуючи при цьому в основному бланкетний спосіб зв’язку матеріальних норм Закону України “Про інформацію” з правовими нормами, що передбачають відповідальність за правопорушення. Виняток становить питання про притягнення до цивільно-правової відповідальності за порушення законодавства про інформацію, у тому числі про персоніфіковану інформацію. Зокрема, стаття 49 Закону України “Про інформацію” передбачає відшкодування матеріальної та моральної шкоди, завданої правопорушеннями, у розмірі, який визначається судом.

Незважаючи на відповідні положення Конституції України і Закону України “Про інформацію”, Кодекс про адміністративні порушення України не передбачає відповідальності за порушення законодавства про інформацію. До останнього часу

лише декілька статей Кримінального кодексу Української РСР від 28 грудня 1960 року із змінами, внесеними до нього [292], передбачали відповідальність за порушення законодавства про персоніфіковану інформацію. Перш за все це стаття 125 КК, яка передбачала відповідальність за наклеп, тобто поширення неправдивих вигадок, що ганьблять іншу особу. Стаття 108-4 КК встановлювала відповідальність за розголошення відомостей про проходження ВІЛ – обстеження і його результати медичними працівниками або іншими службовими особами. Стаття 115-1 КК передбачала відповідальність за розголошення таємниці усиновлення проти волі усиновителя.

Кримінальний кодекс України, прийнятий Верховною Радою України 5 квітня 2001 року, значною мірою розширив можливості притягнення до кримінальної відповідальності за злочини, які посягають на недоторканність приватного життя осіб, у тому числі щодо протизаконного збирання, зберігання, використання чи поширення персоніфікованої інформації [293].

Стаття 132 Кримінального кодексу України передбачає відповідальність за розголошення службовою особою лікувального закладу, допоміжним працівником, який самочинно здобув інформацію, або медичним працівником відомостей про проведення медичного огляду особи на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби, що є небезпечною для життя людини або захворювання на СНІД та його результатів, що стали їм відомі у зв’язку з виконанням службових або професійних обов’язків.

Стаття 145 КК передбачає кримінальну відповідальність за умисне розголошення лікарської таємниці особою, якій вона стала відома у зв’язку з виконанням професійних чи службових обов’язків, якщо така дія спричинила тяжкі наслідки.

Стаття 162 КК встановлює кримінальну відповідальність за незаконне проникнення до житла чи до іншого володіння особи, незаконне проведення в них огляду чи обшуку. Стаття 163 КК визнає злочином порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв’язку або через комп’ютер. Стаття 168 передбачає відповідальність за розголошення таємниці усиновлення всупереч волі усиновителя. Стаття 182 КК

“Порушення недоторканності приватного життя” встановлює кримінальну відповідальність за незаконне збирання, зберігання, використання або поширення конфіденційної відомостей про особу без її згоди або поширення цієї інформації у публічному виступі, творі, що публічно демонструється, чи в засобах масової інформації. Стаття 359 КК передбачає кримінальну відповідальність за незаконне використання спеціальних технічних засобів негласного отримання інформації.

Слід зауважити, що таке детальне визначення складу певних злочинів у галузі захисту права на приватність персоніфікованої інформації сприятиме розвитку інших галузей права, в яких мають дістати детальне врегулювання законами України й питання, пов’язані з обробкою персональних даних.

Разом з тим, за браком чітких положень законодавства щодо механізму узгодження інтересів людини, суспільства і держави в інформаційній сфері є значна загроза використання положень Кримінального кодексу України не на користь інтересам людини і суспільства, а, скажімо, для приборкання свободи слова.

Звертає на себе увагу редакція статті 182 Кримінального кодексу України, яка покликана захистити приватне життя громадян, однак звучить вона доволі категорично, що може на практиці сприйматися неадекватно:

“Стаття 182. Порушення недоторканності приватного життя

Незаконне збирання, зберігання, використання або поширення конфіденційної інформації про особу без її згоди або поширення цієї інформації у публічному виступі, творі, що публічно демонструється, чи в засобах масової інформації, –

караються штрафом до п’ятдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або арештом на строк до шести місяців, або обмеженням волі на строк до трьох років”[1)].

Отже, поширення конфіденційних відомостей про особу у публічному виступі, творі, що публічно демонструється, чи в засобах масової інформації може кваліфікуватися як суспільно небезпечне діяння, що містить ознаки злочину. Зважаючи на офіційне тлумачення Конституційним Судом України частини четвертої

[1)] [291] Кримінальний кодекс України: Офіц. видання. — К.: Видавничий Дім “Ін Юре”, 2001. — 336 с.

статті 23 Закону України “Про інформацію”, зокрема, віднесення всіх відомостей про особу до розряду конфіденційних, кожна журналістська публікація, що містить згадку про будь-яку людину, навіть не посадовця, який боїться публічного поширення доказів його можливої некомпетентності, чи політика, який обвинувачується в корупції або аморальності, – буде мати наслідком порушення кримінальної справи.

В той же час, загальновизнаним є той факт, що право на недоторканність приватного життя не є абсолютним і має бути узгоджено з правом на свободу інформації. Зокрема, це визнається в численних міжнародних документах з прав людини і в Конституції України.

Сама загроза застосування кримінальної відповідальності за публікацію відомостей про будь-яку особу є вже стримуючим фактором, що може негативно вплинути на стан зі свободою слова в Україні. На нашу думку, така редакція статті 182 Кримінального кодексу потребує редакційної правки для врахування принципу пропорційності обмеження права на приватність персоніфікованої інформації.

Встановлення кримінальної відповідальності за незаконне проникнення до житла чи до іншого володіння особи, незаконне проведення в них огляду чи обшуку (стаття 162 КК), за порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв’язку або через комп’ютер (стаття 163 КК), а також за незаконне використання спеціальних технічних засобів негласного отримання інформації (стаття 359 КК) є необхідним, але не достатнім для забезпечення ефективного захисту права людини на приватність персоніфікованої інформації.

Підсумовуючи викладене в цьому підрозділі, можна зробити висновок, що в нашій державі вже давно назріла нагальна потреба систематизації, усунення прогалин і вдосконалення чинного законодавства про персоніфіковану інформацію з урахуванням міжнародних стандартів і досвіду демократичних країн. Звичайно, що при цьому слід виходити з особливостей національної правової системи України і практики правозастосування. Ці питання розглядаються у наступному, завершальному підрозділі дослідження.

3.3. Впровадження європейських стандартів захисту приватності до правової системи України

У попередньому підрозділі сформульовано висновок, що законодавство України з питань захисту приватності персоніфікованої інформації потребує вдосконалення, приведення його у відповідність з міжнародними стандартами. Вивченню основних проблем, що виникають під час впровадження європейських стандартів в галузі захисту приватності персоніфікованої інформації до правової системи України, та визначенню шляхів їх розв'язання присвячується цей підрозділ роботи.

Існуючі прогалини і внутрішні протиріччя в чинному законодавстві негативно позначаються на правах і свободах громадян. Для ефективної реалізації проголошених у статтях 31 і 32 Конституції України прав і свобод громадян щодо персоніфікованої інформації повинен бути створений регулятивний механізм, покликаний реалізувати конституційні гарантії на практиці.

Необхідність вдосконалення і приведення законодавства України в галузі регулювання питань поводження з персоніфікованою інформацією у відповідність до міжнародних, зокрема, європейських стандартів, зумовлена також зовнішньополітичними чинниками. У Постанові Верховної Ради України "Про Засади державної політики України в галузі прав людини" від 17 червня 1999 року вказується, що серед основних напрямів державної політики у галузі прав людини є створення належних умов, вироблення механізмів і процедур для повної і безперешкодної реалізації кожною особою своїх прав та законних інтересів; приведення законодавства України у відповідність з універсальними стандартами прав людини Організації Об'єднаних Націй та Ради Європи [294].

Вступ до такої поважної міжнародної організації як Рада Європи, ратифікація Європейської Конвенції про захист прав людини і основних свобод 1950 року є свідченням намагання нашої держави приєднатися до сім'ї європейських демократичних країн. Конвенція Ради Європи № 108 базується на положеннях

Європейської Конвенції про захист прав людини та основних свобод 1950 року, зокрема, на її статтях 8 і 10, які гарантують право на приватність персоніфікованої інформації і право на вільне одержання і поширення інформації відповідно.

Прикро, але наша держава й досі не є учасницею Конвенції Ради Європи № 108 "Про захист осіб стосовно автоматизованої обробки персональних даних", що вже найближчим часом може створити труднощі і для співробітництва з країнами-учасницями Конвенції, оскільки цим документом передбачається обмеження транскордонної передачі персональних даних третім країнам, які не надають еквівалентного (адекватного) захисту приватності персональних даних. Однак, є сподівання, що ситуація незабаром покращиться. Підставою для цього є початок роботи з підготовки до підписання цієї Конвенції Ради Європи, ініційований Указом Президента України "Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України" [295].

Угода про партнерство і співробітництво між Україною і Європейськими Співтовариствами та їх державами-членами, яка набула чинності 1 березня 1998 року, вказує, що зближення чинного та майбутнього законодавства України із законодавством Співтовариства є важливою умовою для зміцнення взаємних економічних зв'язків [296]. Цей аспект підкреслюється у численних працях українських науковців, зокрема, у наукових статтях П. Лойтена [297]; В. Муравйова [298], Є. Прокопенко [299] та багатьох інших.

Однак не менш важливим вбачається й гуманістичний потенціал процесу європеїзації правової системи України. Як справедливо відзначає В.К. Забігайло, створення в Україні правової системи за європейською моделлю, передбачає, серед іншого, належну повагу до права, виконання його справжньої соціальної цінності не лише як інструменту регулювання та консервативної охорони суспільних відносин, а насамперед, ефективного засобу реалізації та захисту прав, свобод і законних інтересів громадян, інструменту динамічного суспільного прогресу [300, 9].

При цьому, як справедливо зазначає О.В. Задорожній, основним напрямком державної політики України, метою якої є входження України до європейського

правового простору, повинна стати не тільки апроксимація законодавства, а реформування всієї правової системи за європейськими стандартами, які містяться у документах ОБСЄ, Ради Європи та Європейського Союзу, а також з врахуванням національної практики держав-членів ЄС [301, *32*].

В Указі Президента України від 11 червня 1998 року "Про затвердження стратегії інтеграції України до Європейського Союзу" зазначається, що адаптація законодавства України до законодавства ЄС передбачає реформування її правової системи та поступове приведення у відповідність із європейськими стандартами, інтеграцію України до європейського політичного (у тому числі у сфері зовнішньої політики і політики безпеки), інформаційного, економічного та правового простору [302]. Звичайно, це не повинно обмежуватись лише адаптацією законодавства України до законодавства ЄС, а включати комплекс заходів з реформи всієї національної правової системи України для досягнення її відповідності правовим системам провідних європейських держав [303].

Отже, розглядаючи питання вдосконалення чинного законодавства України у галузі захисту приватності персоніфікованої інформації, слід виходити з необхідності впровадження європейських стандартів у цій галузі у вітчизняну правову систему з урахуванням досвіду європейських країн. В рамках цього дослідження доцільно визначити, що саме і яким чином треба зробити для приведення законодавства України у відповідність до вимог як Конвенції Ради Європи № 108 "Про захист осіб стосовно автоматизованої обробки персональних даних", так і Директиви Європейського Союзу 95/46/СЕ "Про захист фізичних осіб стосовно автоматизованої обробки персональних даних та безперешкодного руху цих даних".

Якщо раніше за своїми вимогами ці міжнародні документи певною мірою відрізнялись, то зараз у зв'язку із змінами і доповненнями до Конвенції Ради Європи № 108, зумовленими необхідністю усунення розбіжностей між стандартами Європейського Союзу і Ради Європи в цій галузі, вони суттєво не відрізняються.

З огляду на цей факт Україні доцільно приєднатися до Конвенції Ради Європи № 108 "Про захист осіб стосовно автоматизованої обробки персональних даних", але під час вдосконалення свого законодавства орієнтуватися на Директиву Європейського

Союзу 95/46/СЕ “Про захист фізичних осіб стосовно автоматизованої обробки персональних даних та безперешкодного руху цих даних” як таку, що була прийнята пізніше на 14 років, а тому більш адекватно до вимог часу, з урахуванням досвіду європейських країн і сучасного стану розвитку технічних засобів обробки персональних даних, регулює вказані питання.

Директива Європейського Союзу 95/46/СЕ регулює не лише питання обробки персональних даних, яка здійснюється всередині політико-правового простору Європейського Союзу, а регламентує також питання транскордонної передачі персональних даних. У такий спосіб відбувається “дифузія” її правових норм з законодавством країн Європейського Союзу та інших країн, яке застосовується під час тієї чи іншої транскордонної передачі персональних даних. Упроваджуючи високі стандарти в галузі захисту прав суб’єктів даних, Директива вимагає їх додержання під час транскордонної передачі персональних даних, що має певний вплив на правові системи інших країн.

Зокрема, стаття 25 Директиви передбачає, що передача до третіх країн персональних даних може здійснюватися лише тоді, коли третя країна гарантує адекватний рівень захисту. Адекватність рівня захисту оцінюється з урахуванням усіх обставин, що пов’язані з передачею або низкою операцій з передачі даних; зокрема, враховується характер даних, ціль, тривалість обробки або запропонованих обробок, країна походження і країна кінцевого призначення, стан законності і дотримання норм права – як загальних, так і галузевих, що діють у цій третій країні, а також професійні норми і заходи безпеки, що застосовуються у цій країні.”

Між тим, Директива передбачає також винятки з проголошеного у статті 25 правила з огляду на інтереси суб’єкта даних або важливі державні інтереси, про які, зокрема, йдеться у статті 26. Частина друга статті 26 вказує, що передача персональних даних до третьої країни, яка не забезпечує адекватного рівня захисту, дозволяється в окремих випадках за умови надання відповідних гарантій, які можуть випливати, зокрема, з договірних положень. Однак розглядати можливість застосування передбачених статтею 26 Директиви винятків до передачі персональних даних одержувачам в Україні доцільно лише у тому випадку, якщо вітчизняне

законодавство не буде приведено у відповідність до вимог Директиви Європейського Союзу 95/46/СЕ. Враховуючи нагальну потребу вдосконалення чинного законодавство у цій галузі, слід зосередитися не на пошуку можливих винятків для їх застосування стосовно передачі персоніфікованої інформації до нашої країни, а саме на досягненні *адекватного*, в європейському розумінні, рівня правового захисту відносин щодо використання персоніфікованої інформації.

Оціночна категорія адекватності, запропонована у статті 25 Директиви, вимагала свого подальшого тлумачення, що і було здійснено Робочою групою, створеною на підставі статті 29 Директиви з керівників наглядових органів у галузі обробки персональних даних країн-членів Європейського Союзу, а отже, безпосередніх виконавців Директиви. Перший документ за назвою "Перші орієнтири щодо передачі персональних даних до третіх країн – можливі напрями руху в оцінці адекватності" від 26 червня 1997 року був доповнений положеннями другого – "Передача персональних даних до третіх країн: застосовуючи статті 25 і 26 Директиви ЄС про захист даних", ухваленого Робочою групою 24 липня 1998 року.

Основоположними принципами, які повинні бути впровадженні в законодавство третьої країни і розглядаються як мінімальні вимоги під час аналізу на предмет адекватності, є:

1. Принцип обмеження ціллю – персональні дані повинні оброблятися для спеціальних цілей і використовуватися чи в подальшому передаватися лише тоді, коли це не є несумісним з ціллю передачі. Єдиними винятками з цього правила можуть бути лише ті, що необхідні в демократичному суспільстві, причому на одній з підстав, зазначених у статті 13 Директиви.

2. Якість даних і принцип пропорційності – персональні дані повинні бути точними і в разі необхідності поновлюватися. Дані повинні бути адекватними, відповідними і не надмірними з точки зору цілей, заради яких вони передаються чи в подальшому обробляються.

3. Принцип прозорості – індивіди повинні бути поінформовані щодо цілей обробки, особи контролера даних у третій країні та інших обставин, які потрібні для

забезпечення їх законних інтересів. Єдиними винятками є ті, що дозволяються на підставі положень частини другої статті 11 і статті 13 Директиви.

4. Принцип безпеки – контролером даних повинні вживатися технічні та організаційні заходи з безпеки до ризиків, пов'язаних з обробкою. Будь-яка особа, яка діє від імені контролера даних, включаючи обробника, не повинна обробляти дані інакше, як на підставі інструкцій контролера.

5. Право на доступ, виправлення і заперечення – суб'єкт даних повинен мати право одержати копію всієї інформації, що стосується його/її особисто, і право виправлення тих відомостей, які виявилися неточними. У певних ситуаціях він/вона повинен мати право заперечувати обробці даних, що його/її стосуються. Єдиними виключеннями щодо цих прав повинні бути ті, що дозволяються на підставі положень статті 13 Директиви.

6. Обмеження наступної передачі до інших, третіх, країн – подальші передачі персональних даних з країни призначення до іншої, третьої, країни повинні дозволятися лише тоді, коли наступна – третя – країна також надає адекватний рівень захисту. Єдиними винятками щодо цих прав повинні бути ті, що дозволяються на підставі положень статті 26 Директиви [304].

Перелічені вимоги є мінімальними. Для одержання позитивної оцінки щодо адекватності захисту прав людини в третій країні необхідною умовою є не лише "писане" (позитивне) право, тобто законодавча база цієї країни, яке має відповідати вимогам Директиви, а й дієвість існуючих правових приписів.

Для оцінки ефективності забезпечення дієвості основоположних принципів Робоча група, враховуючи наявність розбіжностей у правових системах європейських і неєвропейських країн, запропонувала стартові питання, не залежні від особливостей правових систем, відповіді на які у своїй сукупності дають уяву про досягнення чи недосягнення існуючою системою адекватного рівня захисту персоніфікованої інформації. В результаті їх впровадження така система повинна: забезпечувати прийнятний рівень додержання правил, надавати підтримку і допомогу індивідам у реалізації прав, гарантувати захист і поновлення порушених прав, притягнення порушників до відповідальності тощо.

Серед перших країн, рівень захисту в яких був підданий оцінці з боку Робочої групи, один з наших сусідів – Угорщина. Робоча група після аналізу стану законодавчого забезпечення права на приватність персоніфікованої інформації у цій країні визнала рівень захисту адекватним до вимог Директиви ЄС [305].

При цьому експертами Робочої групи до уваги бралися такі фактори, що вплинули на результат оцінки:

- додержання міжнародних зобов'язань, прийнятих Угорщиною у зв'язку з ратифікацією 8 жовтня 1997 року Конвенції Ради Європи № 108 "Про захист осіб стосовно автоматизованої обробки персональних даних";
- захист права на недоторканність приватного життя на конституційному рівні, у тому числі стосовно обробки персональних даних;
- наявність базового закону, який регулює питання захисту персоніфікованої інформації (Закон Угорщини "Про захист персональних даних і гласність інформації, що становить інтерес для громадськості" вступив у дію ще 1 травня 1993 року), а також галузевих законів, які містять відповідні положення щодо захисту персональних даних у різних секторах, зокрема, щодо діяльності спецслужб, у статистиці, комерційній діяльності, наукових дослідженнях і медицині;
- вироблення механізму забезпечення прав громадян, зокрема, через діяльність Омбудсмена.

Досягти таких результатів Угорщині допомогло її прагнення наблизити своє законодавство у цій галузі до законодавства Європейського Союзу, що є однією з умов для вступу в сім'ю європейських народів. Але найважливішими були внутрішні чинники, які базувались на усвідомленні громадськістю необхідності захисту права на приватність від втручань як з боку держави, так і приватного сектора.

У своїй доповіді на щорічній міжнародній конференції, організаторами якої є наглядові органи в галузі захисту приватності різних країн, Уповноважений Угорщини з захисту даних і свободи інформації, доктор Л. Майтені підкреслив значення цих внутрішніх і зовнішніх чинників для розвитку законодавства про захист приватності персоніфікованої інформації в країнах Східно-Центральної Європи,

пояснюючи як політичними, так і соціально-правовими особливостями процесу становлення демократії в Угорщині [306].

В Україні існують як внутрішні передумови для розвитку конституційних положень, що гарантують право на приватність, так і зовнішні чинники для впровадження європейських стандартів у вітчизняне законодавство про персоніфіковану інформацію, проте залишається невирішеним питання вибору способів для такого впровадження.

В країнах Європи, Канаді, Австралії, Японії, Гонконгу для закріплення принципів захисту приватності в національних правових системах приймається базовий закон про захист персональних даних, положення якого конкретизуються в галузевих законах, зокрема, щодо захисту тих чи інших категорій вразливих даних. В Україні досі не прийнятий такий спеціальний базовий закон, а загальні положення Закону України "Про інформацію" не можуть його замінити.

Як було вказано вище, інформація про особу не підпадає під класифікацію, в основі якої визначення належності її на праві власності тому чи іншому суб'єкту. Щодо питання кодифікації інформаційного законодавства України точаться наукові дискусії вже давно. Українські науковці Ю. Тодика та В. Серьогін пропонують кодифікувати чинне законодавство України про інформацію з обмеженим доступом шляхом прийняття єдиного, кодифікованого акта – Закону "Про інформацію з обмеженим доступом", який охоплював би правовим регулюванням весь комплекс інформаційних відносин, пов'язаних з реалізацією права на інформацію [307]. Т..А. Костецька пропонує створити загальний "Кодекс інформаційного права України", в якому нормативно-правові положення інформації, інформатики і інформатизації повинні бути уніфіковані й систематизовані [308].

У той же час, необхідність підготовки базового проекту закону, який захищатиме персоніфіковану інформацію, визначається як одне з завдань Національної програми інформатизації [309, 310]. Базовий закон у подальшому може і повинен бути кодифікований з іншими нормативно-правовими актами, які регулюють захист права людини на повагу до приватного життя у різних галузях законодавства, зокрема,

сімейному, соціального страхування, трудовому, фінансовому тощо, а не з нормативно-правовими актами в галузі інформаційної політики.

Надзвичайно важливе теоретичне і практичне значення для забезпечення ефективного і дієвого захисту персоніфікованої інформації має питання належного формулювання відповідних приписів у текстах нормативно-правових актів. “Якість” закону – фактор, який значною мірою зумовлює досягнення чи недосягнення результату його впровадження.

Питання якості закону, який покликаний регулювати відносини з обробки персональних даних у правоохоронній діяльності, неодноразово розглядалося під час вирішення Європейським Судом з прав людини справ про порушення права на повагу до приватного життя під час здійснення правоохоронними органами оперативно-розшукових заходів, зокрема, прослуховування телефонних розмов.

У справі “*Мелоуні проти Сполученого Королівства*” Суд, встановивши факт втручання у права заявника, гарантовані статтею 8 Європейської Конвенції про захист прав людини і основних свобод, дав оцінку, чи було таке втручання у відповідності до вимог, що їх містить частина друга статті 8. Суд постановив, що фраза “у відповідності до закону” відсилає не лише до національного законодавства, але також стосується якості закону – вимагає його відповідності принципу верховенства права, яке чітко сформульовано у преамбулі до Конвенції. Крім того, закон повинен бути достатньо конкретним у поняттях, щоб надати громадянам адекватну картину щодо обставин в яких і за яких умов, публічна влада уповноважена звернутися до цих секретних і потенційно небезпечних втручань у право на повагу до приватного життя і кореспонденції [311].

Конкретність закону, окрім іншого, означає і передбачуваність щодо його наслідків. Розглядаючи це питання, доцільно звернутися до практики Європейського Суду з прав людини, яким дається оцінка національного законодавства і його застосування на відповідність Європейській Конвенції з прав людини. Рішення цієї європейської правозахисної інституції демонструють досягнення сучасної правової теорії, застосовані до обставин конкретних справ у різних країнах. Дійсно таким, на

нашу думку, є одне з недавніх рішень Європейського Суду з прав людини, що має безпосереднє відношення до предмету цього дослідження.

Розглядаючи справу "*Аманн проти Швейцарії*" [312], Європейський Суд з прав людини встановив, що 12 жовтня 1981 року до позивача, який займався продажем косметичних засобів, зателефонувала жінка з колишнього посольства СРСР у Берні для замовлення одного з таких засобів. Телефонна розмова була підслухана Федеральною прокуратурою, яка за наслідками розслідування, проведеного поліцією, завела на заявника секретну картку, що містила інформацію з результатами перевірки у вигляді шифру.

У 1990 році позивачу стало відомо про існування картки. На його запит було надіслано копії картки, однак певна інформація в ній була викреслена. Заявник звертався до національних органів з метою дізнатися про зміст невідомих для нього даних, однак повною мірою його вимоги задоволені не були.

Європейський Суд з прав людини, оцінюючи правомірність втручання з боку публічної влади у приватне життя позивача, зважав на вимогу щодо якості закону, яка вимагає, щоб він був доступний для зацікавленої особи і передбачуваний щодо його наслідків.

Щодо правових гарантій під час застосування прослуховування телефонної розмови у цій справі Суд дав таку оцінку:

- правило є передбачуваним, якщо воно сформульовано достатньо конкретно для надання будь-якому індивіду за необхідністю відповідної поради для регулювання його поведінки;

- закон повинен визначати межі повноважень компетентних органів і спосіб їх застосування з достатньою ясністю, з урахуванням легітимної мети їх застосування у конкретному випадку для надання індивідам адекватного захисту проти свавільного втручання;

Європейський Суд з прав людини дійшов висновку, що право заявника на повагу до приватного життя було порушено внаслідок того, що положення національного законодавства були написані у поняттях дуже загальних і не могли задовольнити вимоги передбачуваності. Отже, щоб задовольнити вимоги, висунуті Європейським

Судом з прав людини, законодавство України має ретельно визначити права та обов'язки суб'єктів відносин з обробки персоніфікованої інформації. Врахування в законотворчій роботі правових позицій Європейського Суду дозволить значною мірою покращити нормативне забезпечення прав людини в Україні, у тому числі, права на приватність персоніфікованої інформації.

Висновки до розділу 3

Проведене у третьому розділі роботи дослідження законодавства та досвіду демократичних країн щодо захисту права на приватність персоніфікованої інформації, сучасного стану розвитку українського законодавства у цій сфері, а також шляхів його удосконалення відповідно до вимог європейських стандартів дозволяє сформулювати наступні висновки:

Виявлено три основні національні моделі правового захисту приватності персоніфікованої інформації: соціально-захисна (більшість європейських країн), ліберальна (США), змішана (Канада, Австралія). Для сучасного стану розвитку соціально-захисної моделі принциповим є поширення правил правового захисту персоніфікованої інформації, а також наглядових повноважень не тільки на публічні, але й рівною мірою й на приватноправові відносини. Поширена в США ліберальна модель ґрунтується на принципі невтручання держави у відносини між приватними особами, що обумовлює особливості національного режиму захисту персональних даних у приватному секторі США. Основний недолік ліберальної моделі виявляється у наявності нормативних прогалин у правовому механізмі захисту прав людини, зокрема, у приватному секторі економіки, що підтверджується прикладами із практики Федеральної торгової комісії США.

Простежується тенденція поширення соціально-захисної моделі в країни, які є традиційно ліберальними у їхньому ставленні до відносин між публічним і приватним секторами економіки, що підтверджується нещодавніми змінами у законодавстві Австралії й Канади. Це підтверджує необхідність запровадження європейської, соціально-захисної моделі захисту права на приватність в Україні.

Чинному законодавству України про захист персоніфікованої інформації бракує системності та термінологічної узгодженості, що не сприяє дотриманню законності і негативно позначається на правах і свободах громадян. Для впровадження європейських стандартів (соціально-захисної моделі) у законодавство України

необхідно прийняти базовий спеціальний закон, який повинен відповідати вимогам якості, сформульованим Європейським Судом з прав людини, - бути доступним і передбачуваним щодо наслідків для суб'єктів відносин з обробки персональних даних. З метою запобігання застосуванню обмежень щодо транскордонної передачі персональних даних, Україні потрібно приєднатись до Конвенції Ради Європи № 108, а також удосконалити національне законодавство з урахуванням положень Директиви ЄС № 95/46.

ВИСНОВКИ

Проведене дослідження міжнародно-правових актів та національне законодавство різних країн, доктрини і судової практики щодо забезпечення реалізації і захисту права людини на приватність персоніфікованої інформації дозволяє сформулювати узагальнені висновки, що зводяться до таких основних наукових положень:

- персоніфікована інформація є відображенням індивідуальності людини як носія певних елементів фізичної, фізіологічної, психічної, економічної культурної або соціальної тотожності. Розвиток засобів збирання і передачі інформації несе ризики неправомірного використання персоніфікованої інформації, втручання у приватне життя, що потребує адекватного правового забезпечення на національному й міжнародному рівнях;
- право на приватність персоніфікованої інформації є загальновизнаним правом людини. Воно не є абсолютним і підлягає за необхідністю обмеженню на законних підставах і в легітимних цілях. Правова конкуренція права на приватність персоніфікованої інформації з правом на свободу інформації та інтересами суспільства у боротьбі із злочинністю вимагає від держави створення механізму погодження задіяних інтересів шляхом встановлення справедливого балансу, а також оцінки застосованих обмежень на відповідність принципу пропорційності;
- міжнародно-правовий інститут захисту приватності персоніфікованої інформації складається з системи загальних і спеціальних норм, які забезпечують право людини на приватність, у тому числі під час передачі персоніфікованої інформації через кордони, а також норм, які гарантують безперешкодність інформаційного транскордонного обміну;
- міжнародно-правові стандарти, що втілені в Конвенції Ради Європи “Про захист осіб стосовно автоматизованої обробки персональних даних” 1981 року і

Директиві № 95/46 СЕ Європейського Парламенту і Ради “Про захист фізичних осіб стосовно автоматизованої обробки персональних даних та безперешкодного руху цих даних” 1995 року, відбивають загальноєвропейський, соціально-захисний підхід до регулювання обробки і транскордонної передачі персональних даних. “Керівні принципи, що регулюють захист приватності і транскордонні потоки персональних даних” Організації Економічного Співробітництва і Розвитку 1980 року, а також “Керівні принципи стосовно комп’ютеризованих файлів персональних даних” ООН 1990 року виникли внаслідок досягнення міжнародного консенсусу між країнами з різними правовими традиціями і базуються на ліберальному, орієнтованому на ринкові відносини підході до регулювання захисту приватності;

- країни Європейського Союзу гармонізують своє законодавство у галузі використання персоніфікованої інформації в правоохоронній діяльності на основі принципів, закладених у Директиві ЄС 95/46, а також Конвенції Ради Європи № 108 і Рекомендації Комітету Міністрів Ради Європи № R (87)15. Інкорпорація зазначених принципів у Шенгенську Конвенцію і Конвенцію Європол позитивно вплинула на врегулювання питань обробки персональних даних у правоохоронній діяльності на європейському рівні;

- договірна модель визнається в теорії і на практиці як один з можливих засобів поширення дії національного адекватного (еквівалентного) захисту приватності на відносини з передачі персональних даних до третіх країн. Правові питання укладення таких договорів ще не врегульовані належним чином; а тому відмічається наявність розбіжностей у підходах на національному і міжнародному рівнях. Модель забезпечення безперешкодної передачі даних між країнами з різним рівнем захисту персоніфікованої інформації під назвою “Рятувальна Гавань”, яка ґрунтується на домовленості між Європейським Союзом і Сполученими Штатами, має обмежений характер, оскільки поширюється лише на окремі сегменти приватного сектора економіки США і пристосована до особливостей національного механізму публічно-правового нагляду за комерційною практикою;

- виявлено три основні національні моделі правового захисту приватності персоніфікованої інформації: соціально-захисна (більшість європейських країн), ліберальна (США), змішана (Канада, Австралія). Для сучасного стану розвитку соціально-захисної моделі принциповим є поширення правил правового захисту персоніфікованої інформації, а також наглядових повноважень не тільки на публічні, але й рівною мірою й на приватноправові відносини. Поширена в США ліберальна модель ґрунтується на принципі невтручання держави у відносини між приватними особами, що обумовлює особливості національного режиму захисту персональних даних у приватному секторі США. Основний недолік ліберальної моделі виявляється у наявності нормативних прогалин у правовому механізмі захисту прав людини, зокрема, у приватному секторі економіки, що підтверджується прикладами із практики Федеральної торгової комісії США;

- простежується тенденція поширення соціально-захисної моделі в країни, які є традиційно ліберальними у їхньому ставленні до відносин між публічним і приватним секторами економіки, що підтверджується нещодавніми змінами у законодавстві Австралії й Канади. Це підтверджує необхідність запровадження європейської, соціально-захисної моделі захисту права на приватність в Україні;

- чинному законодавству України про захист персоніфікованої інформації бракує системності та термінологічної узгодженості, що не сприяє дотриманню законності і негативно позначається на правах і свободах громадян. Для впровадження європейських стандартів (соціально-захисної моделі) у законодавство України необхідно прийняти базовий спеціальний закон, який повинен відповідати вимогам якості, сформульованим Європейським Судом з прав людини, - бути доступним і передбачуваним щодо наслідків для суб'єктів відносин з обробки персональних даних. З метою запобігання застосуванню обмежень щодо транскордонної передачі персональних даних, Україні потрібно приєднатись до Конвенції Ради Європи № 108, а також удосконалити національне законодавство з урахуванням положень Директиви ЄС № 95/46.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1]. Джинчарадзе Н.Г. Інформаційна культура. — К. — 1999. — С. 9.

[2]. Clarke R. The Digital Persona and its Application to Data Surveillance // The Information Society. 1994. — № 10.

[3]. Social Risks of Smart Cards // Report of the Ministry of Justice working group. — The Hague: 1998. — 30 p.

[4]. Grijpink J.H.A.M. Identity fraud in an information society: the case of a chain approach // Interpol publications. — The Hague: 2001. — 15 p.

[5]. Mnookin R.N. The Public/Private Dichotomy: Political Disagreement and Academic Reputation // University of Pennsylvania Law Review. — 1982. — № 130. — P. 1429.

[6]. Hallborg R.B. Principles of Liberty and Right to Privacy // Law and Philosophy. — 1986. — № 5.

[7]. Privacy and Human Rights: An International Survey of Privacy Laws and Developments. — Global Internet Liberty Campaign, 1998.

[8]. Brandeis Louis D., Warren Samuel D. The Right to Privacy // Harvard Law Review. — 1890. — P. 193-220.

[9]. Levine Mortone. Privacy in the Tradition of the Western World // Pastoral Psychology Series (papers of Pastoral Psychology Institute). — N.Y. — 1979. — P.3.

[10]. Prosser William L. Handbook of the Law of Torts. – St. Paul: West Publication Corp., 1964. – P. 810-811.

[11]. Bloustein Edward J. Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser // NYU Law Review — 1964. — № 39. — P. 1003.

[12]. Stromholm S. La protection de la vie privee — essai de morphologie juridique comparee // Copyright and jurisprudence. — 1983. — P. 213-238.

[13]. Alan F. Westin. Privacy and Freedom. — New York: Atheneum, 1967. — P. 7.

[14]. Arthur R. Miller The Assault on Privacy. — Univ. of Mich. Press, 1971 — P. 25.

[15]. Юсупов Р.М., Заболотский В.П., Иванов В.П. Человек в информационном пространстве // Проблемы информатизации. — 1996. — № 4. — С. 3-7.

[16]. Privacy and Human Rights: An International Survey of Privacy Laws and Developments. — Global Internet Liberty Campaign, 1998. — P. 7.

[17]. Жуковська О. Правовий зміст поняття “відомостей, що не відповідають дійсності”, поширення яких є підставою для цивільної відповідальності // Адвокат. — 1999. — №3. — С. 14-19.

[18]. Жуковська О. Право на свободу слова та інформації в українському законодавстві та судовій практиці (деякі аспекти проблеми) // Свобода висловлювань і приватність. — 2002. — № 2. — С. 4-12.

[19]. Захаров Є. Свобода вираження поглядів в Україні в 2001р. // Свобода висловлювань і приватність. — 2001. — № 4. — С. 4-9.

[20]. Захаров Є., Рапп І. Аналіз практики доступу до урядової інформації // Свобода висловлювань і приватність. — 2002. — № 1. — С. 4-6.

[21]. Захаров Є., Рапп І. Аналіз доступу до інформації про незаконні дії співробітників правоохоронних органів // Свобода висловлювань і приватність. — 2002. — № 2. — С. 12-16.

[22]. Костецька Т.А. До питання про систему інформаційного законодавства // Концепція розвитку законодавства України: матеріали наук.-практ. конференції. — К.: Ін-т законод. Верх. Ради України, 1996. — С. 67-68.

[23]. Костецька Т.А. Право на інформацію в Україні. — К., 1998. — 39 с.

[24]. Місьо М., Петрова Н. Українське законодавство і захист преси. // Свобода висловлювань і приватність. — 2000. — № 1-2. — С. 3-34.

[25]. Іванов В.Ф. Інформаційне законодавство: український та зарубіжний досвід. — К.: Центр вільної преси, 1999. — 210 с.

[26]. Кураков Л.П., Смирнов С.Н. Информация как объект правовой защиты. — М.: Гелиос, 1998. — 240 с.

[27]. Буль Г.П. Доступ до інформації: юридичні аспекти. Нове законодавство щодо архівів як продукт сучасної юридичної думки: баланс свободи інформації і захисту даних // Свобода висловлювань і приватність. — 2001. — № 4. — С. 14-19.

[28]. Ван Вліт А.П. Право знати, право забути? Персональна інформація в публічних архівах // Свобода висловлювань і приватність. — 2001. — № 4. — С. 19-23.

[29]. Жеплінський А. Право на знання архівних даних про себе. Архіви колишніх спецслужб // Свобода висловлювань і приватність. — 2001. — № 4. — С. 23-26.

[30]. Куінтана А.Г. Архіви служб безпеки колишніх репресивних режимів // Свобода висловлювань і приватність. — 2002. — № 1. — С. 16-26.

[31]. Колосов Ю.М. 1974. – С. 32

[32] Pearce Graham, Platten Nicholas. Achieving Personal Data Protection in the European Union // Journal of Common Market Studies, Oxford. — 1998. — Vol. 36. —No. 4. — P. 529-547.

[33]. L. Thierry, P. Yves. La protection des donnees a caractere personnel en pleine (r)evolution. La loi du 11 decembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 // Journal des Tribunaux, Bruxelles. — 1999. — 22 mai. — Annee 118. — No. 5928. — P. 377-396.

[34]. Boulanger Marie-Helene, Terwangne Cecile de, Leonard Thierry. La protection des donnees a caractere personnel en droit communautaire. I // Journal Des Tribunaux Droit Europeen, Bruxelles. — 1997. — Annee 5. — No. 40. — P. 121-127.

[35]. Boulanger Marie-Helene, Terwangne Cecile de, Leonard Thierry. La protection des donnees a caractere personnel en droit communautaire. II // Journal Des Tribunaux Droit Europeen, Bruxelles. — 1997. — Annee 5. — No. 41. — P. 145-155.

[36]. Ponthoreau Marie-Claire. La directive 95/46 CE du 24 octobre 1995 relative a la protection des personnes physiques a l'egard du traitement des donnees a caractere personnel et a la libre circulation de ces donnees // Revue Francaise De Droit Admimistratif, Paris. — 1997. — Janvier - fevrier. — Annee 13. — No. 1. — P. 125-150.

[37]. Donk Wim van de, Duivenboden Hein van, Raab Charles D. Dossier: Les politiques et la politique de protection des donnees. II. (Fin) // Revue Internationale Des Sciences Administratives, Bruxelles. — 1996. — Decembre. — Vol. 62. — No. 4. — P. 613-689.

[38]. Bruhann Ulf. La protection des donnees a caractere personnel et la Communaute europeenne // Revue Du Marche Commun Et De L'union Europeenne, Paris. — 1999. — Mai. — No. 428. — P. 328-341.

[39]. Mayer-Schönberger. Generational Development of Data Protection in Europe // Technology and Privacy: The New Landscape; Ed. Philip E. Agre, Marc Rotenberg. — Cambridge: The MIT Press, 1997. — P. 224.

[40]. Blume Peter. The Data Protection Directive and Danish Law // International Review of Law Computers and Technology, Cambridge. — 1997. — March. — Vol. 11. — No. 1. — P. 65-77.

[41]. Saarenpaa Ahti. Data Protection: In Pursuit of Information. Some Background to, and Implementations of, Data Protection in Finland // International Review of Law Computers and Technology, Cambridge. — 1997. — March. — Vol. 11. — No. 1. — P. 47-64.

[42]. Chalton Simon. The Transposition into UK Law of EU Directive 95/46/EC (the Data Protection Directive) // International Review of Law Computers and Technology, Cambridge. — 1997. — March. — Vol. 11. — No. 1. — P. 25-32.

[43]. Morton Jeremy. Data Protection and Privacy: R v Brown // European Intellectual Property Review, Oxford. — 1996. — October. — Vol. 18. — No. 10. — P. 558-561.

[44]. Donk Wim van de, Bennett Colin J., Raab Charles D. Dossier: Les politiques et la politique de protection des donnees. I // Revue Internationale Des Sciences Administratives, Bruxelles. — 1996. — Decembre — Vol. 62. — No. 4. — P. 549-611.

[45]. Brouwer Frederic de. Protection of Personal Data: a New Belgian Legal Framework // Revue de Droit Des Affaires Internationales, Paris. — 1999. — No. 2. — P. 181-206.

[46]. Garstka Hansjurgen. Empfiehlt es sich Notwendigkeit und Grenzen des Schutzes personenbezogener — auch grenzuberschreitender — Informationen neu zu bestimmen? // Deutsches Verwaltungsblatt, Koln. — 1998. — September. — Nr. 18. — S. 981-992.

[47]. Mayer-Schonberger Viktor, Zeger Hans G., Kronegger Dieter Auf dem Weg nach Europa: Zur Novellierung des Datenschutzgesetzes // Osterreichische Juristen-Zeitung, Wien. — 1998. — April. — Jahrg. 53. — Nr. 7. — S. 244-251.

[48]. Castono Suarez Raquel. Directiva 95/46, de 24 de octubre de 1995, relativa a la proteccion de las personas fisicas en lo que respecta al tratamiento de datos personales y a la libre circulacion de estos. Similitudes y diferencias con la Ley Organica 5/1992, de 29 de octubre (LORTAD) // Noticias De La Union Europea. CISS, Valencia. - 1998. - Julio. - Ano 14. - No. 162. - P. 9-15.

[49]. Ruiz Miguel Carlos. En torno a la proteccion de los datos personales automatizados // Revista De Estudios Politicos, Madrid. - 1994. - Abril - Junio. - No. 84. - P. 237-264.

[50]. Imperiali d'Afflitto Rosario. La direttiva comunitaria sulla privacy informatica // Diritto Comunitario E Degli Scambi Internazionali, Parma. 1995. - Luglio - dicembre. - Anno 34. – No 3-4. - P. 569-588.

[51]. Nova Antonio. La tutela del diritto alla riservatezza nel trattamento dei dati personali // Aggiornamenti Sociali, Milano. — 1998. — Aprile. — Anno 49. — No. 4. — P. 259-272.

[52]. Vassilaki Irini. The constitutional background of privacy protection within the European Communities: Basic principles for the interpretation and implementation of the EC Data Protection Directive. // Revue Europeenne de Droit Public. Revue quadrilingue, London. — 1994. — Vol. 6. — No. 1. — P. 109-129.

[53]. Braibant Guy, Bruhann Ulf, Raab Charles D. La protection des donnees personnelles. I // Revue Francaise D'administration Publique, Paris. — 1999. — Janvier-mars. — No. 89. — P. 5-48.

[54]. Mallet-Poujol Nathalie, Mestre Delagado Juan Francisco, Poullet Yves La protection des donnees personnelles. II // Revue Francaise D'administration Publique, Paris. — 1999. — Janvier-mars. — No. 89. — P. 49-81.

[55]. Cadoux Louise; Rule James B La protection des donnees personnelles. III // Revue Francaise D'administration Publique, Paris. — 1999. — Janvier-mars. — No. 89. — P. 83-104.

[56]. Warufsel Bertrand, Burkert Herbert La protection des donnees personnelles. IV. (Fin.) // Revue Francaise D'administration Publique, Paris. — 1999. — Janvier-mars. — No. 89.

— P. 105-163.

[57]. Cox Jean-Claude. Base de donnees et protection de la vie privee: mythe ou necessite? // Reflets Et Perspectives De La Vie Economique, Bruxelles. — 1996. — T. 35. — No. 3. — P. 345-354.

[58]. Simitis Spiros. Reconsidering the Premises of Labour Law: Prolegomena to an EU Regulation on the Protection of Employees' Personal Data // European Law Journal, Oxford. — 1999. — March. — Vol. 5. — No. 1. — P. 45-62.

[59]. Krimphove Dieter. Neuer Europaischer Datenschutz im Arbeitsrecht // Neue Zeitschrift Fur Arbeitsrecht, Munchen. — 1996. — November. — Jahrg. 13. — Nr. 21. — S. 1120-1125.

[60]. Wohlgemuth Hans H. Auswirkungen der EG-Datenschutzrichtlinie auf den Arbeitnehmer-Datenschutz // Betriebsberater, Heidelberg. — 1996. — Marz. — Jahrg. 51. — Nr. 13. — S. 690-695.

[61]. Harala Riitta, Reinikainen Anna-Leena. Confidentiality in the use of administrative data sources // Statistical Journal. United Nations Economic Commission for Europe, Geneva. — 1996. — Vol. 13. — No. 4. — P. 361-368.

[62]. Bruhann Ulf. La protection des donnees dans le commerce electronique // Revue Du Marche Commun Et De L'union Europeenne, Paris. — 1999. — No. 430. — P. 464-471.

[63]. Linant de Bellefonds Xavier. Les resistances des droits comptables et fiscaux europeens au developpement des echanges de donnees informatisees // Revue Internationale De Droit Compare, Paris. — 1995. — Janvier - mars. — Annee 47. — No. 1. — P. 77-96.

[64]. Schild Hans-Hermann. Die Richtlinie uber die Verarbeitung personenbezogener Daten und den Schutz der Privatsphare im Bereich der Telekommunikation // Europaische Zeitschrift Fur Wirschaftsrecht, Frankfurt am Main. — 1999. — Februar. — Jahrg. 10. — Nr. 3. — S. 69-74.

[65]. Geis Ivo. Internet und Datenschutzrecht // Neue Juristische Wochenschrift, Munchen. — 1997. — Januar. — Jahrg. 50. — Nr. 5. — S. 288-293.

[66]. Иванский В.П. Правовая защита информации о частной жизни граждан. Опыт современного правового регулирования: Монография. — М.: Изд-во РУДН, 1999. — 276 с.

[67]. Иванский В.П. Теоретические проблемы правовой защиты частной жизни в связи с использованием информационных технологий: Дис… канд. юрид. наук: 12.00.01. — М., 1998. — С. 31.

[68]. Platten Nicolas. Orchestrating Transatlantic Approaches to Personal Data Protection: a European Perspective // Fordham International Law Journal, New York. — 1999. — June. — Vol. 22. — No. 5. — P. 2024-2051.

[69]. Mei Peter. The EC Proposed Data Protection Law // Law and Policy in International Business, Washington. — 1993. — Vol. 25. — No. 1. — P. 305-334.

[70]. Regan Priscilla M. American Business and the European Data Protection Directive: Lobbying Strategies and Tactics // Visions of Privacy: Policy Choices for the Digital Age; Ed. By Colin J. Bennett, Rebecca Grant. — Toronto. — P. 204.

[71]. Fleischmann Amy Personal Data Security: Divergent Standards in the European Union and the United States // Fordham International Law Journal, New York. — 1995. — October. — Vol. 19. — No. 1. — P. 143-180.

[72]. Donk Wim van de, Bennett Colin J., Raab Charles D. Dossier: Les politiques et la politique de protection des donnees. I // Revue Internationale Des Sciences Administratives, Bruxelles. — 1996. — Decembre. — Vol. 62. — No. 4. — P. 549-611.

[73]. Escobar de la Serna Luis. La proteccion de datos en el ambito internacional y en el derecho comunitario // Comunidad Europea Aranzadi. Editorial, Pamplona. — 1996. — Evero. — Ano 23. — No. 1. — P. 45-50.

[74]. Bennett C.J., Raab C.D. The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response // The Information Society. — 1997. — № 13.

[75]. Bennett C.J., Raab C.D. Taking the Measure of Privacy: Can Data Protection be Evaluated? // International Review of Administrative Sciences. — 1996. — № 4 (62).

[76]. Bennett C.J., Raab C.D. Protecting Privacy Across Borders: European Policies and Prospects // Public Administration. — 1994. — № 1 (72).

[77]. Carlin Fiona M. The Data Protection Directive: the introduction of common privacy standards // European Law Review, London. — 1996. — February. — Vol. 21. — No. 1. — P. 65-70.

[78]. Longworth E. Contractual Privacy Solutions // 22nd International Conference on Privacy and Data Protection. — Venice: 2000. — 21 p.

[79]. Kotschy W. Model Contracts for securing data protection in cases of transborder data flow to countries without adequate data protection // 22nd International Conference on Privacy and Data Protection. — Venice: 2000. — 8 p.

[80]. Dix A. Case Study: North America and the European Directive. The German Railway Card: A Model contractual solution of the ‘adequate level of protection’ issue? // 18th International Privacy and data Protection Conference ‘Privacy beyond Borders’. — Ottawa: 1996. — 6 p.

[81]. Буткевич В.Г. Соотношение внутригосударственного и международного права. — К., 1981.

[82]. Денисов В.Н. Актуальні питання застосування норм міжнародного права у внутрішньому праві України // Правова держава Україна: проблеми, перспективи розвитку: Короткі тези доповідей та наукових повідомлень республіканської науково-практичної конференції. 9-11 листопада 1995р.— Харків: НЮА України, 1995.— С. 153-156.

[83]. Денисов В.Н. Ефективність міжнародного права у правовому механізмі зовнішньополітичної діяльності держав // Законодавство: проблеми ефективності. — К., 1995.

[84]. Денисов В.Н. Коллизионные вопросы применения международного права во внутреннем праве // Колізії у законодавстві України: проблеми теорії і практики. Матеріали Міжнародної науково-практичної конференції, Київ, 23-24 жовтня 1995 р. — К.: Генеза, 1996.

[85]. Денисов В.Н. Развитие теории и практики взаимодействия международного права и внутреннего права // Реализация международно-правовых норм во внутреннем праве. — К., 1992. — С. 7-24.

[86]. Денисов В.Н., Евинтов В.И. Реализация международно-правовых норм во внутреннем праве. — К. — Наук. думка, 1992.

[87]. Денисов В.Н., Євінтов В.І. Суверенітет України і міжнародне право. — К.: Манускрипт, 1995.

[88]. Онопчук І.Ю. Міжнародно-правові проблеми формування інформаційної інфрастурктури України // Законодавство України та міжнародне право / проблеми гармонізації: Збірник наук. праць Ін-т законод. Верх. Ради України. — К., 1998. — в. 4. — С. 102-113.

[89]. Онопчук І.Ю. Окремі проблеми міжнародного та національного інформаційного права // Проблеми гармонізації законодавства України з міжнародним правом: матеріали наук. - практ. конференції. — К.: Ін-т закнод. Верх. Ради України, 1998. — С. 312-316

[90]. Опришко В. Питання трансформації Європейського права в законодавство України // Право України. — 2001.— № 2.— С. 27-30.

[91]. Павличенко О. Захист прав людини — до норм Ради Європи // Закон і бізнес.— 1996.— 23 жовтня. — С. 6.

[92]. Нормативно-правовое обеспечение в сфере информации, информатизации и информационной безопасности в Украине // Винарик Л.С. и др.; НАН Украины, Ин-т экономики и промышленности. — Донецк, 1996. — 25 с.

[93]. Шевчук С.В. Доступ до документованої інформації про особу: європейське право та практика Конституційного Суду України // Проблеми гармонізації законодавства України з міжнародним правом: матеріали наук.-практ. конференції. — К.: Ін-т законод. Верх. Ради України. — К., 1998. — в. 4. — С. 170-173.

[94]. Костецька Т.А. Гармонізація національного інформаційного законодавства як умова входження України в світове інформаційне середовище // Проблеми

гармонізації законодавства України з міжнародним правом: матеріали наук.-практ. конференції. — К.: Ін-т законод. Верх. Ради України, 1998. — С. 286-289.

[95]. Полінкевич К.Б. Окремі питання гармонізації законодавства України та міжнародного права в інформаційній сфері // Законодавство України та міжнародне право / проблеми гармонізації: Збірник наук. праць Ін-т законод. Верх. Ради України. — К., 1998. — в. 4. — С. 114-123.

[96]. Полінкевич К.Б. Проблеми впровадження міжнародно-правових стандартів захисту конфіденційної інформації про особу // Проблеми гармонізації законодавства України з міжнародним правом: матеріали наук.-практ. конференції. — К.: Ін-т законод. Верх. Ради України. — К., 1998. — в. 4. — С. 319-323.

[97]. Баранов А., Брыжко В, Базанов Ю. Защита персональных данных. — К.: Национальное агенство по вопросам информатизации при Президенте Украины, 1998. — 128с.

[98]. Баранов А., Брыжко В, Базанов Ю. Права человека и защита персональних данных. — К.: Государственный комитет связи и информатизации Украины, 2000.

[99]. Антонович М.М. Права людини та міжнародне гуманітарне право // Права людини і Україна. – Львів: Світ, 1999. – С. 61-65.

[100]. Дмитрієв А.І. Міжнародне гуманітарне право: основи концепції / Інститут держави і права ім. В.М.Корецького НАН України; Вища школа права при Інституті держави і права ім. В.М.Корецького НАН України. — К. : Логос, 1999. — 119с.

[101]. Dinstein Y. International Humanitarian Law // International Human Rights Law: Theory and Practice / Ed. by I. Cotler and F.P. Eliadis. – Montreal: The Canadian Human Rights Foundation, 1992. – P. 208-209.

[102]. Hampson F.J. Human Rights Law and International Humanitarian Law: Two Coins or Two Sides of the Same Coin? // Bulletin of Hum. Rts. – 1991. – V. 1. – P. 48-49.

[103]. Антонович М.М. Україна в міжнародній системі захисту прав людини. — К.: Видавничий дім "КМ Academia", 2000. — 262 с.

[104]. Международное право: Учебник / Отв. ред. Ю.М. Колосов, В.И. Кузнєцов. – М.: Международные отношения, 1994. – С. 297.

[105]. С. Васильева Т. А., Карташкин В. А., Колесова Н. С., Колотова Н. В., Ледях И. А. Права человека: Учебник для вузов / Комиссия по правам человека при Президенте РФ; Институт государства и права РАН / Е.А. Лукашева (отв.ред.). — М. : Норма, 2000. — 573с.

[106]. Заблоцька Л. Виникнення та формування міжнародних стандартів у галузі прав людини // Український часопис прав людини. —1995.— № 1.— С. 37-42.

[107] Рабінович П.М. Основні права людини: поняття, класифікації, тенденції // Укр. Часопис прав людини. – 1995. - № 1. – С. 14-22.

[108]. Загальна декларація прав людини. — К.: Право, 1995.

[109]. Міжнародний пакт про громадянські та політичні права і Факультативний проокол № 1 до Міжнародного пакут про громадянські та політичні права. — К.: Право, 1995.

[110]. Конвенція ООН про права дитини 1989 року, схвалена на 44-й сесії Генеральної Асамблеї ООН (резолюція 44/25 від 20 листопада 1989 року). — ООН A/RES/44/25. — 1989; ратифікована Постановою Верховної Ради Української РСР від 27.02.1991 № 789-XII // Відомості Верховної Ради України. — 1991. — N 13. — Стор. 145.

[111]. Конвенція ООН про захист прав всіх трудящих-мігрантів та членів їхніх родин 1990 року // Права людини і професійні стандарти для юристів в документах міжнародних організацій. — 1996 р.

[112]. Конвенція про захист прав людини та основних свобод. Із поправками, внесеними відповідно до положень Протоколу №11. Офіційний переклад МЗС України та Української правничої фундації. — К.: УПФ. — 31 с.

[113]. Дженіс М., Кей Р., Бредлі Е. Європейське право у галузі прав людини: джерела і практика застосування. Пер. з англ. — К.: “АртЕк”, 1997. — С. 251.

[114]. Доповідь Європейської Комісії з прав людини по справі Ван Остервійк проти Бельгії. — 1979.

[115]. *Burghartz v. Switzerland* (1994). — Publications of the European Court of Human Rights. — Ser. A. — No. 280-B (надалі: "ECHR").

[116]. *N v. Sweden* (1986). — Decisions and Reports of the European Commission of Human Rights. — No. 11366/85, 50. — DR. 173 (надалі: "Decisions and Reports").

[117]. *McFeeley v. United Kingdom* (1980). — Decisions and Reports. — No. 8317/78, 20. — DR 44.

[118]. *Niemietz v. Germany* (1992). — ECHR. — Ser. A. — No. 251-B.

[119]. *X and Y v. Netherlands* (1985). — ECHR. — Ser. A. — No. 91.

[120]. *Dudgeon v. United Kingdom* (1981). — ECHR. — Ser. A. — No. 45

[121]. *B v. France* (1992). — ECHR. — Ser. A. — No. 232-C.

[122]. *Rayner v. United Kingdom* (1986). — Decisions and Reports. — No. 9310/81, 47 — DR. 5).

[123]. *Lopes Ostra v. Spain* (1994). — ECHR. — Ser. A. — No. 303-C.

[124]. *Z v. Finland* (1997). — Reports of Judgements and Decisions. — 1997. — No. 1

[125]. Цивільний кодекс України: Офіц. видання. – К.: Видавничий Дім "Ін Юре", 2003. – 664 с.

[126]. Указ Президії Верховної Ради Української РСР "Про ратифікацію Міжнародного пакту про економічні, соціальні і культурні права та Міжнародного пакту про громадянські і політичні права" від 19 жовтня 1973 р. — N 2148 - VIII.

[127]. Recommendation 4/99 on the inclusion of the fundamental right to data protection in the European catalogue of fundamental rights adopted on 7 September 1999. — The Working Party on the Protection of Individuals with regard to the Processing of Personal Data. — Brussels. — 1999.

[128]. Charter of Fundamental Rights of the European Union // Official Journal. — 2000. — C 364. — P. 1-22.

[129]. Конвенція Ради Європи No. 108 “Про захист осіб стосовно автоматизованої обробки персональних даних” // Пазюк А.В. Захист прав людини стосовно обробки персональних даних: міжнародні стандарти. — К.: МГО Прайвесі Юкрейн, 2000. — 88 с.

[130]. Директива 95/46 СЕ Європейського Парламенту і Ради “Про захист фізичних осіб стосовно автоматизованої обробки персональних даних та безперешкодного руху цих даних” // Пазюк А.В. Захист прав людини стосовно обробки персональних даних: міжнародні стандарти. — К.: МГО Прайвесі Юкрейн, 2000. — 88 с.

[131]. *Z v. Finland* (1997). — Reports of Judgments and Decisions. — 1997. — № 1.

[132]. Privacy and Human Rights 2000: An International Survey of Privacy Laws and Developments. — EPIC. — 2000. — P. 1.

[133]. *Olmstead v. United States* (1928). — 277 U.S. — 438.

[134]. *Katz v. United States* (1967). — 389 U.S.

[135]. *Griswold v. Connecticut* (1965). — 381 U.S. — 479.

[136]. *Rees v. United Kingdom* (1986). — ECHR. — Ser. A. — No. 106.

[137]. Defining Defamation: Principles on Freedom of Expression and Protection of Reputation. Comment on Principle 8. — ARTICLE 19. — London: UNESCO, 2000.

[138]. М. Місьо, Н.Петрова. Українське законодавство і захист преси. // Свобода висловлювань і приватність. — 2000. — № 1-2. — С. 3.

[139]. *Lingens v. Austria* (1989). — Reports of Judgments and Decisions. — 1989. — Ser. A. — No. 103. — P. 41.

[140]. *Oberschlick v. Austria* (1995). — Reports of Judgments and Decisions. — 1995. — Ser. A. — No. 313.

[141]. *Bruggemann and Scheuten v. the Federal Republic of Germany* (1977). — Decisions and Reports. — No. 6959/75.

[142]. *Silver and Others v. United Kingdom* (1983). — Judgements and Decisions. — Ser. A. — No. 61.

[143]. Lord Bingham of Cornhill. The Way We Live Now: Human Rights in the New Millennium. — 1998.

[144]. *Gaskin v. UK* (1989). — Reports of Judgments and Decisions. — 1989. — Series A. — No. 160.

[145]. *U.S. West, Inc. v. Federal Communications Commission, and United States of America*. — US Court of Appeals. — Tenth Circuit. — No. 98-9518. — Washburn University School of Law. — 1999.

[146]. Fight Against Organized Crime and Control of Personal Data // European Commission Falcone Programme Project. — Rome: 2000. — P. 223-241.

[147]. Определение Конституционного Суда РФ от 14 июля 1998 года по делу о проверне конституционности отдельных полонений Федерального закона "Об оперативно-розыскной деятельности" по жалобе гражданки И.Г.Черновой / Пазюк А.В. Захист прав громадян у зв'язку з обробкою персональних даних у правоохоронній діяльності: європейські стандарти і Україні. — К.: МГО Прайвесі Юкрейн, 2001. — С. 213-256.

[148]. Пазюк А.В. Захист прав громадян у зв'язку з обробкою персональних даних у правоохоронній діяльності: європейські стандарти і Україні. — К.: МГО Прайвесі Юкрейн, 2001. — 258 с.

[149]. Governing global networks: international regimes for transportation and communications / Mark W. Zacher, Brent A. Sutton. – Cambridge University Press. – 1996. – 299 p.

[150]. Иванский В.П. Теоретические проблемы правовой защиты частной жизни в связи с использованием информационных технологий: Дис... канд. юрид. наук: 12.00.01. — М., 1998. — С. 31.

[151]. Declaration on mass media and human rights adopted by the Parliament Assemble Resolution N 428// Strasbourg: Council of Europe. — 1970.

[152]. Right to privacy: Committee on Legal Affairs and Human Rights Report (Doc. 8130, 3 June 1998) // Strasbourg: Council of Europe. — 1998.

[153]. Recommendation Data Protection law and the media. — The Working Party on the Protection of Individuals with regard to the Processing of Personal Data. — Brussels. — 1997. — P. 4.

[154]. Международная конвенция о пресечении обращения порнографических изданий и торговли ими (Женева, 12 сентября 1923 года) / Сборник действующих договоров, соглашений и конвенций, заключенных СССР с иностранными государствами. - Вып. IX. - М., 1938.

[155]. Международная конвенция об использовании радиовещания в интересах мира // Ведомости Верховного Совета СССР. – 1983.- № 16.

[156]. Резолюция 110 (II) Генеральной Ассамблеи ООН “Меры, которые должны быть приняты против пропаганды и поджигателей новой войны” / Организация Объединенных Наций. Официальные отчеты второй сессии Генеральной Ассамблеи. – 1947. - A/519. - С. 12.

[157]. Резолюция 127 (II) Генеральной Ассамблеи ООН “Ложная или извращенная информация” / СССР и международное сотрудничество в области прав человека. Документы и материалы.- М.: “Международные отношения”, 1989.

[158]. Міжнародна конвенція про ліквідацію всіх форм расової дискримінації // Відомості Верховної Ради УРСР. - 1969. - № 5. - Ст.27.

[159]. Резолюция 2037 (XX) Генеральной Ассамблеи ООН Декларация о распространении среди молодежи идеалов мира, взаимного уважения и взаимопонимания между народами 1965 г. / СССР и международное сотрудничество в области прав человека. Документы и материалы.- М.: "Международные отношения", 1989.

[160]. Декларация об основных принципах, касающихся вклада средств массовой информации в укрепление мира и международного взаимопонимания, в развитие прав человека и в борьбу против расизма и апартеида и подстрекательства к войне / СССР и международное сотрудничество в области прав человека. Документы и материалы.- М.: "Международные отношения", 1989.

[161]. Международное право: Учебник для обуч. по спец. "Правоведение (междунар. право)", "Междунар. отношения", и "Междунар. экон. отношения" / Дипломатическая академия МИД РФ; Московский гос. ин-т международных отношений (ун-т) МИД РФ / Ю.М. Колосов (отв.ред.), В.И. Кузнецов (отв.ред.). — 2.изд., доп. и перераб. — М. : Междунар. отношения, 1998. — 624с.

[162]. Mayer-Schönberger. Generational Development of Data Protection in Europe // Technology and Privacy: The New Landscape; Ed. Philip E. Agre, Marc Rotenberg. — Cambridge: The MIT Press, 1997. — P. 224.

[163]. Davies S.G. Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity // Technology and Privacy: The New Landscape; Ed. Philip E. Agre, Marc Rotenberg. — Cambridge: The MIT Press, 1997. — P. 150-152.

[164]. Flaherty D.H. Controlling Surveillance: Can Privacy Protection Be Made Effective? // Technology and Privacy: The New Landscape; Ed. Philip E. Agre, Marc Rotenberg. — Cambridge: The MIT Press, 1997. — P. 171.

[165]. Recomendation # 1/99 On Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware adopted by the Working Party on 23 February 1999. — The Working Party on the Protection of Individuals with regard to the Processing of Personal Data. — Brussels: European Union, 1999.

[166]. Green Paper “On the Protection of Minors and Human Dignity in Audiovisual and Information Services”. — Brussels: European Union, 1996. — COM (96). — P. 487.

[167]. Standardization and the Global Information Society: The European Approach. Communication from the Commission to the Council and the Parliament. — Brussels: European Union, 1996. — COM (96). — P. 359.

[168]. Hes R., Borking J. Privacy Enhancing Technologies: the Path to Anonymity. — The Hague. — 1998.

[169]. Recomendation EU Anonymity on the Internet adopted by Working Party on 3 December 1997. — The Working Party on the Protection of Individuals with regard to the

Processing of Personal Data. — Brussels: European Union, 1997.

[170]. Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country? — The Working Party on the Protection of Individuals with regard to the Processing of Personal Data. — Brussels: European Union, 1998.

[171]. Kirby M. D. Privacy Protection — A New Beginning. — Hong Kong. — 1999 – 15 p.

[172] Okinawa Charter on Global Information Society. — Okinawa, 2000.

[173]. Dempsey J., Weitzner D. Regardless of Frontiers: Protecting Human Right to Freedom of Expression on the Global Internet. – Washington: Center for Democracy and Technologies, 1998. – 38 p.

[174]. Указ Президиума Верховного Совета СССР от 12 августа 1988 года «О ратификации о распространении несущих программы сигналов, передаваемых через спутники» // Ведомости Верховного Совета СССР. - 1988. - № 34. - Ст. 550.

[175]. Закон України “Про ратифікацію Статуту і Конвенції Міжнародного союзу електрозв'язку” // Відомості Верховної Ради України. - 1994. - № 33. - Ст. 306.

[176]. Рекомендації Ради Організації Економічного Співробітництва і Розвитку стосовно Керівних принципів, що регулюють захист приватності і транскордонні потоки персональних даних // Пазюк А.В. Захист прав людини стосовно обробки персональних даних: міжнародні стандарти. — К.: МГО Прайвесі Юкрейн, 2000. — 88 с.

[177]. First Report On the Implementation of the Data Protection Directive (95/46/EC). – Brussels: Commision of the European Communities, 2003. – COM (2003) 265 final.

[178]. Michael J. Privacy and Human Rights. — Paris: UNESCO, 1994. — P. 35.

[179]. Recommendation No. Rec(81)1 of the Committee of Ministers to member states on regulations for automated medical data banks (adopted by the Committee of Ministers on 23 January 1981 at the 328th meeting of the Ministers' Deputies). — Council of Europe, 1981.

[180]. Recommendation No. Rec(97)5 of the Committee of Ministers to member states on the protection of medical data (adopted by the Committee of Ministers on 13 February 1997 at the 584th meeting of the Ministers' Deputies). — Council of Europe, 1997.

[181]. Recommendation No. Rec(83)10 of the Committee of Ministers to member states on the protection of personal data used for scientific research and statistics (adopted by the Committee of Ministers on 23 September 1983 at the 362nd meeting of the Ministers' Deputies). — Council of Europe, 1983.

[182]. Recommendation No. Rec(85)20 of the Committee of Ministers to member states on the protection of personal data used for the purposes of direct marketing (adopted by the Committee of Ministers on 25 October 1985 at the 389th meeting of the Ministers' Deputies). — Council of Europe, 1985.

[183]. Recommendation No. Rec(86)1 of the Committee of Ministers to member states on the protection of personal data used for social security purposes (adopted by the Committee of Ministers on 23 January 1986 at the 392nd meeting of the Ministers' Deputies). — Council of Europe, 1986.

[184]. Recommendation No. R (87) 15 of the Committee of Ministers to member states on the protection of personal data used in the police sector (adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies). — Council of Europe, 1987.

[185]. Recommendation No. R (89) 2 of the Committee of Ministers to member states on the protection of personal data used for employment purposes (adopted by the Committee of Ministers on 18 January 1989 at the 423rd meeting of the Ministers' Deputies). — Council of Europe, 1989.

[186]. Recommendation No. R (90) 19 of the Committee of Ministers to member states on the protection of personal data used for payment and related operations (adopted by the Committee of Ministers on 13 September 1990, at the 443rd meeting of the Ministers' Deputies). — Council of Europe, 1990.

[187]. Recommendation No. R (95) 4 of the Committee of Ministers to member states on the protection of personal data collected and processed in the area of telecommunication services, with particular reference to telephone services (adopted by the Committee of Ministers on 7 February 1995 at the 528th meeting of the Ministers' Deputies). — Council of Europe, 1995.

[188]. Recommendation No. R (97) 18 of the Committee of Ministers to member states on the protection of personal data collected and processed for statistical purposes (adopted by the Committee of Ministers on 30 September 1997 at the 602nd meeting of the Ministers' Deputies). — Council of Europe, 1997.

[189]. Recommendation No. R (91) 10 of the Committee of Ministers to member states on the communication to third parties of personal data held by public bodies (adopted by the Committee of Ministers on 9 September 1991 at the 461st meeting of the Ministers' Deputies). — Council of Europe, 1991.

[190]. Recommendation No. Rec(99)5 of the Committee of Ministers to member states on the protection of privacy on the Internet (adopted by the Committee of Ministers on 23 February 1999 at the 660th meeting of the Ministers' Deputies). — Council of Europe, 1999.

[191]. Recommendation No. Rec(2002)9 of the Committee of Ministers to member states on the protection of personal data collected and processed for insurance purposes (adopted by the Committee of Ministers on 18 September 2002 at the 808th meeting of the Ministers' Deputies). — Council of Europe, 2002.

[192]. David Wolstenholme. Police Requirements and Practices in the Information Society 'The case in the United Kingdom' // ADACS/DGI (2000) 3 Sem.: Data protection in Police Sector. Council of Europe Regional Seminar under the activities for the development and consolidation of democratic stability. — Strasbourg. — Council of Europe. — 2000.

[193]. The introduction and use of personal identification numbers: the data protection issues / Study prepared by the Committee of experts on data protection (CJ-PD). — Council of Europe, 1991.

[194]. Model Contract to ensure equivalent protection in the context of transborder data flows with explanatory report / Stude made jointly by the Council of Europe, the Commission of the European Communities and the International Chamber of Commerce. — Council of Europe. — Strasbourg, 1992.

[195]. Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal data, adopted by the Council 23 September 1980. — Paris: OECD, 1981.

[196]. Declaration on Transborder Data Flows — OECD. — Paris: OECD, 1985.

[197]. Recommendation of the Council concerning Guidelines for the Security of Information Systems — Paris: OECD, 1992.

[198]. Guidelines for Cryptography Policy — Paris: OECD, 1997.

[199]. OECD Ministerial Declaration on Privacy on Global Networks // I-Ways. — 1998.— 4th Quarter. — P. 48.

[200]. Guidelines for the Regulation of Computerized Personal Data Files, adopted by General Assembly resolution 45/95 of 14 December 1990 // Human Rights: A Compilation of International Instruments, Vol. I (Second Part). — New York and Geneva: Centre for Human Rights, Geneva, 1994. — P. 540-543.

[201]. Chapter of Fundamental Rights of the European Union // Official Journal of the European Communities. — 2000. — C. 364 — P. 10.

[202]. Шевчук С., Кравчук І Ніццький договір та розширення ЄС / Центр порівняльного права / С. Шевчук (наук.ред.), А. Пендак (пер.). — К.: Логос, 2001. — 195с.

[203]. Council Resolution on a Community policy on data processing // Official Journal. — 1974. — C. 086.

[204]. Commission Recommendation relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data // Official Journal. — 1981. — L 246.

[205]. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data // Official Journal. — 1995. — L 281. — P. 31-50.

[206]. Regan Priscilla M. American Business and the European Data Protection Directive: Lobbying Strategies and Tactics // Visions of Privacy: Policy Choices for the Digital Age; Ed. By Colin J. Bennett, Rebecca Grant. — Toronto. — P. 204.

[207]. Recommendation 1/2000 on the Implementation of Directive 95/46/EC adopted on 3rd February 2000. — The Working Party on the Protection of Individuals with regard to the Processing of Personal Data. — Brussels. — 2000.

[208]. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector // Official Journal. — 1998. — L 024. — P. 1-8.

[209]. Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware adopted on 23 February 1999. — The Working Party on the Protection of Individuals with regard to the Processing of Personal Data. — Brussels. — 1999.

[210]. Recommendation on the Respect of Privacy in the context of Interception of Telecommunications adopted on 3 May 1999. — The Working Party on the Protection of Individuals with regard to the Processing of Personal Data. — Brussels. — 1999.

[211]. Opinion 1/2000 on certain data protection aspects of electronic commerce adopted on 3rd February 2000. — Article 29 Data Protection Working Party. — Brussels. — 2000.

[212]. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) // Official Journal. — 2002. — L 201. — P. 37-47.

[213]. України і Шенген: приватний вимір європейського вибору. — Київ: Центр миру, конверсії та зовнішньої політики України, 2001. — 67 с.

[214]. Dumortier Jos. The Protection of Personal Data in the Schengen Convention // International Review of Law Computers and Technology, Cambridge. — 1997. — March. — Vol. 11. — No. 1. — P. 93-106.

[215]. Salberini Giuliano. L'Integrazione Europea e il trattamento dei dati personali // Affari Esteri, Roma. — 1996. — Aprile. — Anno 28. — No. 110. — P. 411-423.

[216]. Corrado Laura. L'attuazione della Convenzione di Schengen in Italia // Affari Esteri, Roma. — 1997. — Ottobre. — Anno 29. — No. 116. — P. 847-860.

[217]. Janer Torrens, Joan David. La proteccion de los particulares en el ambito del Convenio Europol (reflexiones con motivo de su entrada en vigor) // Gaceta Juridica De La CE. Boletin, Madrid. — 1999. — Enero - Febrero. — No. 140. — P. 15-26.

[218]. Zerdick Thomas. European Aspects of Data Protection: What Rights for the Citizen? // Legal Issues of European Integration, Deventer. — 1995. — No. 2. — P. 59-86.

[219]. Fight Against Organized Crime and Control of Personal Data // European Commission Falcone Programme Project. — Rome: 2000. — 288 p.

[220]. Stephen Kabera Karanja. The Schengen Co-operation: Consequences for the right of EU Citizens. — 2000.

[221]. Data protection in Police Sector. Council of Europe Regional Seminar under the activities for the development and consolidation of democratic stability // ADACS/DGI (2000) 3 Sem. — Strasbourg: 2000.

[222]. Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty of European Union the Convention on Mutual Assistance in Criminal Matters between the member States of the European Union // Official Journal of the European Communities. — 2000. — C. 197.

[223]. Council Decision of 14 December 2000 setting up a Provisional Judicial Cooperation Unit // Official Journal of the European Communities. — 2000. — L 324.

[224]. EU agrees principles for Eurojust // EUobserver.com. — 2001. — September 28.

[225]. *Z v. Finland* (1997). — Reports of Judgments and Decisions. — 1997. — I. — P. 347-348.

[226]. Council Decision of 17 October 2000 establishing a secretariat for the joint supervisory data protection bodies set up by the Convention on the Establishment of a European Police Office (Europol Convention), the Convention on the Use of Information Technology for Customs Purposes and the Convention implementing the Schengen Agreement on the gradual abolition of checks at the common borders (Schengen Convention) // Official Journal of the European Communities. — 2000. — L 271. — P. 1-3.

[227]. Bennett C.J. Implementing Privacy Codes of Practice: A Report to the Canadian Standards Association. — Rexdale: CSA, 1995.

[228]. Canadian Standards Association Model Code for the Protection of Personal Information. CAN/CSA-Q830-96. — Rexdale: CSA, 1996.

[229]. Reidenberg J.R. Resolving Conflicting International Data Privacy Rules in Cyberspace // Stanford Law Review. — 2000. — Vol. 52. — P. 1359.

[230]. Standardization and the Global Information Society: The European Approach. Communication from the Commission to the Council and the Parliament. — Brussels: European Union, 1996. — COM (96). — P. 359.

[231]. Initiative on Privacy Standardisation in Europe: Final Report. — Brussels: CEN/ISSS, 2002. — 87 p.

[232]. Opinion 1/2002 on the CEN/ISSS Report on Privacy Standardisation in Europe adopted on 30 May 2002 by Data Protection Working Party. — Brussels. — 2002.

[233]. OECD Ministerial Declaration on Privacy on Global Networks // I-Ways. — 1998.— 4-th Quarter. — P. 48.

[234]. R. Doray. A Word from the President of the Conference // Privacy: the New Frontier. Program Book of Abstracts from the International Conference on Privacy. — Montreal, Quebec: 1997. — P. 5.

[235]. Model Contract to ensure equivalent protection in the context of transborder data flows with explanatory report / Stude made jointly by the Council of Europe, the Commission of the European Communities and the International Chamber of Commerce.

— Council of Europe. — Strasbourg, 1992.

[236]. Dix A. Berlin DPA supervises German Railway and Citibank TBDF contract // Privacy Laws and Business Newsletter. — 1996. — No 37. — P. 6-10.

[237]. Dix A. Case Study: North America and the European Directive. The German Railway Card: A Model contractual solution of the 'adequate level of protection' issue? // 18th International Privacy and data Protection Conference 'Privacy beyond Borders'. — Ottawa: 1996. — 6 p.

[238]. Commission Decision Pursuant to Directive 95/46/EC of the European Parliament and of the Council on Standard Contractual Clauses for the transfer of personal data to third countries under article 26 (4) of Directive 95/46/EC / Draft Version 27 March 2001.

[239]. Kotschy W. Model Contracts for securing data protection in cases of transborder data flow to countries without adequate data protection // 22nd International Conference on Privacy and Data Protection. — Venice: 2000. — 8 p.

[240]. Transborder Data Flow contracts in the Wider Framework of Mechanisms for Privacy Protection on Global Networks // Working Party on Information Security and Privacy; Directorate for Science, Technology and Industry; Committee for Information, Computer and Communications Policy; OECD: 1999. — DSTI/ICCP/REG(99)15/FINAL. — P. 26 (47)

[241]. Commission Decision Pursuant to Directive 95/46/EC of the European Parliament and of the Council on Standard Contractual Clauses for the transfer of personal data to third countries under article 26 (4) of Directive 95/46/EC / Draft Version 27 March 2001.

[242]. Safe Harbor Privacy Principles issued by the U.S. Department of Commerce on July 21, 2000. — Brussels: The U.S. Mission to the European Union, 2000.

[243]. *Hessisches Datenschutzgesetz*. — 1970. — GVBl. — I.

[244]. *Law Against the misuse of data*. — 1974. — GVBl.

[245]. *Datalag* (Swedish Data Act). — 1973.

[246]. Act No. 78-17 on Data Processing, Data Files and Individual Liberties. — 1978.

[247]. Datenschutzgesetz (Law on the protection of personal data). — 1978. — BGBl.

[248]. Danish Private Registry Etc. Act. — 1978.

[249]. Norwegian Data Protection Act. — 1978. — No. 48.

[250]. Decision of the First Senate (1983). — 1 BvR. — 209/83—NJW.

[251]. German Federal Data Protection Act. — 1990.

[252]. Henkilorekisterialaki (Finish Persons Register Act). — 1987. — 471—HE. — 49/86.

[253]. *Eleventh Report of the Data Protection Registrar*. — 1995. — HC 629.

[254]. Raab Ch. D. From Balancing to Steering: New Directions for Data Protection / Visions of Privacy: Policy Choices for the Digital Age; Ed. Bennett C.J., Grant R. — University of Toronto Press, 1999. — P. 73.

[255]. Additional Protocol to the Convention No 108. — Council of Europe Press: Strasbourg, 2000.

[256]. Swiss Data Protection Act. — 1992.

[257]. Rotenberg M. Preface to first edition //The Privacy Law Sourcebook 2001. — Washington: EPIC, 2001.

[258]. United States Right to Financial Privacy Act of 1978. — 12 USC. — No. 3401.

[259]. United States Privacy Protection Act of 1980. — Public Law. — No. 96-440.

[260]. United States Electronic Communications Privacy Act of 1986. — Public Law. — 99-508. — 100 Stat. — No. 1848-73.

[261]. United States Privacy Act of 1974. — 5 U.S.C. — No. 552a.

[262]. United States Video Privacy Protection Act of 1988. — Public Law. — No. 100-618.

[263]. United States Telephone Consumer Protection Act of 1991. — Public Law. — No. 102-243.

[264]. United States Federal Trade Commission Act of 1914. — 15 U.S.C. — No. 45(a).

[265]. FTC & Liberty Financial Companies, Inc. Agreement. — 1999. — File No. 982 — 3522.

[266]. Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country? — Working Document. — Brussels: Data Protection Working Party, 1999.

[267]. Canadian Personal Information and Electronic Documents Act. — 2000.

[268]. Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act. — Brussels: Data Protection Working Party, 2001.

[269]. Australian Privacy Amendment (Private Sector) Act. — 2000.

[270]. Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000. — Brussels: Data Protection Working Party, 2001.

[271]. Історія української Конституції / Упор. А.Г. Слюсаренко, М.В. Томенко. — К.: Право. 1997. — С. 319.

[272]. Конституція України // Відомості Верховної Ради України. — 1996. — № 30. — Ст. 141.

[273]. Конституції нових держав Європи та Азії / Упор. С. Головатий. — К.: Укр. Правн. Фундація. Вид-во "Право", 1996. — 544 с.

[274]. *Gaskin v. UK* (1989). — Reports of Judgments and Decisions. — 1989. — Series A. — No. 160. — P. 20.

[275]. Закон України "Про інформацію" від 2 жовтня 1992 р. // Голос України. — 1992, 21 травня.

[276]. Закон України "Про свободу совісті та релігійні організації" від 23 квітня 1991 року N 987-XII // Відомості Верховної Ради. — 1991. — N 25. — Ст.283.

[277]. Закон України "Про адвокатуру" від 19 грудня 1992 р. № 2887-XII // Відомості Верховної Ради. — 1993. — N 9. — Ст. 62.

[278]. Закон України "Про захист інформації в автоматизованих системах" від 5 липня 1994 р. // Відомості Верховної Ради. — 1994. — № 31. — Ст. 286.

[279]. Закон України "Про оперативно-розшукову діяльність" від 18.02.1992 № 2135-XII // Відомості Верховної Ради. — 1992. — N 22. — Ст. 303.

[280]. Закон України "Про розвідувальні органи України" від 22 березня 2001 р. // Відомості Верховної Ради. — 2001. — № 19. — Ст. 94.

[281]. Закон України "Про рекламу" від 3 липня 1996 р. // Відомості Верховної Ради. — 1996. — № 39. — Ст. 181.

[282]. Закон України “Основи законодавства України про охорону здоров’я” від 19.11.1992 № 2801-XII // Відомості Верховної Ради. — 1993. — N 4. — Ст. 19.

[283]. Закон України “Про телебачення і радіомовлення” від 21 грудня 1993 р. // Відомості Верховної Ради. — 1994. — № 10. — Ст. 43.

[284]. Постанова Кабінету Міністрів України від 04.06.1998 року № 794 “Про персоніфікований облік у системі пенсійного забезпечення” Офіційний вісник України. — N 22. — Ст. 37.

[285]. Наказ МВС, Міністерства охорони здоров’я, Комітету про запобіганню захворюванням на СНІД від 18 травня 1997 року “Про затвердження Положення про порядок проведення медичного обстеження на ВІЛ засуджених до позбавлення волі” (втратив чинність) // Офіційний вісник України. — 1997. — N 26. — Ст. 59.

[286]. Тодика Ю., Серьогін В. Конституційний принцип гласності як гарантія основних прав і свобод громадян // Право України. — 1998.— № 6.— С. 22-24.

[287]. Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України "Про інформацію" та статті 12 Закону України "Про прокуратуру" (справа К.Г.Устименка) від 30 жовтня 1997 року // Офіційний вісник України. – 1997. - № 46. - Ст. 126.

[288] Словник іншомовних слів / За ред. О.С. Мельничука. – К.: 1974. – 774 с.

[289]. Модельный закон «О персональных данных» // Информационный бюллетень (Межпарламентская Ассамблея государств-участников Содружества Независимых Государств). — 1999. — № 23.

[290]. Закон України від 18.01.2001 № 2246-III Про внесення змін до Закону України “Про оперативно-розшукову діяльність” // Відомості Верховної Ради України. — 2001. — N 14. — Ст. 72.

[291]. Наказ Голови Служби безпеки України

[292]. Кримінальний кодекс Української РСР від 28 грудня 1960 року // Відомості Верховної Ради УРСР. — 1961. — № 2. — Ст. 14.

[293]. Кримінальний кодекс України: Офіц. видання. — К.: Видавничий Дім “Ін Юре”, 2001. — 336 с.

[294]. Постанова Верховної Ради України “Про Засади державної політики України в галузі прав людини” від 17 червня 1999 року // Відомості Верховної Ради. — 1999. — N 35. — Ст. 303.

[295]. Указ Президента України “Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року “Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України” // Офіційний вісник України . — 2001. — N 50. — Ст. 28.

[296]. Закон України “Про ратифікацію Угоди про партнерство і співробітництво між Україною і Європейськими Співтовариствами і їх державами членами” від 10 листопада 1994 року N 237/94-вр // Відомості Верховної Ради. — 1994. — N 46. — Ст. 415.

[297]. Лойтен П. Зобов’язання України у сфері зовнішньої торгівлі, що випливають з Угоди про партнерство і співробітництво, умв членства в СОТ // Український правовий часопис. – 1998. – № 2. – С. 7-17.

[298]. Муравйов В. Положення Угоди про партнерство та співробітництво, які регулюють сферу підприємництва та інвестицій (питання імплементації) // Український правовий часопис. – 1998. – № 2. – С. 31-34.

[299]. Прокопенко Є. Зобов’язання України та ЄС у сфері конкуренції згідно Угоди про партнерство та співробітництво // Український правовий часопис. – 1998. – № 2. – С. 35-40.

[300]. Забігайло В.К. Право України в контексті його апроксимації до права Європейського Союзу // Українсько-європейський журнал міжнародного та порівняльного права. – Том. 1. Випуск 1. Осінь 2000. – С. 9.

[301]. Задорожній О.В., Гнатовський М.М. Правова система України в Європейському правовому просторі // Український часопис міжнародного права. – 2002. - №2. – С. 29-32.

[302]. Указ Президента України “Про затвердження стратегії інтеграції України до Європейського Союзу” від 11 червня 1998 року № 615/98 // Офіційний вісник України. — 1998. — N 24. — С. 3.

[303]. Задорожній О.В., Гнатовський М..М. Адаптація законодавства України до законодавства Європейського Союзу: парламентський вимір // Законодавство України: проблеми вдосконалення. Збірник наукових праць Інституту законодавства Верховної Ради України. – Випуск 7. – К., 2001. – С. 56-63.

[304]. First orientations on Transfers of Personal Data to Third Countries — Possible Ways Forward in Assessing Adequacy (D/5020/97). — Brussels: European Commission, DG XV, Working Party on the Protection of Individuals With Regard to the Processing of Personal Data, 1997. — P. 4.

[305]. Opinion 6/99 concerning the level of personal data protection in Hungary adopted on 7 September 1999 by Data Protection Working Party. — Brussels. — 1999.

[306]. Majtenyi L. The Cause of Data Protection in East Central Europe. — 2000. — P. 1-2.

[307]. Тодика Ю., Серьогін В. Вдосконалення законодавства про інформацію з обмеженим доступом — вимога сьогодення // Вісник Академії правових наук України. — 1999. — № 4. — С. 42-49.

[308]. Костецька Т.А. Право на інформацію в Україні. — К.: Вища школа права при Інституті держави і права ім.. В.М. Корецького, 1998. — С. 9-10.

[309]. Закон України “Про Національну програму інформатизації” від 4 лютого 1998 р. // Відомості Верховної Ради України. — 1998. — № 27-28. — Ст. 181.

[310]. Закон України “Про Концепцію Національної програми інформатизації” від 4 лютого 1998 р. // Відомості Верховної Ради України. — 1998. — № 27-28. — Ст. 182.

[311]. *Malone vs. the United Kingdom* (1984). — Judgments and Decisions. — Series A. — No. 82.

[312]. *Amann v. Swiss* (2000). — ECHR 2000-II. — No. 27798/95.