Науково-дослідний інститут інформатики і права
Національної академії правових наук України

Національний інститут стратегічних досліджень

Секретаріат Уповноваженого Верховної Ради України
з прав людини

Факультет соціології і права
Національного технічного університету України
«Київський політехнічний інститут»

ПРОБЛЕМИ ЗАХИСТУ ПРАВ ЛЮДИНИ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

МАТЕРІАЛИ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ
01 квітня 2016 року

Київ – 2016

УДК 34:004](063)+342.72/.73:[316.42:004](063)
ББК 67.404.3я43+67.400.7я43
П68

Проблеми захисту прав людини в інформаційному суспільстві : матеріали наук.-практ. конф. / 1 квітня 2016 р., м. Київ / Упорядн. : В. М. Фурашев, С. Ю. Петряєв. – К. : НДІІП НАПрН України, Національний інститут стратегічних досліджень, Секретаріат Уповноваженого Верховної Ради України з прав людини, НТУУ «КПІ» Вид-во «Політехніка», 2016. – 150 с. – 100 пр.

Подано матеріали з актуальних питань проблем захисту прав людини в інформаційному суспільстві. Доповіді учасників конференцій, що опубліковані у збірнику, можуть бути корисними для вчених, фахівців та експертів інформаційної сфери, науково-педагогічних працівників, аспірантів, докторантів, студентів вищих навчальних закладів, а також усіх, хто цікавиться сучасними суспільно-правовими проблемами розвитку інформаційного суспільства, а також проблемами захисту прав людини в інформаційному суспільстві.

Організаторами заходу виступили: Навчально-науковий центр інформаційного права та правових питань інформаційних технологій ФСП НТУУ «КПІ», Науково-дослідний інститут інформатики і права НАПрН України, Національний інститут стратегічних досліджень, а також Секретаріат Уповноваженого Верховної Ради України з прав людини. Участь у конференції взяли провідні експерти і вчені наукових установ і навчальних закладів України, представники зацікавлених державних органів та громадських організацій. Інформаційну підтримку у проведенні заходу надали: журнали «Інформація і право», «Правова інформатика», «Теорія і практика», «Інформація та безпека» та Вісник НТУУ «КПІ» «Політологія. Соціологія. Право».

Матеріали викладено в авторській редакції.

***Упорядники*: Фурашев В. М., Петряєв С. Ю.**

Оформлення обкладинки:
Лабораторія технічної естетики та дизайну ФСП НТУУ «КПІ» (designlab.kpi.ua@gmail.com)
Балашов Д. В. (balashov.dim@gmail.com)

Рекомендовано до друку
Вченою радою Науково-дослідного інституту інформатики і права
Національної академії правових наук України
Протокол № 5 від 04.05.2016 р.
Вченою радою факультету соціології і права Національного технічного
Університету України «Київський політехнічний інститут»
Протокол № 9 від 25.04.2016 р.

ISBN 978-966-622-765-5

З М І С Т

В. Г. Пилипчук,
д.ю.н., професор, член-кореспондент
Національної академії правових наук України,
заслужений діяч науки і техніки України

АКТУАЛЬНІ ПИТАННЯ ЗАХИСТУ ПРАВ, СВОБОД І БЕЗПЕКИ ЛЮДИНИ В СУЧАСНОМУ ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

За останні роки в Українському суспільстві значно змінилося розуміння важливості проблем становлення інформаційного суспільства, розвитку інформаційної сфери та необхідності забезпечення інформаційної безпеки. На державному рівні у цій сфері вжито низку правових, організаційних та інших заходів.

Водночас, як свідчить аналіз, система захисту прав, свобод і безпеки людини в умовах інтенсивного розвитку інформаційних технологій, інформаційних ресурсів, продукції і послуг залишається далекою від ідеальної та потребує суттєвих трансформацій.

Враховуючи зазначене звернімо увагу на низку актуальних проблем, що потребують всебічного наукового опрацювання і належного правового забезпечення, зокрема:

1. Проблеми додержання прав людини при формуванні єдиних державних електронних реєстрів:

– при створенні вказаних реєстрів, за нашими оцінками, пріоритет надається принципу публічності, а не пріоритету захисту прав і свобод людини, як базової цінності ЄС;

– реєстри переважно підконтрольні одному відомству – Міністерству юстиції, що не відповідає практиці країн-членів ЄС;

– відсутні належні організаційно-правові механізми захисту відомостей стосовно громадян України, що містяться у державних реєстрах;

– не відпрацьовано спеціальний режим доступу до відомостей у цих реєстрах, які стосуються військовослужбовців і працівників сектору безпеки, у т.ч. звільнених у запас чи відставку, та членів їх сімей;

– повна відкритість державних реєстрів, як свідчить аналіз, може створювати реальні та потенційні загрози національній безпеці України;

– відкритий доступ до узагальнених відомостей про громадян та їхнє майно може використовуватись злочинними організаціями, групами і особами та створювати реальні загрози правам і безпеці громадян.

2. Проблеми захисту персональних даних:

– спостерігається певна тенденція щодо спроб нівелювати право людини розпоряджатися власними персональними даними;

– є спроби використання можливостей ІТ-компаній, сучасних інформаційних технологій та інформаційно-комунікаційних мереж для несанкціонованого збору персональних даних;

– не забезпечено реалізацію «права бути забутим» у мережі Інтернет.

3. Проблеми збору, зберігання та використання біометричних даних громадян:

– при оформленні закордонних паспортів застосовано т.зв. «поліцейську» біометричну систему – збір відбитків пальців людини;

– відсутні ефективні правові механізми забезпечення зберігання вказаних даних і надання до них доступу, у т.ч. третім особам;

– потребують належного врегулювання питання обміну і захисту біометричних даних на міждержавному та міжнародному рівні.

4. Проблеми поширення інформаційної агресії і насильства в національному та глобальному інформаційному просторі, що пов’язані із:

– веденням інформаційної війни проти України, яка поширилась на інші країни світу;

– негативним інформаційно-психологічним впливом на свідомість, застосуванням інформаційних технологій на шкоду життю і здоров’ю людини;

– падінням професійного рівня вітчизняної журналістики та залежністю ЗМІ від фінансово-промислових груп чи партійно-політичних структур;

– активним використанням мережі Інтернет для проведення інформаційних операцій чи компрометації опонентів або конкурентів.

5. Проблеми правової культури та моральності в інформаційній сфері:

– спостерігається тенденція до різкого падіння моральності й поваги до загальнолюдських цінностей при т.зв. «віртуальному» спілкуванні;

– відсутні ефективні правові механізми протидії порушенням прав і свобод людини в мережі Інтернет та ЗМІ;

– обмежені можливості судового захисту честі, гідності чи приватності громадян.

6. Проблеми у сфері доступу громадян до публічної інформації:

– дискусійним залишається визначення понять «публічна інформація» та «службова інформація»;

– потребує удосконалення правове забезпечення доступу громадян до публічної інформації;

– актуальним є питання пошуку балансу між відкритістю і правом людини на доступ до інформації та обмеженням доступу до інформації при захисті законних інтересів суспільства й держави.

Наведені проблеми, за нашими оцінками, є далеко не вичерпними.

За цих умов вкрай актуальним постає питання їх комплексного наукового опрацювання та спільного пошуку шляхів вирішення в інтересах людини, суспільства і держави.

==========***==========

І. В. Арістова,
доктор юридичних наук, професор

СОЦІАЛЬНО-ПРАВОВИЙ МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ ПРАВ ЛЮДИНИ В УМОВАХ РОЗВИТКУ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА: ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ

Моніторинг забезпечення прав людини в Україні дозволив переконатися, що між теорією і практикою прав людини існує певний розрив, а саме: формально визнані, законодавчо закріплені вони реально не завжди одержують втілення в життя, оскільки ними нерідко неможливо скористатися. Вважаємо за необхідне підтримати існуючу точку зору, що така ситуація є показником того, що соціально-правовий механізм забезпечення прав і свобод людини є недостатньо ефективний [1, с. 223]. Усвідомлюючи важливість дослідження усіх аспектів функціонування зазначеного механізму, вважаємо за доцільне акцентувати увагу на окремих теоретико-методологічних засадах формування механізму.
У роботі пропонується визначитися із основними поняттями, сутністю та особливостями використання системного підходу під час дослідження прав людини та соціально-правового механізму їх забезпечення.

Виходячи із того, що у науковій літературі поняття «права людини» та «соціально-правовий механізм» розглядаються як системні утворення, у роботі вважалося за доцільне передусім визначитися із поняттям «система». Слід підкреслити, що відповідно до системного підходу саме «система» постає тим ізоморфним принципом, який проникає через усі кордони, що історично склалися між різними науками [2].

Проведений у роботі аналіз доктринальних досліджень у галузі юриспруденції щодо розуміння понять «система», «правова система», «система права» (наприклад, робота [3, с. 9-60]) дозволив дійти висновку, що усі існуючі визначення поняття «система» є випадковими, не відображають справжніх сутнісних властивостей і тому, звичайно, не є конструктивними, тобто, не допомагають ставити нові, більш масштабні

питання для дослідника. У зв’язку із зазначеним вважалося за можливе запропонувати використання загальної теорії функціональних систем [2] під час проведення наукових досліджень у сфері юриспруденції

Ґрунтуючись на основних засадах загальної теорії функціональних систем, було встановлено доцільність використання під час дослідження соціально-правового механізму забезпечення прав людини в умовах інформаційного суспільства наступного визначення поняття «система»: це сукупність вибірково включених компонентів, у яких взаємодія та взаємовідносини набувають характеру сприяння (рос. взаимосодействия) компонентів на отримання сфокусованого корисного результату [2].

Важливо, що: а) компонент (елемент) системи має певні «ступені свободи» (зв’язки); б) корисні зв’язки завжди підпорядковані досягненню результату (мети) системи; в) некорисні зв’язки усуваються; г) системи функціонують як «ціле» задля досягнення корисного результату; д) результат активно впливає на вибір тих ступенів свободи у компонентів системи, які під час їх інтегрування визначають у подальшому отримання повноцінного результату. Зважаючи на те, що система прав людини і громадянина складається із підсистем (громадянських, політичних, соціально-економічних, культурних, солідарних та пов’язаних з науковими відкриттями в галузі мікробіології, медицини, генетики) прав людини, а також зв’язків між ними, виникає об’єктивна потреба у з’ясуванні корисних зв’язків, які сприяють отриманню корисного результату. На нашу думку, таким корисним результатом (метою) має бути створення необхідних для розвитку людини та громадянина конкретних напрямів діяльності у різних сферах його життя, що закріплені у нормативно-правових актах. Водночас, варто зазначити, що визначення мети формування системи прав людини та громадянина повинно бути пов'язано із функцією, яку ця система реалізує у надсистемі. Абстрактною надсистемою доцільно визнати систему колективних прав суспільства. Що стосується надсистеми у конкретному розумінні, то, з нашої точки зору, це суспільство, зокрема інформаційне.

Констатуючи відсутність усталеного визначення поняття «інформаційне суспільство» (як законодавчого, так і доктринального), у роботі вважалося за доцільне використовувати наступне його визначення. Це громадянське суспільство з розвинутим інформаційним виробництвом і високим рівнем інформаційно-правової культури, в якому ефективність діяльності людей забезпечується розмаїттям послуг, заснованих на інтелектуальних інформаційних технологіях та технологіях зв'язку [4, с. 12]. Акцентовано увагу, що: а) громадянське суспільство і держава – це взаємопов'язані, але відносно самостійні соціальні системи; б) розвинуте інформаційне суспільство є передумовою інформаційної держави [4, с. 12]; в) держава за допомогою соціально-правового механізму забезпечення прав людини і громадянина створює необхідні умови для здійснення зазначених прав [1, с. 224]. У роботі соціально-правовий механізм розглядається, як система, невід'ємними взаємопов'язаними складовими якої постають механізм реалізації, механізм охорони та механізм захисту [1, с. 224]. Ґрунтуючись на визначенні поняття «система», виникає потреба у з'ясуванні корисних зв'язків та мети, яка має бути досягнута внаслідок функціонування соціально-правового механізму забезпечення прав людини і громадянина в умовах інформаційного суспільства. На нашу думку, мета механізму як системи визначається функцією, яку зазначена система реалізує у надсистемі і яку доцільно визначити (у абстрактному розумінні) як соціально-правовий механізм забезпечення колективних прав суспільства, а у конкретному розумінні – як інформаційну державу [4, с. 12].

Вважаємо, що необхідно актуалізувати використання логіки для правильного конструювання визначення понять (зокрема, «права людини і громадянина», «соціально-правовий механізм забезпечення прав людини і громадянина», «інформаційне суспільство», «інформаційна держава»). Акцентовано увагу на існуванні різних класів понять (наприклад, індивідуальні, загальні, збірні, абстрактні, конкретні, відносні, абсолютні) [5, с. 7 – 12], що треба враховувати під час формування

понятійної бази передусім науки «інформаційне право», яка знаходиться на етапі свого становлення. Підкреслено важливість розуміння змісту та обсягу понять; різниця між ними полягає у наступному: обсяг понять визначає таку сукупність елементів, до якої додається дане поняття, а зміст визначає такі ознаки, які притаманні тому чи іншому поняттю [5, с. 15]. До речі, з'ясовано, що відношення між обсягом та змістом понять «суспільство» та «інформаційне суспільство» наступне. Зміст поняття «інформаційне суспільство» більше, ніж поняття «суспільство», а обсяг поняття «інформаційне суспільство» менше, ніж поняття «суспільство». Отже, у процесі збільшення змісту поняття відбувається зменшення його обсягу, і навпаки. Що стосується ознак понять, то з часів Аристотеля вони поділяються на п'ять класів: родова ознака, видова відмінність, вид, власна ознака, невласна ознака [5, с. 13, 14]. Вважаємо, що спеціального дослідження потребує і проблема відношення між поняттями, що пов'язано із розглядом логічних відношень, наприклад, субординація понять, координація понять, рівнозначність понять, протилежність понять, практичність понять та ін.

Усвідомлюючи, що головна мета визначення поняття – розкрити зміст поняття, зробити зміст поняття таким, щоб він був точним, у роботі акцентується увага на двох способах визначення поняття: а) перерахування ознак, які притаманні даному поняттю; б) визначення здійснюється за допомогою найближчого роду та видової різниці; визначення відбувається за допомогою судження, яке містить підмет та присудок; правильне визначення зумовлено дотриманням чотирьох спеціальних правил [5, с. 26–28]. Слід визнати, що існують і інші способи, наприклад, вказівка, опис, характеристика, порівняння та ін. Водночас, вельми корисними з методологічної точки зору постають дослідження процесу ділення, який, на відміну від процесу визначення, розкриває обсяг поняття. Йдеться, зокрема, про ділення роду на види, видів на підвиди, що також пов'язано із дотриманням певних правил [5, с. 31–33]. До речі, одним із таких правил є те,

що ділення повинно мати одну підставу. На жаль, зазначене правило дуже часто порушується, про що свідчать проведені дослідження.

Аналіз багатьох наукових досліджень у галузі юриспруденції (передусім дисертаційних досліджень) переконливо доводить, що використання логіко-семантичного методу для визначення понятійної бази лише анонсується, і насправді є суттєві підстави для активізації наукової дискусії щодо правильного мислення, яке має бути підпорядковано вимогам чотирьох його законів. Розуміючи важливість і одночасно складність порушеного питання, вважаємо за необхідне привернути увагу наукової спільноти до спільного вирішення зазначеного питання. Очевидно, що не лише проблема забезпечення прав і свобод людини і громадянина в умовах інформаційного суспільства за допомогою соціально-правового механізму держави потребує правильного визначення понять та конструктивного використання, зокрема, системного та логічного методів дослідження. Вважаємо, що це вельми актуально для будь-яких наукових юридичних досліджень, передусім для науки «інформаційне право», теоретико-методологічні засади якої сприятимуть розвитку галузі права «інформаційне право», яка у країнах Європейського Союзу постає правовим фундаментом інформаційного суспільства.

Література

1. Скакун О. Ф. Теорія держави і права (Енциклопедичний курс) / О.Ф.Скакун: підруч. [вид. 2-е , перероб. і доп.]. – Харків: Еспада, 2009. – 752 с.

2. Анохин П.К. Принципиальные вопросы общей теории функциональных систем: монография / П.К.Анохин [Електронний ресурс]. – Режим доступу: http://www.keldysh.ru/pages/BioCyber/RT/Functional.pdf

3. Луць Л.А. Європейські міждержавні правові системи та проблеми інтеграції з ними правової системи України (теоретичні аспекти): монографія /Л.А.Луць. – К.: Ін-т держави і права ім. В.М.Корецького НАН України, 2003. – 304 с.

4. Арістова І. В. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади: автореф. дис. … докт. юрид. наук: 12.00.07/ І. В. Арістова. – Харків, 2002.– 39 с.

5. Челпанов В. Г. Учебник логики / В. Г. Челпанов.– М.: Научная библиотека, 2010.– 128 с.

==========***==========

О. А. Баранов,
д.ю.н., с.н.с.,
керівник Центру теоретико-правових
проблем інформаційної сфери
НДІІП НАПрН України

ПРАВОВІ ПРОБЛЕМИ ІНТЕРНЕТУ РЕЧЕЙ В КОНТЕКСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

В 1999 году К. Ештон вперше застосував термін «інтернет речей» (Internet of Things). Протягом останніх 15-20 років, а особливо останні 7-8 років, з'явилися публіцистичні, технічні та наукові публікації, які описують появу сотень і тисяч проектів створення тих чи інших технологій інтернету речей (IP) та їх практичне застосування. У багатьох передових країнах усвідомили, що в сегменті ринку, пов'язаному з технологіями IP, закладено величезний потенціал як значного підвищення ефективності практично будь-якого виду людської діяльності, а значить і національних економік, так і просто колосальні перспективи зростання власне ринку розробки та виробництва технологій IP. Прогнозується, що у 2025 році ринок технологій IP тільки у Європі буде складати до 1 трлн. євро.

Однак разом з тим з'ясувалося, що незважаючи на неосяжні можливості застосування найрізноманітніших технологій IP, початковий рух по впровадженню цих проривних технологій природно було зорієнтоване на найбільш виграшні і найбільш ефектні зразки технологій і варіанти додатків. Чисельні корпорації в різних країнах розробляють окремі додатки, системи та комплекси технологій IP найрізноманітнішого призначення.

Отримані результати демонструють значні потенційні можливості технологій IP. Але стає зрозумілою необхідність розроблення загальної концепції, прогнозного баченням розвитку різних секторів економіки і суспільного життя в умовах широкого використання технологій Інтернету речей.

Тому в останні роки в багатьох країнах було вжито заходи як на урядових рівнях, так на рівнях експертних і професійних спільнот для аналізу стану справ з впровадженням технологій IP, локалізації проблем та загроз, які мають місце або можуть виникнути в майбутньому, з метою формування загальної стратегії розвитку промисловості виробництва технологій IP і їх застосування в різних секторах економіки і суспільного життя. Таке системне інтелектуальне опрацювання має дуже важливе значення в силу декількох причин:

наявність великої кількості центрів розробки технологій IP, в, зокрема, одного і того ж призначення;

високі темпи розробок, виробництва і впровадження окремих пристроїв, компонент технологій і, в цілому, технологій IP;

безпрецедентна потенційна масштабність використання технологій IP, як в окремих країнах, так і в цілому в світі;

прояви синергетичного ефекту від використання технологій IP, який позначиться, в тому числі, і в появі абсолютно нових за споживчими властивостями послуг і в можливості проведення нового виду робіт;

необхідність забезпечення взаємодії як різних технологій IP, так і різних впроваджень цих технологій чи шляхом інтеграції, то чи шляхом автономної взаємодії;

висока вартість можливих помилок внаслідок масштабності використання технологій IP;

необхідність залучення значних обсягів інвестицій за короткий проміжок часу;

впровадження технологій IP потребує інтенсивних наукових досліджень щодо оптимізації тих чи інших видів діяльності в зв'язку з новими функціональними можливостями;

розвиток технологій IP є найпотужнішим стимулюючим фактором для інноваційного розвитку нанотехнологій, мікроелектроніки, напівпровідникових технологій, мікромініатюризації виконавчих пристроїв, телекомунікацій, радіотехнологій, програмних обчислювальних засобів і багато іншого.

Все це призводить до появи потенційних ризиків і проблем внаслідок масштабного, повсюдного і багато секторального впровадження технологій IP. Найбільш вагому групу ризиків складають правові проблеми, що обумовлюється з однієї сторони виникненням якісно нової множини суспільних відносин, які базуються на використанні технологій IP, а з іншої – невизначеністю правового регулювання зазначених правовідносин. Ситуація загострюється ще і внаслідок того, що зростання подібних правовідносин буде лавиноподібним за відносно невеликий проміжок часу. Тому перед правовою наукою постають наступні завдання:

– визначення теоретично-методологічних засад правового регулювання суспільних відносин, пов’язаних з використанням технологій інтернет речей, необхідно для зменшення ризиків та бар’єрів просування інтернету речей у всі сфери життєдіяльності у суспільстві, а також для створення наукового підґрунтя для подальшого вдосконалення законодавства у сфері інформатизації, телекомунікацій, електронної комерції, захисту персональних даних, інфраструктурної безпеки, кібербезпеки тощо;

– вивчення особливостей виникнення та реалізації правовідносин, що базуються на використанні технологій IP, зокрема і з елементами штучного інтелекту;

– визначення концептуальних підходів щодо правових механізмів регулювання забезпечення інфраструктурної безпеки впровадження та використання технологій IP;

– правового регулювання забезпечення кібербезпеки в умовах транскордонного використання технологій IP;

– з’ясування нових системних правових проблем забезпечення конфіденційності, зокрема і захисту персональних даних;

– правого регулювання застосування інтернет технологій та використання радіочастотного ресурсу в умовах масового використання радіоприладів тощо;

– вдосконалення законодавства, насамперед інформаційного, що повинно забезпечити правові умови для розроблення, впровадження та використання технологій IP.

Вирішенню проблеми вдосконалення теоретичних засад правового захисту приватності людини в умовах широкого використання інформаційних комп’ютерних технологій, зокрема захисту права людині на конфіденційність її персональних даних приділяється значна увага як на рівні міжнародного права, так і на рівні національного законодавства різних держав.

В останні роки вишукується теоретичні засади та практичні пропозиції щодо вирішення проблеми правового захисту конфіденційності персональних даних в умовах застосування можливостей профайлінгу. Технології IP значно підсилюють ризики порушення конфіденційності персональних даних внаслідок того, що вони ИВ передбачають накопичення, циркулювання і використання великого, просто величезного територіально і технологічно розподіленого обсягу інформації (даних) про конкретну людину.

Підсумовуючі можна зробити висновки, що широке використання технологій інтернету речей призводить до необхідності вирішення таких основних правових проблем: визначення правових механізмів реалізації принципу попередньої згоди на використання персональних даних, реалізація «права бути забутим», регулювання транскордонних потоків персональних даних, використання персональних даних інтелектуальними комплексами, що функціонують без участі суб'єктів (юридичних або фізичних осіб).

Крім того, інтернет речей буде передбачати необхідність створення багаторівневої і багато об'єктної системи захисту персональних даних, що потребує створення системи нового правового регулювання.

==========***==========

В. М. Фурашев,
к.т.н., с.н.с., доцент Навчально-наукового центру інформаційного права та правових питань інформаційних технологій ФСП НТУУ "КПІ". НДІ ІП НАПрН України

ПРАВА ЛЮДИНИ: ОСНОВНІ ЗАГРОЗИ ЇХ ЗАБЕЗПЕЧЕННЯ В УКРАЇНІ

Основоположні права людини вперше, на міжнародному рівні, були викладені та зафіксовані у грудні 1948 року у «Загальній декларації прав людини», прийнятій та проголошеній 10 грудня 1948 року резолюцією 217 А (III) Генеральної Асамблеї ООН 10 грудня 1948 року [1].

Подальша деталізація основоположних прав людини та, головне, визначення механізму їх забезпечення відображено у «Конвенції про захист прав людини і основоположних свобод» прийнятій в Римі 4 листопада 1950 року урядами держав – членів Ради Європи [2].

Верховна Рада України ратифікувала дану Конвенцію 17.07.1997 р., яка набрала чинності для України 11.09.1997 р.

Тобто 18,5 років потому Україна визнала верховенство «Конвенції про захист прав людини і основоположних свобод» у системі системоутворюючих національних законів у цій сфері.

Необхідно зауважити, що Конституція України, більшість законів України цілком відповідають положенням даної Концепції, але чомусь Україна з кожним роком стає все більш «поважним клієнтом» Європейського суду з прав людини (ЄСПЧ) у частині звернень до нього. У чому причина?

[1] Джерело інформації: http://zakon3.rada.gov.ua/laws/show/995_015
[2] Джерело інформації: http://zakon5.rada.gov.ua/laws/show/995_004

Що є основною загрозою дотримання, забезпечення та розширення основоположних прав людини?

Відповідей, як виправдовувальних, так і звинувачувальних можна знайти безліч, але недарма кажуть: «той хто хоче – шукає шляхи, той хто не хоче – виправдання». Але для того, щоб шукати шляхи, непогано було б встановити джерела такого становища, знайти першопричини.

На погляд автора, відповідь потрібно шукати у підходах до моделі державного будівництва у період 1992-1994 років, коли остаточно ставка була зроблена на великий бізнес як основу економічного фундаменту держави, її економічного розвитку, «локомотиву» забезпечення високого рівня життя. Але при цьому не було враховано, що у період 1917 – 1991 років виховання **всього** населення було спрямоване на: а) витравлення поняття «заробляти» та прищеплення поняття «отримання»; б) «керівник будь-якого рангу, особливо партійний або радянський функціонер – особлива каста, яка живе та підкоряється своїм законам»; в) інші заповіді, які створювали досить «комфортні» умови партійно-радянській номенклатурі проводити «колективізацію», «індустріалізацію», будувати «соціалізм та комунізм», «доганяти та обганяти Америку». Ця система - це виховання, яка за своєю сутністю, не визнавала та й не могла визнавати конкуренцію, як основну рушійну силу соціально-економічного розвитку держави зі всіма витікаючими наслідками. Ця система, це виховання, спокійно сприймала відомий указ Й.В. Сталіна щодо трьох колосків – вкрав три колоски з колгоспного поля – одного із «закладів» ГУЛАГ - гарантовано забезпечений, вкрав машину, а тим більше вагон зерна – поважна та дуже поважна людина. Ця система не сприймала й не могла сприймати такі юридичні, управлінські постулати та, суто людські, постулати, як «закон – один для всіх» та «невідворотність покарання».

Побудована олігархічно-кланова модель управління державою, яка поступово трансформувалася у олігархічну, зі всіма «родимими плямами»

радянського періоду, не надає шансів на поліпшення ситуації у сфері дотримання та забезпечення прав людини.

До тих пір поки у системі державного управління буде діяти принцип «політичної доцільності», широко введений у практичну діяльність після подій 2004 року, не слід очікувати поліпшення ситуації у сфері дотримання та забезпечення прав людини.

До тих пір поки юридично не буде врегульоване поняття «політичне переслідування», яке на сьогодні надає можливість будь-яке діяння адміністративного або кримінального характеру представляти у цій якості, зрушень у сфері дотримання та забезпечення прав людини не буде.

Все перелічене вище є основою, живильним середовищем корупції, причому корупції не обмеженої або вибіркової, а тотальної. А там де корупція з її багатогранністю – які можуть бути питання щодо прав людини? Але це вже тема окремого дослідження.

В обсягах тез неможливо окреслити, а тим більше розкрити, навіть, основні загрози дотримання прав людини в нашій країні – кожне наведене та не наведене висловлювання потребує деталізації, аргументації, дискусій, окремих наукових досліджень.

Але головне полягає у тому, що всі основні загрози у сфері дотримання та забезпечення прав людини полягають у:

- відсутності на практиці реалізації принципів «закон – один для всіх» та «невідворотність покарання»;
- неусвідомленні всіма прошарками населення різниці між поняттями «заробляти» та «отримувати»;
- нерозумінні того, що рівень дотримання та забезпечення прав людини є індикатором ступеню забезпеченості державності, територіальної цілісності, суверенітету та всіх складових безпеки (національної, державної, інформаційної, економічної, екологічної та ін,);
- неусвідомленні, що боротьба з корупцією, як головним чинником порушення прав людини, з одного боку, а з іншого – похідною від перших

двох перелічених основних загроз, є справою не лише державних установ на кшталт Антикорупційного бюро України, прокурорської та судової систем, а кожного громадянина України, кожного з нас.

Розуміння наведеного, практичне, а не декларативне, відтворення висловленого надасть змогу кардинальним зрушенням у сфері прав людини та перетворить Україну у дійсно поважного, без лапок, клієнта ЄСПЧ, якій не створює жодний клопіт його суддям, особливо за статтею 34 «Індивідуальні заяви».

==========***==========

О. Д. Довгань,
к.ю.н., с.н.с., учений секретар
НДІІП НАПрН України

ДОТРИМАННЯ ІНФОРМАЦІЙНИХ ПРАВ І СВОБОД ГРОМАДЯН: ПРАВОВІ НОРМИ

В демократичному суспільстві загальновизнані права людини і громадянина в сфері інформації виступають основним критерієм, що характеризує стан інформаційної безпеки конкретної особи і суспільства в цілому. Оскільки, одним з основних пріоритетів інформаційної політики будь-якої країни є дотримання балансу відповідних інтересів особистості, суспільства і держави. Країни, що обрали демократичний шлях розвитку, принципово виходять при цьому з примату прав і свобод особистості.

На нормативному рівні це зазвичай виражається у конституційних гарантіях свободи слова та доступності інформації для кожного громадянина (свобода публічних висловлювань незалежно від їхнього політичного змісту; забезпечення безперешкодного отримання громадянами повної та неупередженої інформації). Обмеження цього фундаментального права особистості розглядається як виняток із загального принципу відкритості інформації та реалізується тільки відповідно до чинного законодавства і лише в окремих випадках.

Конституція України виступає гарантом зазначених положень. Крім того, Основний закон є нормативно-правовим фундаментом інформаційного законодавства України. Це стосується ст.ст.3, 34-та, а також низки інших (10, 15, 17, 23. 28, 29, 31, 32, 40, 50, 53, 54, 55, 57) статей Конституції України. Зокрема, стаття 3 Конституції України (норми прямої дії) проголошують: “Людина, її життя і здоров’я, честь і гідність, недоторканість і безпека визнаються в Україні найвищою соціальною цінністю. Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов’язком держави”.

«Стаття 34. Кожному гарантується право на свободу думки і слова, а вільне вираження своїх поглядів і переконань. Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб - на свій вибір.

Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя».

В міжнародних документах, таких як Загальна декларація прав людини та Міжнародний пакт про громадянські і політичні права (Стаття 19), дотримуватися яких зобов’язалися країни-учасниці ОБСЄ, у т.ч. і Україна, яка є стороною вищезазначених документів, йдеться про дотримання свободи слова. Зокрема, стаття 19 Загальної декларації говорить: “Кожна людина має право на свободу переконань і на вільне їх виявлення; це право включає свободу безперешкодно дотримуватися своїх переконань та свободу шукати, одержувати і поширювати інформацію та ідей будь-якими засобами і незалежно від державних кордонів”. Крім того, це право вказане та

юридично закріплене у Статті 19 Міжнародного пакту про громадянські та політичні права.

Свобода слова також передбачена Статтею 10 Європейської конвенції про захист прав людини та основоположних свобод:

“1. Кожен має право на свободу вираження поглядів. Це право включає свободу дотримуватися своїх поглядів, одержувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів. Ця стаття не перешкоджає державам вимагати ліцензування діяльності радіомовних, телевізійних або кінематографічних підприємств.

2. Здійснення цих свобод, оскільки воно пов’язане з обов’язками і відповідальністю, може підлягати таким формальностям, умовам, обмеженням або санкціям, що встановлені законом і є необхідними в демократичному суспільстві в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, для охорони здоров’я чи моралі, для захисту репутації чи прав інших осіб, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету і безсторонності суду”

Таким чином, норми щодо дотримання інформаційних прав і свобод людини містяться, насамперед, в Конституції України, міжнародно-правових актах з прав людини, галузевих міжнародних та національних правових актах, якими врегульовані окремі питання інформаційних прав людини. Ці норми потрібно дотримуватися і виконувати.

Тому, у подальшому, виходячи з положень статей 3 та 21 Конституції України, які визначають природне право початком і основою української правової системи, необхідно дотримуватися двох напрямків: правоохоронного, який полягає у можливості реалізації прав і свобод людини, та правозахисного щодо захисту порушених суб’єктивних прав. Метою останнього повинно бути упередження, припинення правопорушення та відновлення бажаних для людини, суспільства або держави прав і свобод, встановлених нормативно-правовими актами.

І. М. Забара,
к.ю.н., доцент кафедри міжнародного права
Інституту міжнародних відносин
Київського національного університету
ім. Т.Шевченка

ЗАХИСТ ПРАВ ЛЮДИНИ У ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ: КОНЦЕПТУАЛЬНІ ПІДХОДИ У НАУЦІ МІЖНАРОДНОГО ПРАВА

У своєму розвитку права і свободи людини пройшли досить тривалий шлях. Вони потребували і визначення, і визнання, і закріплення, і механізмів захисту, і спрямування подальшого розвитку.

Не стала виключенням і проблема захисту прав і свобод людини в нових, сучасних умовах – в умовах становлення і розвитку як окремих національних інформаційних суспільств, так і глобального інформаційного суспільства.

Проблема захисту прав людини у інформаційному суспільстві ускладнюється кількома чинниками, серед яких найважливішими, на нашу думку, варто назвати наступні:

по-перше, складність визначення інформаційного суспільства (нараховується шість концепцій його розвитку) і наявність разом із його позитивними аспектами, ще і негативних, таких що можуть нести загрози існуючим правам людини;

по-друге, невизначеність масштабного впливу інформаційно-комунікаційних технологій як на саму людину, так і відповідно на її права і свободи;

по-третє, відсутність у науці і практиці міжнародного права загальноприйнятого визначення «інформаційні права людини»;

по-четверте, необхідність реалізації одного із основних принципів міжнародного права – принципу поваги прав та основних свобод людини.

Невизначеність призводить до пошуку відповідей на низку принципових питань. Зокрема, які права потребують захисту в інформаційному суспільстві? Яке розуміння і відношення повинно бути до

вже існуючих прав в умовах інформаційного суспільства? Як враховувати неоднозначне розуміння і тлумачення категорії (групи) нових «інформаційних прав», що пов'язані із використанням інформаційно-комунікаційних технологій?

Розглядаючи проблему захисту прав людини у інформаційному суспільстві, варто відмітити її широке формулювання і складність сприйняття. Вірогідно, що це пов'язано з тим, що єдність думок на проблему захисту прав людини у інформаційному суспільстві відсутня. Тому виникає питання щодо ознайомлення з найбільш поширеними науковими підходами і поглядами у доктрини міжнародного права.

В першу чергу це стосується відповіді на наступне питання: які саме права, разом вже із визначеними і закріпленими міжнародним правом, підлягають захисту в інформаційному суспільстві?

Відповідь на це питання веде до розгляду кількох згрупованих за певними схожими ознаками концептуальних підходів і наукових поглядів.

В основу класифікації цих підходів і поглядів, на нашу думку, варто покласти критерій впливу сучасних інформаційно-комунікаційних технологій на реалізацію прав і свобод людини. Зазначимо, що запропонована нами класифікація має умовний характер і враховує потребу її подальшого наукового осмислення і розробки.

Узагальнюючи зауважимо, що існує кілька підходів. Принципових може бути виокремлено чотири:

1. «Загальний підхід»: захисту підлягає весь перелік існуючих прав людини, визначених міжнародно-правовими актами;

2. «Вибірковий підхід»: захисту підлягають тільки ті права і свободи, що визначаються в якості основи для формування групи «інформаційних прав» людини; решта прав розглядається через співвідношення до них;

3. «Спеціальний підхід»: захисту підлягають тільки ті права, що визначені і закріплені міжнародним правом, реалізація цих прав пов'язана із

інформацією з обмеженим доступом, несанкціоноване поширення такої інформації та порушення режиму доступу завдає шкоди власнику інформації;

4. «Тематичний підхід»: захисту підлягає тільки категорії прав, що пов'язані із сучасним розвитком інформаційно-комунікаційних технологій в умовах розвитку інформаційного суспільства – «цифрові права і свободи людини» (digital rights and freedoms).

Варто коротко охарактеризувати кожен з них.

Суть першого, «загального», підходу полягає у тому, щоб зазначити перелік прав і свобод, що визначені у міжнародно-правових актах, які за умов розвитку інформаційного суспільства і різноманітного впливу інформаційно-комунікаційних технологій, потребуватимуть захисту.

За основу такого переліку прав людини, в якості джерел беруться: Всесвітня декларація прав людини 1948 р, Міжнародний пакт про громадянські і політичні права 1966 р. і Міжнародний пакт про економічні, соціальні і культурні права 1966 р.

Як один з варіантів, вірогідний і різноманітний вплив інформаційно-комунікаційних технологій на права людини може розглядаються за групами прав (громадянські, політичні, економічні, соціальні, культурні), а також з урахуванням поколінь розвитку прав людини (I, II, III та можливо IV покоління).

З урахуванням правової природи прав, автори роблять відповідні висновки щодо реалізації і можливого захисту кожного з прав у інформаційному суспільстві. Увага, як правило, акцентується на особливостях реалізації щодо кожного з прав (групи прав) у інформаційному суспільстві і його відповідному захисті.

Зазначається, що майже усі права, в тій чи іншій мірі, мають прояв у інформаційному суспільстві.

За цим підходом увага концентрується також і на питанні щодо гарантій прав і свобод людини і громадянина (інституційні гарантії, процесуальні гарантії, матеріальні гарантії).

Висловлюється думка про необхідність удосконалення систем захисту прав людини у інформаційному суспільстві відповідно на універсальному, регіональному і національному рівнях.

Зрозуміло, що за таким підходом, обсяг аргументації щодо кожного з прав (групи прав) різниться, або взагалі може бути відсутнім.

Суть другого, «вибіркового», підходу полягає у визначенні в якості ключових елементів кількох категорій прав і свобод та побудова на їх основі певної групи інформаційних прав, що підлягатимуть захисту.

В якості ключових обрано три категорії: «свобода інформації», «право на інформацію», «право на комунікацію».

За основу для визначення «свободи інформації» (свободу шукати, отримувати і поширювати інформацію) в якості джерел беруться відповідні положення універсальних і регіональних міжнародно-правових актів.

Основою для визначення «права на інформацію» («права на доступ до інформації», «права на доступ до публічної інформації») виступають доктринальні погляди і міжнародно-правові акти.

В якості основи «права на комунікацію» («права на доступ до засобів комунікації», «право на доступ до Інтернет»)» виступають доктринальні погляди), Статут міжнародного союзу електрозв’язку 1992 р.

Думки щодо складу групи «інформаційних прав» різняться.

Одні обмежуються включенням до її складу зазначених «свободи інформації», «права на інформацію» і «права на комунікацію».

Інші вважають, що ця група інформаційних прав може бути розширена за рахунок появи нових прав і свобод, в умовах їх реалізації у інформаційному суспільстві та під впливом, або із використанням інформаційно-комунікаційних технологій. Саме таку групу прав, їх автори визначають, як окрему групу, тобто групу «інформаційних прав» людини. Підкреслюється, що така група інформаційних прав вирізнятиметься своїми особливостями. При цьому дискусійним залишається перелік прав, що входять (входитимуть) до складу такої групи.

Разом з тим, припускається її включення до низки інших груп прав людини (поряд із громадянськими, політичними, економічними, соціальними, культурними).

Суть третього, «спеціального», підходу полягає у визначені в якості базових категорій, що підлягають захисту, тільки тих прав, які сукупно відповідають наступним умовам: (а) визначені і закріплені міжнародним правом, (б) їх реалізація пов'язана із інформацією з обмеженим доступом (конфіденційна інформація; таємна інформація), (в) несанкціоноване поширення такої інформації та порушення відповідного режиму доступу завдає шкоди власнику інформації.

За таким підходом захисту підлягають: персональні дані особи, генетична інформація особи, лікарська таємниця, професійна таємниця суддів, адвокатська таємниця, нотаріальна таємниця, журналістська таємниця.

Разом з тим, наголошується на необхідності особливої уваги до захисту цих прав в умовах розвитку інформаційного суспільства і масштабного використання інформаційно-комунікаційних технологій.

Суть четвертого, «тематичного», підходу полягає у розгляді і визначені, з метою правового захисту, сукупності тільки тих прав, що пов'язані із сучасним розвитком інформаційно-комунікаційних технологій в умовах розвитку інформаційного суспільства – т. з. «цифрові права і свободи людини» (digital rights and freedoms), «Інтернет-права» тощо.

На думку авторів саме ці права мають безпосереднє відношення до категорії інформації і комунікації або до «сучасної інформаційної та комунікаційної сфер» в умовах розвитку інформаційного суспільства.

В основі такого підходу лежать погляди на «цифрові права і свободи людини» закладені у Хартії Глобального інформаційного суспільства 2000 року.

За цим підходом, до категорії інформаційних прав відносять усю можливу сукупність прав, пов’язуючи їх реалізацію і захист виключно з умовами розвитку цифрових інформаційно-комунікаційних технологій.

Таким чином, узагальнюючи зазначене, відмітимо наступне:

- проаналізовані концептуальні підходи не є вичерпними і охопили тільки принципові погляди на проблематику захисту прав людини в умовах розвитку інформаційного суспільства;

- розглянуті підходи підкреслюють важливість захисту прав людини в умовах масштабного використання інформаційно-комунікаційних технологій;

- відсутність у науці і практиці міжнародного права загальноприйнятого визначення «інформаційні права людини» ускладнює їх єдине розуміння проте, не зупиняє пошуку взаємоприйнятного рішення щодо визначення їх переліку і відповідного захисту.

==========***==========

В. М. Поперечнюк,
НДІІП НАПрН України

КОНСТИТУЦІЙНІ ГАРАНТІЇ ПРАВА ЛЮДИНИ НА ІНФОРМАЦІЮ В УКРАЇНІ: ПРОБЛЕМНІ ПИТАННЯ

Уявити сучасне демократичне суспільство без гарантування та забезпечення права кожної людини на збирання, зберігання, використання, поширення інформації та свободи вираження поглядів, апріорі неможливо. Дане право закріплюється на рівні міжнародних актів та знаходить своє продовження в національних конституціях.

Конституція України у ст. 34 гарантує кожному свободу думки і слова, вільне вираження поглядів і переконань, закріплює право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший прийнятний для особи спосіб [1]. Хотілося ще раз звернути увагу на зміст даного права, який законодавець визначає у гіпотезі даної норми у

ключі – збирання, зберігання, використання і поширення інформації. При цьому цілком поділяючи позицію В.Г. Пилипчука та В.М. Брижка, про доцільність розширення конституційного переліку дій з інформацією: «Види інформаційної діяльності знаходяться в жорстких рамках того, що прописане в Конституції України (збір, зберігання, використання, поширення), хоча сучасний електронний простір (е-простір) визначає свої принципово інші види діяльності (обробка, введення, вивід, передача, компіляція, відображення даних та ін.)» [2, с. 15-16; 3, с. 11].

Крім того, на рівні Основного Закону визначені виключні випадки законодавчого обмеження даного права: «… в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя» [1].

З позиції закріплення даного положення, варто детальніше розглянути кожен із зазначених випадків обмеження права на інформацію та свободу вільного вираження поглядів і переконань, адже, створення і гарантування державою вільного обігу інформації є не лише однією із головних умов розвитку демократичної держави та ключовим мірилом демократичних процесів розвитку суспільства.

1) Інтереси національної безпеки України. Закон України «Про основи національної безпеки України» визначає лише *національні інтереси*, та тлумачить їх, як «… *життєво важливі* матеріальні, інтелектуальні і духовні *цінності Українського народу* як носія суверенітету і єдиного джерела влади в Україні, визначальні потреби суспільства і держави, реалізація яких гарантує державний суверенітет України та її прогресивний розвиток» [4], а також визначає поняття: «*Національна безпека* – захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення,

запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сферах правоохоронної діяльності, боротьби з корупцією, прикордонної діяльності та оборони, міграційної політики, *охорони здоров'я*, освіти та науки, науково-технічної та інноваційної політики, культурного розвитку населення, забезпечення свободи слова та інформаційної безпеки…» [4]. Із аналізу поняття національної безпеки бачимо, що національні інтереси є складовою останньої, тому конструкція *«інтереси національної безпеки»,* відверто кажучи є не цілком зрозумілою.

Взагалі аналізуючи положення даної норми, виникла думка про те що законодавець, як мінімум пропустив одне слово: «Здійснення цих прав може бути обмежене законом в інтересах ***забезпечення*** національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам…» – здається що так все цілком логічно та зрозуміло. Проте це не єдина хиба цієї статті Основного Закону:

2) *Територіальна цілісність та охорона здоров'я*. Згідно із Законом України «Про основи національної безпеки» до об'єктів національної безпеки також відноситься *територіальна цілісність* (ст. 3), а в ст. 1 визначено сферу *охорони здоров'я*, як складову національної безпеки України [4], тобто ці категорії можна не розкривати окремо, адже сутність поняття національна безпека та національні інтереси, в себе їх вже включають.

3) Поняття *громадський порядок* передбачено ст.1 Закону України «Про особливості забезпечення громадського порядку та громадської безпеки у зв'язку з підготовкою та проведенням футбольних матчів», як «…сукупність суспільних відносин, що забезпечують нормальні умови життєдіяльності людини, діяльності підприємств, установ і організацій (під час підготовки та проведення футбольних матчів) шляхом встановлення, дотримання і реалізації правових та етичних норм» [5]. У принципі, якщо застосувати аналогію закону та прибрати частину що стосується характерних особливостей суспільних відносин, на регулювання яких прийнятий даний

Закон, то що таке громадський порядок у контексті ст. 34 Конституції України зрозуміло.

Характерно, що обмеження права на інформацію можливе для умовного (адже законодавець цього не передбачає) забезпечення *«територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам»*, тобто є певна мета такого обмеження, при цьому посягання на територіальну цілісність і недоторканість України є самостійним складом злочину (ст.110 КК України), а щодо забезпечення громадського порядку в тому ж КК України виділено окремий XII розділ («Злочини проти громадського порядку та моральності»), окрім того цей розділ передбачає відповідальність за ст. 294 масові заворушення[6].

4) *Для захисту репутації або прав інших людей.* Нині законодавець використовує словосполучення *ділова репутація,* яку Пленум Верховного Суду України у постанові «Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи» розглядає як набуту особою суспільну оцінку її ділових і професійних якостей при виконанні нею трудових, службових, громадських чи інших обов'язків [7]. Еквівалентом даної категорії, якщо йдеться про фізичну особу та її особисті якості, є поняття «честь і гідність», тому суто гіпотетично, можна припустити, що можливо законодавець мав на увазі саме дані категорії.

5) Для запобігання розголошенню інформації, одержаної конфіденційно, цікаво що термін «конфіденційність» законодавець використовує у словосполученні «конфіденційна інформація», зокрема ст. 7 Закону України «Про доступ до публічної інформації»: «Конфіденційна інформація – інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов» [8]. Ст. 21 Закону України «Про інформацію» надає таке ж визначення конфіденційної інформації.

Закон України «Про державну статистику» має своє, відмінне від попередніх, поняття конфіденційної інформації, як статистичної інформації, яка належить до інформації з обмеженим доступом і знаходиться у володінні, користуванні або розпорядженні окремого респондента та поширюється виключно за його згодою відповідно до погоджених з ним умов [9].

При цьому на рівні підзаконних актів, використовується поняття «конфіденційність» лише в Указі Президента України «Про Положення про технічний захист інформації в Україні»: «як властивість інформації бути захищеною від несанкціонованого ознайомлення» [10].

б) Для підтримання авторитету і неупередженості правосуддя. Якщо правосуддя буде відбуватись неупереджено, об'єктивно та справедливо, то дана норма не матиме взагалі необхідності. Не говорячи вже про закони України «Про доступ до публічної інформації» та «Про доступ до судових рішень» та певних положень процесуального законодавства, які у частині гласності та публічності діяльності судової системи, просто не будуть чинними.

Отже, на основі аналізу ст. 34 Конституції України, варто зробити висновок, про певну недосконаліть, а подекуди і недолугість визначення питань, що стосуються права на інформацію та свободу вираження поглядів, а також випадки їх легального обмеження. Окрім того, на думку автора перелік обмежень даного права, як і інших права має бути конкретним та вичерпним, а механізми прозорими та чітко визначеними в законодавчих актах. Також варто, більш уважніше поставитись до переліку дій які пояснюють зміст права на інформацію, що потребує додатково осмислення та подальшого дослідження.

Література

1. Конституція України [Електронний ресурс] : закон України від 28. 06. 1996 р. № 254к/96-ВР із змін., внес. згідно із Законами України та Рішеннями Конституційного Суду : за станом на 04. 02. 2011 р. № 2952-17. –

Електрон. дан. (1 файл). – Режим доступу : http://zakon1.rada.gov.ua. – Назва з екрану.

2. Пилипчук В.Г. Актуальні проблеми становлення і розвитку правової науки в інформаційній сфері // Інформація і право. – № 1(4) – 2012. – С. 15-22

3. Брижко В.М. Про концептуальні основи системного впорядкування суспільних відносин в інформаційній сфері України // Інформація і право, № 2(5)/2012. – С. 10-17.

4. Про основи національної безпеки України [Електронний ресурс] : Закон України від 19.06.2003 № 964-IV. – режим доступу. – http://zakon0.rada.gov.ua/laws/show/964-15 – назва з екрану.

5. Про особливості забезпечення громадського порядку та громадської безпеки у зв'язку з підготовкою та проведенням футбольних матчів [Електронний ресурс] : Закон України від 08.07.2011 № 3673-VI – режим доступу. – http://zakon3.rada.gov.ua/laws/show/3673-17 – назва з екрану.

6. Кримінальний кодекс України [Електронний ресурс] : Кримінальний кодекс України від 05.04.2001 № 2341-III. – режим доступу. – http://zakon0.rada.gov.ua/laws/show/2341-14– назва з екрану.

7. Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи [Електронний ресурс] : Постанова Пленуму Верховного Суду України від 27.02.2009 N 1 – режим доступу. – http://zakon3.rada.gov.ua/laws/show/v_001700-09 – назва з екрану.

8. Про доступ до публічної інформації [Електронний ресурс] : Закон України від 13.01.2011 № 2939-VI. – режим доступу. – http://zakon5.rada.gov.ua/laws/show/2939-17 – назва з екрану.

9. Про державну статистику Електронний ресурс] : Закон України від 17.09.1992 № 2614-XII. – режим доступу. – http://zakon0.rada.gov.ua/laws/show/2614-12 – назва з екрану.

10. Про Положення про технічний захист інформації в Україні [Електронний ресурс] : Указ Президента України від 04.05.2008, підстава 333/2008 – режим доступу. – http://zakon0.rada.gov.ua/laws/show/1229/99 назва з екрану.

==========***==========

В. М. Панченко,
к.т.н., с.н.с.,
Національна академія СБ України

ПРОБЛЕМИ ЗАХИСТУ ПРАВ ЛЮДИНИ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ: ДОСВІД ЕСТОНІЇ

Однією із проблем захисту прав людини, обумовлених розвитком інформаційного суспільства, є проблема вироблення норм поведінки у кіберпросторі. Вона полягає у тому, що кіберпростір з його відкритістю та глобальністю часом призводить до порушення певних норм поведінки для окремих націй (держав), у тому числі моральних та правових. Разом з тим, спільний простір, яким є кіберпростір, вимагає відпрацювання спільних норм поведінки. Слід також врахувати, що норми поведінки визначаються правовими, політичними, суспільними, етичними особливостями націй тощо. Це також ускладнює відповідь на запитання, що таке кібернорми. Як розробити норми поведінки, які будуть найбільш прийнятними для усіх суб'єктів кіберпростору? Як забезпечити ефективність їх дотримання? Яким є статус таких норм, чи обов'язкові вони до виконання?

Питання вироблення кібернорм поведінки є актуальним, насамперед, для інформаційних суспільств, які характеризуються високим рівнем інформатизації. На нашу думку, такий рівень інформатизації сьогодні має Естонія.

Так, кожен громадянин Естонії має т.зв. ідентифікаційну картку, яка є одночасно паспортом і використовується не лише для ідентифікації особи, але й для фінансових розрахунків, навіть за проїзд у транспорті.

Система електронного урядування надає доступ до персональних даних користувача (ПІБ, місце і дата народження, місце роботи, родинні зв'язки тощо) залежно від рівня авторизації різним користувачам і службам. Зокрема, правоохоронні органи та спеціальні служби мають доступ до персональних даних громадян. Проте будь-який громадянин через систему електронного урядування може переглянути, хто цікавився його профайлом. Кожен суб'єкт, який отримав доступ до персональних даних громадянина, зобов'язаний протягом п'яти діб надати останньому на його вимогу вичерпну інформацію, з яких причин він цікавився цими відомостями.

Крім цього, в Естонії функціонує система електронного голосування. Таким чином, громадянин Естонії може виконати свій громадський обов'язок, знаходячись у будь-якій точці світу, де є інтернет. Електронне голосування розпочинається за тиждень до відкриття виборчих дільниць. Протягом цього тижня виборець може змінювати свою думку, і голосувати необмежену кількість раз, змінюючи при цьому свій вибір. Як результат буде зараховано останній варіант голосування. У день голосування виборець, який віддав свій голос через електронну систему голосування, має право прийти на виборчу дільницю і проголосувати ще раз. У такому випадку буде зараховано думку, яку виборець висловив під час традиційного "паперового" голосування.

Натомість в Україні сьогодні існує значний розрив між рівнем інформатизації суспільства та державних структур. Зокрема, в Адміністрації Президента України є 527 комп'ютерів, з них 176 ноутбуків придбав П.Порошенко за власні кошти [1]. Тобто 34% засобів ЕОТ зазначеної державної установи були закуплені протягом останніх півтора років. За таких умов маємо дисбаланс між уявленнями нашого суспільства про можливості держави «знати про особу все» та її реальними можливостями. Очевидно, що міф «держава знає про особу все та використовує це на її шкоду» породжений рефлексією на радянську політичну систему, за якої втручання у приватне життя громадян в інтересах держави було звичним явищем, та/або

невдалою спробою штучного перенесення реалій «високо інформатизованих» держав західного світу чи авторитарних країн на сучасні українські реалії. Водночас, інформатизація українських урядових структур та створення державних електронних реєстрів відбувається за відсутності чітких нормативно встановлених правил гри, що обумовлює високий рівень ентропії у цій сфері: кожне відомство в Україні формує власні електронні бази даних, тому навіть у випадку розслідування злочинів можливості українських правоохоронних органів щодо встановлення особи злочинця за допомогою електронних ресурсів значно обмежені. Переваги ж від цього хаосу отримують кіберзлочинці та спецслужби іноземних держав, зокрема РФ. Зауважимо, що правове поле останньої зобов'язує провайдерів інтернет-послуг до однозначної ідентифікації особи їх користувачів.

Таким чином, інформаційне суспільство має не рівні можливості для розвитку в умовах різних політичних систем. Країни з високим рівнем інформатизації вирішують сьогодні проблему вироблення норм поведінки у кіберпросторі. Натомість для України у сфері розвитку інформаційного суспільства на сьогодні більш актуальним є питання захисту прав людини в умовах створення електронних державних реєстрів. При вирішенні цього питання, на нашу думку, може бути корисним досвід Естонії, якій завдяки продуманій системі авторизації доступу до персональних даних громадян, вдалося досягнути розумного балансу між інтересами суспільства у безпеці та захистом права людини на «приватність». Більш розвинені в інформаційному вимірі суспільства завдяки впровадженню систем електронного урядування та голосування створили умови для вільного та оперативного обміну інформацією, що сприяє прозорості у стосунках із владою, а відтак і подоланню корупції.

Література

1. Інформація до відома // Тижневий журнал по-українськи «Країна». – 2016. – № 9 (312). – С. 4.

==========***==========

О. С. Петряєв,
аспірант Національного інституту
стратегічних досліджень України

ДЕСТРУКТИВНА ПРОПАГАНДА МОСКОВСЬКОЇ ПРАВОСЛАВНОЇ ЦЕРКВИ НА ТЕРИТОРІЇ УКРАЇНИ ЯК ЕЛЕМЕНТ ГІБРИДНОЇ ВІЙНИ

Сьогодні в Україні після початку сепаратистського руху на Донбасі, загострився релігійний міжконфесійний конфлікт. Релігійно-конфесійна карта України дуже різноманітна. До основних церков відносяться: Українська Православна Церква Київського Патріархату (УПЦ-КП), Українська Православна Церква Московського Патріархату (УПЦ- МП) і Українська Греко-Католицька Церква (УГКЦ). Дані церкви відіграють основну роль в релігійному житті України.

З початком антитерористичної операції на сході України, УПЦ- КП і УГКЦ підтримали уряд Києва в наведенні конституційного ладу в Донецькій і Луганській областях і протидії Російської інтервенції. УПЦ-МП не підтримала політики Києва стосовно Донбасу, і не приховує своєї критики по відношенню до дій Українського уряду. У свою чергу, Російський уряд вже не приховує, що Російська Православна Церква (РПЦ) координує дії УПЦ-МП для мобілізації своїх парафіян проти київського уряду, як елемент гібридної війни Кремля проти України.

Росія не задоволена демократичними реформами в Україні після Революції Гідності, імплементує елементи звичайної і гібридної війни, щоб уповільнити революційні зміни. Не складно помітити, що Росія віддає важливу роль ведення гібридної війни РПЦ і УПЦ-МП. Російська пропаганда агресивно нав'язує парафіянам УПЦ-МП образ віруючого УПЦ-КП або УГКЦ як людини яка повністю підтримує політику Києва на сході України, прихильника Євромайдану і Революції Гідності. Тим самим РПЦ і УПЦ-МП спеціально створюють громадянський конфлікт серед населення України на

релігійному підґрунті. Цілями РПЦ є відкрита антидержавна пропаганда, яка сприяє сепаратизму і опору нинішній Українській владі.

Одним із прикладів такої антидержавної політики з боку УПЦ-МП може бути події 8 травня 2015 року. Коли на урочистому засіданні Верховної Ради, президент Петро Порошенко зачитував імена загиблих на Майдані героїв України. Предстоятель Української Православної Церкви митрополит Київський і всієї України Онуфрій відмовився встати, щоб вшанувати їх пам'ять, мотивуючи свою дію, протестом проти війни [1].

Позиція РПЦ полягає в тому, що конфлікт на Донбасі - це громадянська війна східної частини українського народу проти української влади. Російська Православна Церква спеціально нагнітає русофільські та українофобські настрої серед населення Донбасу, виправдовує агресію російських терористичних військ, анексію Криму і зміни територіального устрою унітарної держави промовляючи, що: «*с началом боевых действий униаты и раскольники, получив в руки оружие, под видом антитеррористической операции стали осуществлять прямую агрессию в отношении духовенства канонической Украинской Православной Церкви на востоке страны*» [2].

Варто відзначити, що суспільно релігійні організації РПЦ виступають на суспільно-політичній сцені з чітко виробленими цивільними і політичними проектами, які приховані за ширмою релігійної моралі [3].

З боку РПЦ часто можна почути заклики до непокори українському уряду, критику війни за визволення України від терористичних військ, і релігійному протистоянню між віруючими всіх конфесій. Спостерігаються постійні заклики до миру і діалогу, які спрямовані на створення думки про згоди з тим, що не потрібно боротися за територію України. Культивується ідея негативного ставлення до війни, як способу захисту Української території від сепаратистів та російських найманців. [4] РПЦ також заявляє, що батальйони Правого Сектора налаштовані знищити Російську Православну Церкву і вбивати священників Московського Патріархату [5].

Небезпека пропаганди з боку Російської Православної Церкви лунає не тільки з Росії. Предстоятель Української Православної Церкви митрополит Київський і всієї України активно працює над зближенням двох православних церков, Української та Російської, що неминуче веде до узурпації релігії в Україні з боку Російської Православної Церкви [6].

Ефективність церковної пропаганди, як і будь-якої іншої пропаганди, ґрунтується на закономірностях матеріального світу, пов'язаних з психофізіологією і психологією людини. Керівними положеннями церковної пропаганди, як елемента деструктивної пропаганди в умовах інформаційної війни, виступають принципи, які збігаються з основними принципами військової пропаганди, а також принципи, властиві релігійній пропаганді – свободи совісті, гуманізму, публічності та інші. Такий синтез принципів протилежного спрямування, створює сучасний механізм церковної деструктивної пропаганди в умовах інформаційної війни.

Виходячи з вищевикладеного ми можемо зробити наступні висновки:

1. Поряд з традиційними формами деструктивної інформаційної пропаганди активно діє релігійна (або церковна) пропаганда, яка сьогодні, в умовах інформаційної війни між Росією та Україною, здійснюється Російською Православною Церквою проти парафіян церкви Київського Патріархату, Греко-католицької Церкви та інших християнських церков на території України.
2. Російська Православна Церква та її єпархії в Україні діють не як релігійна організація, а як політична сила, що використовує ідеї православ’я задля проросійської пропаганди.
3. Релігійна деструктивна пропаганда як елемент сучасної інформаційної війни є комплексом заходів інформаційного впливу на свідомість та підсвідомість людини яка здійснюється на підставі закономірностей, принципів та методик, сформованих практикою пропаганди і контрпропаганди, задля формування, зміни та руйнування суспільної думки.

4. У відповідності до закономірностей матеріального світу, що пов’язані з психофізіологією та психологією людини, його освіти і світосприйняття, релігійна деструктивна пропаганда має властивість бути ефективною на підставі виключно вибіркового впливу на різні верстви населення, а отже потребує свого різноманіття.
5. На нашу думку у якості контрпропаганди недоцільно використовувати заклики та силові методи виштовхування УПЦ МП з України, як це спостерігається з боку окремих політиків та керівництва УПЦ КП. Така форма контрпропаганди є деструктивною і за законом фізики має адекватний зворотній негативний ефект. Контрпропаганда повинна бути конструктивною за дією та правдивою за змістом. Тільки така форма контрпропаганди сприймається і формує свідомість населення.

Література:

1. Предстоятель УПЦ МП не встал во время почтения памяти военных. / [Электронный ресурс. - Режим доступа: http://korrespondent.net/ukraine/3512823-predstoiatel-upts-mp-ne-vstal-vo-vremia-pochtenyia-pamiaty-voennyk

2. Патриарх Московский и Всея Руси Кирилл. Святейший патриарх Кирилл призвал предстоятелей поместных церквей возвысить голос в защиту православных христиан востока Украины. / [Электронный ресурс].- 14.08.2014./ Режим доступу: https://mospat.ru/ru/2014/08/14/news106782/

3. Шевченко, М. Религиозная журналистика: типы, принципы и проблемы институционализации. / [Электронный ресурс].-21.11.2009. / Режим доступу: http://www.pravmir.ru/religioznaya-zhurnalistika-tipy-principy-i-problemy-institucionalizacii/#ixzz3aQqxwt6G

4. Филарет обвинил патриарха Кирилла в циничной лжи и работе на российскую пропаганду. / [Электронный ресурс]/ 2.09.2014- Режим доступа: http://gordonua.com/news/society/Filaret-obvinil-patriarha-Kirilla-v-cinichnoy-lzhi-i-rabote-na-rossiyskuyu-propagandu-39341.html

5. Епископ Григорий Лурье: Как Украинская церковь Московского патриархата будет отделяться от Москвы. / [Электронный ресурс]/ 25.07.2014- Режим доступа: http://www.religion.in.ua/zmi/foreign_zmi/26456-episkop-grigorij-lure-kak-ukrainskaya-cerkov-moskovskogo-patriarxata-budet-otdelyatsya-ot-moskvy.html

6. Патриарх Кирилл объявил войну в Украине "священной" (sacra bellum). / [Электронный ресурс] / ТСН. - Режим доступа: https://www.youtube.com/watch?v=T40kkgM2MIE

==========***==========

О. Г. Радзієвська,
с.н.с. НДІІП НАПрН України

ДО ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ ДИСКРИМІНАЦІЇ ДІТЕЙ В УКРАЇНІ

Розвиток новітніх інноваційних технологій, розширення технологічних можливостей, переорієнтація суспільства на нові цінності призводить до збільшення ролі інформаційної сфери в житті кожної людини і трансформації суспільства в інформаційне. Інформаційний простір стає найважливішою частиною життя та діяльності сучасного суспільства. Його комунікаційна, суспільна, освітня, комерційна та інші складові дедалі ширше представлені в Інтернеті та мережевих спільнотах. Питання додержання основних прав і свобод людини в інформаційному суспільстві, правових механізмів регулювання суспільних відносин та забезпечення інформаційної безпеки наразі є вкрай актуальними, проте недостатньо вивченими та такими, що потребують комплексного дослідження. Забезпечення ж прав дитини в інформаційному суспільстві та її інформаційна безпека є ще більш нагальними сьогодні.

Основними цінностями в інформаційному суспільстві виступають інформація і знання. Саме широкий доступ громадян до об’єктивної,

достовірної, повної, правдивої та неупередженої інформації, можливість здобувати знання та використовувати їх на практиці а також захищеність свідомості та підсвідомості людини від негативних інформаційних та інформаційно-психологічних впливів є гарантією успішності індивіда в інформаційному суспільстві та гарантуються державою. За Конституцією України дитина, як і будь-який громадянин має право на доступ до інформації (ст. 34) [1]. Теж саме задекларовано у статті 28 Конвенції про права дитини [2].

Рівність прав дітей в Україні незалежно від їх походження гарантовано ст. 52 Конституції України. [1]. Також, за Конституцією України держава гарантує дітям право на безкоштовну освіту (ст. 53) та можливість «вільно збирати, зберігати, використовувати та поширювати інформацію усно, письмово, або в інший спосіб – на свій вибір» (ч. 2 ст. 34). Проте в інформаційній сфері України спостерігається так звана «цифрова нерівність». Мова йде про неоднакові можливості у доступі до інформації та знань з використанням сучасних засобів інформаційно-комунікаційних технологій дітьми різних соціальних груп в залежності від місця їх проживання. Якщо міські школи, зокрема гімназії, ліцеї та інші елітні навчальні заклади, можуть похвалитись не лише забезпеченням комп’ютерами усіх учнів, але й створення власних інформаційних мереж, навчальних та методичних баз даних, електронних щоденників, системи електронного відвідування, тощо, то у сільській школі – заледве є декілька комп’ютерів, а про підключення їх до мережі Інтернет мова взагалі не йде. Станом на 2013 р. в українських містах із населенням понад 10 тис. чоловік, лише 5-7 % мешканців мали доступ до мережі Інтернет через високошвидкісні лінії передачі даних, а в сільській місцевості така ситуація була ще гіршою . [3]. Аналізуючи дані компанії Gemius за 2014 рік приходимо до висновку, що чим більше місто, тим інтенсивніше розвиваються у ньому технології. Зокрема, найбільший приріст користувачів Інтернету спостерігається у містах з населенням більше 500 тис. – 35,7 %, у містах з населенням 101-500 тис. – 24,2 %, менше

100 тис. – 21,1 %, і найменше збільшення кількості інтернет-користувачів у селах – 19,1 %. Тобто тенденції до регіонізації росту інтернет-аудиторії зберігаються й надалі, що є підтвердженням «цифрової нерівності» в Україні. [4]. Це вказує на те, що можливість повноцінного доступу до світового надбання інформації і знань в Україні диференційоване за територіальними особливостями її мешканців.

Таким чином, виникає нерівномірність у доступі до інформації і знань дітей не лише різних соціальних груп, а й різних регіонів України. Така ситуація значно поглиблює «цифрову нерівність» між окремими регіонами та верствами населення. За такої «цифрової нерівності» діти окремих категорій зазнають дискримінації в інформаційній сфері, що суперечить нормам міжнародного та національного права.

На міжнародному правовому рівні проблема рівності можливостей дітей піднімалася ще у 1959 р. У принципі 7 Декларації прав дитини зазначено, що дитина має право на безкоштовну освіту, яка сприяла б її загальному культурному розвитку і завдяки якій вона могла б, на основі рівності можливостей, розвивати свої здібності та особисті судження, відчуття моральної та соціальної відповідальності. [5]. Ці принципи були розширені та доповнені у Концепції про права дитини (далі – Конвенція) [2], яка була ратифікована Україною у 1991 році. Зокрема, у ст. 28 Конвенції визнається право дитини на освіту і на підставі рівних можливостей серед іншого держави-учасниці «забезпечують доступність інформації і матеріалів у галузі освіти й професійної підготовки для всіх дітей» (пп. d п. 1 ст. 28) і створюють можливості для «полегшення доступу до науково-технічних знань і сучасних методів навчання» (п. 3 ст. 28). Стаття 13 Конвенції, перекликаючись із ст. 34 Конституції України, дає право дитині «вільно висловлювати свої думки … шукати, одержувати і передавати інформацію та ідеї будь-якого роду незалежно від кордонів в усній, письмовій чи друкованій формі, у формі творів мистецтва чи за допомогою інших засобів на вибір дитини.», а ст. 17 покладає на державу-учасницю функції по забезпеченню

доступу дитини «до інформації і матеріалів із різних національних і міжнародних джерел, особливо до таких інформації і матеріалів, які спрямовані на сприяння соціальному, духовному і моральному благополуччю, а також здоровому фізичному і психічному розвитку дитини.» І на останок ст. 2 Конвенції зобов'язує держав-учасниць вживати «всіх необхідних заходів для забезпечення захисту дитини від усіх форм дискримінації».

Повертаючись до проблеми «цифрової нерівності» в Україні можемо стверджувати, що на сьогоднішній день не існує рівних можливостей у доступі до інформації та знань у дітей різних регіонів та соціальних груп, що суперечить основним правам дитини на національному та міжнародному рівнях. Така нерівність не лише створює дискримінацію окремих категорій учнів за можливістю доступу до інформації і знань, а й становить загрозу нерівності щодо рівня інтелектуального розвитку між дітьми великих міст та невеликих сіл. Не маючи повноцінного доступу до інформації, знань та технологій сільські діти не зможуть досягти такого ж високого інтелектуального рівня, як їх ровесники великих міст, не вмітимуть повноцінно використовувати сучасні інформаційні технології та засоби комунікації, адаптуватися до вимог нового суспільства, що засноване на широкому впровадженні інформаційних та інноваційних технологій, та стати повноцінними його членами. Зважаючи на те, що за даними статистики кількість сільських мешканців складає третину від загальної кількості мешканців Україні, а приріст населення у сільській місцевості більший за приріст у містах (12,6 осіб на 1000 осіб проти 10,9 у міських поселеннях) [6] та враховуючи трудову міграцію молоді з України у країни Європи та США – можемо стикнутися з проблемою зниженням загального інтелектуального рівня в державі та її конкурентоспроможності, що у подальшому призведе до сповільнення розвитку інформаційного суспільства в Україні загалом. Такі виклики можуть становити загрозу національній безпеці України у майбутньому.

Проблема може ще більше погіршитися у зв'язку з проведення в Україні адміністративно-територіальної реформи, що передбачає передачу закладів загальної середньої та професійної освіти під юрисдикцію органів місцевого самоврядування. Невеликі громади матимуть значно менші можливості щодо матеріально-технічного забезпечення учбових закладів, що належатимуть до їх компетенції. За відсутності належного фінансування цифрова нерівність між дітьми різних регіонів буде лише поглиблюватись. Тому необхідно уже сьогодні на державному рівні передбачити систему цільових грантів для приведення державних навчальних закладів до необхідного рівня матеріально-технічного та кадрового забезпечення. Це дасть можливість не лише позбутися цифрової нерівності, дискримінації дітей в інформаційній сфері, а й підвищити загальний інтелектуальний рівень усього суспільства та досягти мети, що ставилась державою ще у не столь віддаленому 2007 році Законом України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки»[7]: побудувати в Україні орієнтоване на інтереси людей, відкрите для всіх і спрямоване на розвиток інформаційне суспільство. Захист інформаційних прав громадян та забезпечення комп'ютерної та інформаційної грамотності населення, насамперед шляхом створення системи освіти, орієнтованої на використання новітніх інформаційно-комунікаційних технологій у формуванні всебічно розвиненої особистості були його основними цілями і залишаються актуальними і сьогодні.

Література

1. Конституція України [Електронний ресурс] : Закон України від 28.06.1996 № 254к/96-ВР – Режим доступу : http://zakon4.rada.gov.ua/laws/show/254%D0%BA/96-D0%B2%D1%80. – Назва з титул. екрана. – (Дата звернення: 12.03.2016).

2. Конвенція про права дитини [Електронний ресурс] : ООН від 20.11.1989. – Режим доступу : http://zakon1.rada.gov.ua/laws/show/995_021. – Назва з титул. екрана. – (Дата звернення: 12.03.2016).

3. Дубов Д.В., Ожеван М.А. Широкосмуговий доступ до мережі Інтернет як важлива передумова розвитку України : аналіт. доп. / Д.В. Дубов, М.А. Ожеван. – К.-НІСД, 2013. с. 58

4. Аудиторія українського Інтернету сповільнила свій ріст – за рік зросла лише на 12% - Електронне видання – Режим доступу : http://watcher.com.ua/2014/08/19/audytoriya-ukrayinskoho-internetu-spovilnyla-sviy-rist-za-rik-zrosla-lyshe-na-12. – Назва з титул. екрана. – (Дата звернення: 12.08.2015).

5. Международная защита прав и свобод человека / Права человека. Сборник международных договоров. – Москва, Юридическая литература, 1990. – с. 139-141

6. Населення України – Електронний ресурс. – Режим доступу : https://uk.wikipedia.org/wiki/%D0%9D%D0%B0%D1%81%D0%B5%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8#cite_note-ukrstat1-8. – Назва з титул. екрана. – (Дата звернення: 12.03.2016).

7. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки [Електронний ресурс] : Закон від 09.01.2007 № 537-V – Електронний ресурс. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/537-16. – Назва з титул. екрана. – (Дата звернення: 12.03.2016).

==========***==========

УДК 34.096
Г. М. Красноступ,
к.ю.н., с.н.с., *НДІІП НАПрН України*

СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ ДІТЕЙ В АУДІОВІЗУАЛЬНІЙ СФЕРІ

Діти – наше майбутнє. Сьогодні ніхто не заперечуватиме той факт, що телебачення безпосередньо впливає на виховання їх життєвих цінностей.

В Україні вже існує певне правове поле, що регулює питання захисту дітей від шкідливого контенту. Так, частиною четвертою статті 20 Закону України «Про охорону дитинства» забороняється пропагування у засобах масової інформації культу насильства і жорстокості, розповсюдження порнографії та інформації, що зневажає людську гідність і завдає шкоди моральному благополуччю дитини [1].

Згідно з частиною другою статті 6 Закону України «Про телебачення і радіомовлення» не допускається використання телерадіоорганізацій, зокрема для трансляції програм або їх відеосюжетів, які можуть завдати шкоди фізичному, психічному чи моральному розвитку дітей та підлітків, якщо вони мають змогу їх дивитися [2].

Стаття 62 вказаного Закону повністю присвячена питанню захисту суспільної моралі та забезпечення прав неповнолітніх і юнацтва. Так, при створенні, підготовці та розповсюдженні телерадіопрограм та передач телерадіоорганізації і провайдери програмної послуги зобов'язані дотримуватися вимог законодавства України про захист суспільної моралі.

Відповідно до статті 13 Закону України «Про захист суспільної моралі» трансляція теле-, відео- і радіопрограм, що містять елементи еротики, допускається з 24 годин до 4 годин, якщо інше скорочення часу трансляції не передбачено органами місцевого самоврядування. Перед трансляцією теле- і радіопрограм сексуального чи еротичного характеру обов'язково має бути зроблено звукове або текстове повідомлення про характер програми і заборону перегляду чи прослуховування її неповнолітніми [3].

Європейська конвенція про транскордонне телебачення, ратифікована Україною у 2008 році, передбачає захист дітей та підлітків від негативного телеконтенту [4].

Угодою про асоціацію Україна-ЄС передбачаються засади поступового наближення законодавства України до норм і стандартів Європейського Союзу.

Загалом законодавство ЄС не містить єдиного механізму для захисту дітей від шкідливого аудіовізуального контенту, тому в різних країнах запроваджуються власні національні системи з урахуванням національних особливостей.

Деталізовані та ефективні системи маркування продукції, яка поширюється як друкованими, так і електронними засобами масової інформації та новими медіа, запроваджено в більшості європейських країн. Їх розроблено передусім для допомоги батькам, які дбають про моральне і психічне здоров'я своїх дітей. Соціальні дослідження засвідчили, що близько 90% батьків у країнах ЄС повністю підтримують таку політику захисту дітей та молоді від потенційно шкідливого контенту [5]. Такі практики існують у Німеччині, Нідерландах, Туреччині.

Національна рада України з питань телебачення і радіомовлення на засіданні 10 березня 2016 р. внесла зміни до Системи візуальних позначок з індексом кіновідеопродукції залежно від аудиторії, на яку вона розрахована.

Такі зміни були зумовлені прийняттям постанови Кабінету Міністрів постанови від 2 грудня 2015 р. № 1143 «Про внесення змін до Положення про державне посвідчення на право розповсюдження і демонстрування фільмів». Цієї постановою були змінені індекси фільмів, що визначають глядацьку аудиторію. Національна рада привела у відповідність до цієї постанови свій власний регуляторний акт – Систему візуальних позначок з індексом кіно та відеопродукції залежно від аудиторії, на яку вона розрахована. Згідно з Положенням про державне посвідчення змінено вікові категорії глядачів. Їх запропоновано зображувати у жовтому або червоному колі. Показ фільмів з індексами «ДА» (дитяча аудиторія) та «ЗА» (загальна аудиторія) може відбуватися без позначки. Також документ передбачає необхідність позначати упродовж всієї трансляції спеціальними графічними попередженнями (символами) передачі, які містять інформацію, що може завдати шкоду фізичному, психічному або моральному розвитку дитини, а в

аудіопрограмах – на початку передачі оголошувати звукове попередження про шкоду, яку може завдати дітям така передача [6].

У зв'язку з цим, на сьогодні в Україні здійснюється підготовка проекту нової редакції Закону України «Про телебачення і радіомовлення». Вказаний законопроект передбачає спеціальну статтю щодо захисту дітей при наданні аудіовізуальних послуг [7], згідно з якою у програмах, передачах забороняється поширення аудіовізуальної інформації, яка може завдати значну шкоду фізичному, психічному або моральному розвитку дитини, у тому числі порнографічні матеріали, інформацію з надмірним зосередженням уваги на насильстві.

Аудіовізуальна інформація, що може завдати шкоду фізичному, психічному або моральному розвитку дитини, може поширюватися лише за умови, що діти не зможуть за звичайних обставин її почути або побачити.

Зазначена інформація може поширюватися у програмах мовлення, у тому числі шляхом ретрансляції, лише у проміжках часу між 23.00 та 06.00 або через забезпечення кодованого доступу.

У передачах на замовлення зазначена інформація може поширюватися лише в разі забезпечення кодованого доступу до перегляду (прослуховування) таких передач.

Передачі, що поєднують аудіо та візуальну інформацію і які містять інформацію, що може завдати шкоду фізичному, психічному або моральному розвитку дитини, повинні бути позначені спеціальними графічними попередженнями (символами), що показуються упродовж всієї передачі. У передачах, які містять аудіо інформацію, що може завдати шкоду фізичному, психічному або моральному розвитку дитини, на початку передачі оголошується звукове попередження про шкоду, яку може завдати дітям така передача.

Відповідні графічні попередження (символи) зазначаються у розкладі передач або в каталозі передач на замовлення, які складаються та оприлюднюються суб'єктами надання аудіовізуальної послуги.

Під час трансляції (ретрансляції) передач мовлення (крім новин, реклами, спортивних передач), що поєднують аудіо та візуальну інформацію і які не містять інформацію, що може завдати шкоду фізичному, психічному або моральному розвитку дитини, на початку передачі показується спеціальне графічне попередження (символ), що вказує на рівень впливу відповідної передачі на дітей певної вікової групи.

Відповідальність за забезпечення передач відповідними графічними попередженнями (символами) або звуковими попередженнями, передбаченими цією статтею, покладається на суб'єкта надання аудіовізуальної послуги.

Передбачено, що Національна рада України з питань телебачення і радіомовлення (національний регулятор) має затверджувати у порядку, визначеному цим Законом:

1) характеристики інформації, зазначеної у частинах першій-другій цієї статті, критерії її класифікації;

2) розподіл дітей у вікові групи та критерії класифікації передач залежно від рівня їх впливу на дітей певної вікової групи з урахуванням часу трансляції (ретрансляції) передач, передбачених частиною четвертою цієї статті;

3) зразки та вимоги до показу графічних попереджень (символів) та оголошення звукових попереджень, передбачених цією статтею;

4) порядок віднесення суб'єктом надання аудіовізуальної послуги передач до категорій, визначених цією статтею, та обрання відповідних попереджень (символів).

Вимоги до програмних або технічних засобів, які застосовуються для обмеження доступу до передач, передбачених цією статтею, шляхом кодованого доступу визначаються центральним органом виконавчої влади в галузі зв'язку.

Суб'єкт надання аудіовізуальної послуги на підставі характеристик і критеріїв класифікації інформації (передач), визначених Національною

радою відповідно до цієї статті, самостійно відносить передачі до певної категорії та застосовує відповідні попередження (символи).

Разом з цим, слід розуміти, що будь-яким змінам до чинного законодавства в частині захисту дітей від шкідливого медіа контенту має передувати проведення їх широкого громадського обговорення із залученням медіа експертів та представників галузі телебачення.

Література:

1. Про охорону дитинства : Закон України від 26 квітня 2001 р. № 2402-III // Відомості Верховної Ради України. – 2001. – № 30. – ст. 142. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2402-14/page

2. Про телебачення і радіомовлення : Закон України від 21 грудня 1993 р. № 3759-XII // Відомості Верховної Ради України. – 2006. – № 18. – ст. 155. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/3759-12

3. Про захист суспільної моралі : Закон України від 20 листопада 2003 р. № 1296-IV // Відомості Верховної Ради України. – 2004. – № 14. – ст. 192. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/1296-15

4. Європейська конвенція про транскордонне телебачення від 5 травня 1989 р. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/994_444

5. Мудрак Л.М. Європейський Союз ставить вимоги щодо захисту дітей від шкідливого контенту в ефірі перед кожною державою, що прагне до нього приєднатися // – Режим доступу : http://osvita.mediasapiens.ua/mediaprosvita/kids/zakhist_ditey_vid_shkidlivogo_kontentu_evropeyskiy_dosvid/

6. Нацрада затвердила нову систему аудіовізуальних позначок контенту. – Режим доступу : http://detector.media/rinok/article/113434/nacrada_zatverdila_novu_sistemu_vizualnih_poznachok_kontentu/

7. Проект Закону України «Про внесення змін до Закону України «Про телебачення і радіомовлення» (нова редакція). – Режим доступу : http://comin.kmu.gov.ua/control/uk/publish/article?art_id=121247&cat_id=80453

К. В. Юдкова,
аспирант НИИИП НАПрН Украины,
преподаватель кафедры информационного права
и права интеллектуальной собственности
ФСП НТУУ «КПИ»

ОБЕСПЕЧЕНИЕ ПРАВ ЧЕЛОВЕКА В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ: ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Мы живем в мире, где информационные и коммуникационные технологии (ИКТ) и обширные потоки информации стали естественными и несомненные чертами современной жизни.

Сегодня права человека в информационной сфере, фактически, включают:

• Право на доступ к Интернету;

• Право на полноценную жизнь с использованием Интернета;

• Право на сбалансированное использование Интернета в повседневной жизни;

• Право на свободу слова и выражения в Интернете.

• Право на образование, знания и связи с использованием Интернет.

Названные права приводят к возникновению основных направлений организационно-технических сложностей и задач, которые необходимо решать. Названные направления можно классифицировать по следующим группам:

1) «End user» - конечный пользователь – соблюдение прав конкретного человека, защита его чести и достоинства, других неимущественных прав, связанных с человеческой индивидуальностью;

2) «Legal frameworks» - правовые рамки – законодательное регулирование имеет меньшую динамику в развития, нежели процесс формирования новых общественных отношений;

3) «Jurisdictional complexity» - юрисдикционная сложность – здесь мы подразумеваем проблему кроссрегионального распространения информации.

То есть, как результат отсутствия фактических границ и рубежей для распространения информации возникает необходимость перманентного согласования национального права различных государств. Немаловажным является также процесс интеграции конкретного локального (государственного) права в мировую практику;

4) «Technological complexity» - технологическая сложность – высокие скорость и оборот прогресса и разработки новых технологий с непредсказуемыми, зачастую негативными, последствиями для прав человека

5) B2B и B2G отношения - взаимоотношения бизнес-бизнес и бизнес-государство в сфере обеспечения прав человека.

Многие компании уже предпринимают мощные шаги, чтобы ИКТ донести более широкой глобальной аудитории. Так, например, компания Unilever установила партнерские отношения с Facebook под руководством альянса Internet.org, чтобы понять, как предоставить доступ в Интернет миллионам людей по всей сельской местности Индии (в настоящее время только 11,4% индийского населения имеет доступ к Интернету [1]).

Альянс Internet.org - глобальное партнерство между лидерами в области технологий, некоммерческих организаций, местных общин и экспертов, которые совместно работают над «Расширение доступа в Интернет с целью донести Интернет до двух третей населения земного шара, что не имеет его» [2]. Основатели и партнеры: Ericsson, Facebook, Mediatek, Nokia, Opera, Qualcomm и Samsung.

Следующим примером B2B и B2G отношений является проект, созданный Amnesty International. Так, компания разработала «panic button» (русск. "кнопку паники") приложение – имеет интуитивно понятный интерфейс и реализацию в форме стандартной утилиты, - которое позволяет пользователям тайно отправлять уведомления к заранее выбранным контактам путем быстрого нажатия на кнопку включения телефона (или любую другую внешнюю кнопку на корпусе). Одна из преследуемых целей: предоставить журналистам, которые подвергаются нападению или

задержаны, возможность об этом сообщить компетентным лицам. Описанное имело место в 2010 году. А сегодня похожей кнопкой оснащены практически любые мобильные гаджеты.

Вместе с тем, развитие B2B и B2G отношений в сфере обеспечения прав человека имеют также и ряд негативных аспектов. Так, во многих странах интернет-компании сталкиваются с требованиями, ограничить доступ к веб-сайтам, удалить пользовательский контент или предоставлять личную информацию правоохранительным органам или иным государственным структурам. Риски для прав человека, свободы слова и неприкосновенности частной жизни имеют отношение ко всей цепочке ИКТ. Например, внедрение системы контроля использования ИКТ во время выборов в Иране вызвало серьезные общественные обсуждения и привлекло внимание ряда правозащитных организаций. А выявление уязвимости телекоммуникационных провайдеров услуг государственным требованиям в Египте привело к массовым закрытиям таких провайдеров.

Таким образом, можно выделить несколько «risk drivers» (русск. «зон риска»):

1) Телекоммуникации Услуги (например, требования государства раскрыть тайну частной информации для оказания помощи правоохранительным органам или по иным причинам);

2) Сотовые телефоны и мобильные устройства (риски нарушения конфиденциальности, которые вызваны возможностью скрытого определения местоположения);

3) Интернет-сервисы (возможность как правомерно, так и неправомерно получить доступ к содержимому фильтра удалить, блокировать или отключить отдельные учетные записи пользователей, а также существенные риски хранения информации с использованием т.н. облачных ресурсов);

4) Бытовая электроника (риски установки специального программного обеспечения с целью скрытого наблюдения и снятия информации).

Во взаимосвязи между правами человека, бизнесом, правительством, правоохранительными органами, а также интересами национальной безопасности очень важно иметь четкое представление о некоторых специфических особенностях таких отношений. Названную специфику можно достаточно точно описать утверждением, которое отлично выразил в 2008 году Специальный представитель Генерального секретаря Организации Объединенных Наций по вопросам бизнеса и прав человека: государства обязаны защищать права человека, а компании несут ответственность за неуважение к правам человека [3].

В указанных взаимоотношениях необходимо обозначить следующих два нюанса:

во-первых, существуют законные основания для государства (наблюдательные, контролирующие, правоохранительные органы) и различных компаний для ограничения свободного потока информации (например, удаление изображений насилия) или, наоборот, разрешения доступа к личной информации (например, борьба с мошенничеством, терроризмом). В данном контексте может идти речь о позитивном вмешательстве, поскольку основной целью является защита прав человека;

во-вторых, в то время как указанная деятельность (оправданное вмешательство) в приведенных примерах проводится с позитивными целями, тем не менее, всегда существует риск того, что внешняя организация (государственные или частные структуры) потребуют перевести частную жизнь в сферу публичной, - для её защиты, обеспечения прозрачности и т.д. То есть, создать законные основания для вмешательства. В данном случае уместным будет указать в качестве примера информационную резервацию Северной Кореи.

Контраст между названными особенностями взаимоотношений велик. Таким образом, наиболее верным подходом будет соблюдение определенного баланса:

- прозрачность законодательного регулирования;

- согласованность национального права и международных норм и практик;

- практика оправданного вмешательства;

- индивидуальный и ситуативный подход.

Литература

1. Данные International Telecommunication Union [Электронный ресурс] – Режим доступа: http://www.itu.int/en

2. Официальный сайт Internet.org [Электронный ресурс] – Режим доступа: https://info.internet.org/en/

3. Данные официального сайта The Office of the United Nations High Commissioner for Human Rights (OHCHR) [Электронный ресурс] – Режим доступа: http://www.ohchr.org

==========***==========

Р. Стадник,
аспірант НДІІП НАПрН України,
заступник директора Департаменту інформації
та комунікацій з громадськістю, начальник Управління
забезпечення доступу до публічної інформації
Секретаріату Кабінету Міністрів України

ЗАБЕЗПЕЧЕННЯ ДОСТУПУ ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ ЯК ФАКТОР ВІДКРИТОСТІ ТА ПРОЗОРОСТІ ОРГАНІВ ВЛАДИ

Основною метою Закону України «Про доступ до публічної інформації» (далі – Закон) [1] - є забезпечення прозорості та відкритості діяльності органів влади шляхом створення ефективних та дієвих механізмів реалізації права кожного на доступ до публічної інформації. Які ж засоби забезпечення права на доступ до публічної інформації вже створені у органах влади?

Перш за все, з початку дії Закону, Урядом схвалено ряд підзаконних нормативно-правових актів, які розроблені за активної участі представників громадянського суспільства. Серед них: затвердження примірної форми та

порядку подання запитів на інформацію, граничних норм витрат на копіювання або друк документів, питання системи обліку публічної інформації та інші акти у сфері доступу до публічної інформації. Разом з тим, на виконання ст. 14 Закону розпорядники інформації зобов'язані утворити спеціальні структурні підрозділи або визначити відповідальних осіб, які організовують доступ до публічної інформації. Станом на січень 2016 року у 17% органах виконавчої влади функціонують структурні підрозділи з питань доступу до публічної інформації. У 34,1% органах визначено відповідальних осіб. Серед іншого, 48,9% органів виконавчої влади мають структурний підрозділ у складі відділу/управління/департаменту [6]. Також розроблені форми, порядок складення та подання запитів на інформацію поштою чи електронною поштою, телефоном чи факсом; створено електронні адреси, відкрито телефонні та факсові лінії із максимально спрощеною процедурою подання запиту.

Один із видів доступу до публічної інформації - «активний», який з точки зору запитувачів, полягає у обов'язку розпорядників інформації надавати інформацію у відповідь на їхні запити [4]. Як свідчать результати анкетування органів виконавчої влади, проведеного Секретаріатом Кабінету Міністрів, в період з 9 травня 2011 року по грудень 2015 року, робота щодо розгляду запитів органами влади триває. Так, органами виконавчої влади за вказаний період розглянуто 216581запит на інформацію [6]. Секретаріатом Кабінету Міністрів України надано відповідь на 11684 запити на інформацію [5]. Найбільша кількість запитів була отримана Міністерством внутрішніх справ (58674), Київською міськдержадміністрацією (13708), Міністерством юстиції (11878), Адміністрацією Державної прикордонної служби (5224), Державною службою статистики (8460), Міністерством охорони здоров`я (7987), Державною фіскальною службою (6852), Харківською облдержадміністрацією (6339), Міністерством освіти і науки (5821), Міністерством соціальної політики (5268), Міністерством екології та

природних ресурсів(4366), Міністерством оборони (4243), Антимонопольним комітетом (3726), Міністерством економічного розвитку і торгівлі (3097), Міністерством регіонального розвитку, будівництва та житлово-комунального господарства (3036), Пенсійним фондом (2790), Державною міграційною службою (2494) [6].

Найбільш поширеними каналами надходження запитів залишається електронна пошта - 101676 (46,9% від загальної кількості). Звичайною поштою скористалися 88599 запитувачів – (40,9%), 5122 – факсом (2,4%), 1970 (0,9) – телефоном (2%), 19214 – іншими каналами (8,9%). Від фізичних осіб до органів виконавчої влади надійшло 140545 запитів (64,9%), від юридичних осіб – 48459 (22,4%), від об'єднань громадян без статусу юридичної особи – 13281 (6,1%), від представників засобів масової інформації – 14296 (6,6%) [6]. Переважну більшість запитувачів цікавила правова інформація (37341 запит), інформація про фізичеу особу (25252), статистична інформація (24005), довідково-енциклопедичного характеру (20611) [6].

Крім того, задля підвищення ефективності та прозорості діяльності органів державної влади розпорядники, які мають офіційний веб-сайт, зобов'язані оприлюднювати на ньому інформацію, передбачену законодавством про доступ до публічної інформації та Постановою Кабінету Міністрів України «Про порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади» [2]. Це так званий «пасивний» доступ до публічної інформації, який з точки зору запитувача означає, що інформація вже була оприлюднена розпорядником, і запитувачу не потрібно вчиняти активні дії із запитуванням такої інформації, а достатньо лише ознайомитися із поширеною інформацією [4]. Стаття 15 Закону встановлює перелік відомостей, що підлягають обов'язковому оприлюдненню розпорядником інформації. Зокрема, інформацію про свою діяльність, а саме: організаційну структуру, місцезнаходження, повноваження, структуру, поіменний керівний склад, їх службові номери

телефонів, адреси електронної пошти, розклад роботи та графік прийому громадян, порядок та умови надання послуг, обсяг та механізми витрачання бюджетних коштів, тощо. Важливо те, що розпорядники інформації зобов'язані серед іншого оприлюднювати прийняті ними рішення, тобто нормативно-правові акти, акти індивідуальної дії (крім внутрішньоорганізаційних) – не більше п'яти робочих днів з дня затвердження документа, а прийняті проекти рішень, що підлягають обговоренню – не пізніше двадцяти робочих днів до дати їх розгляду з метою прийняття [1].

Так, на веб-сайтах 13 органів виконавчої влади на 100% розміщено необхідну інформацію обов'язковість оприлюднення якої визначено статтею 15 Закону України «Про доступ до публічної інформації» (Державна архівна служба, Державна служба з питань інвалідів та ветеранів, Державне агентство водних ресурсів, Державне космічне агентство, Державний комітет телебачення і радіомовлення, Національне агентство з питань державної служби, Дніпропетровська, Волинська, Кіровоградська, Луганська, Одеська, Сумська та Харківська облдержадміністрації). Аналіз представлення видів інформації на веб-сайтах органів виконавчої влади, показав, що більше ніж на 50% веб-сайтів представлено 11 із 12 видів інформації [7].

Найменше представлено інформацію про систему обліку, види інформації, яку зберігає розпорядник», і яку висвітлено лише на 46% веб-сайтах. Це пов'язано з низкою проблемних питань. Переважно це стосується питань фінансування робіт щодо створення систем обліку публічної інформації, інтегрування її до офіційних веб-сайтів, уніфікації інтерфейсу, створення комплексної системи захисту інформації тощо. Загалом, станом на грудень 2015 року система обліку публічної інформації функціонує у 86 % органів виконавчої влади [6]. Для прикладу, заслуговує на увагу система обліку публічної інформації створена у Секретаріаті Кабінету Міністрів [8], яка функціонує на базі Урядового веб-порталу та повністю відповідає вимогам

визначеним у Положенні про систему обліку публічної інформації [3]. Досить оптимальною, зрозумілою, простою та зручною у використанні є система обліку публічної інформації, створена Міністерством юстиції України [9] та Кіровоградською облдержадміністрацією [10].

Разом з тим, у органів виконавчої влади під час забезпечення доступу до публічної інформації виникають проблемні питання щодо: опрацювання великої кількості кореспонденції з посиланням на Закон, які за змістом є зверненнями, роз'ясненнями, клопотаннями; стислих термінів надання відповідей за запитами на інформацію; захисту персональних даних в контексті доступу до публічної інформації; питання надання інформації з обмеженим доступом; відсутності окремого структурного підрозділу, який організовує доступ до публічної інформації тощо [6]. Наразі за рейтингом забезпечення права на доступ до інформації, розробленим провідними міжнародними організаціями Access Info Europe (Іспанія) та Democracy (Канада) Закон України «Про доступ до публічної інформації» посідає 19 місце серед 89 країн світу. Тому органи влади повинні вирішити ще багато завдань щодо створення ефективних та дієвих механізмів реалізації права кожного на доступ до публічної інформації. Адже, Закон гарантував відкритість та прозорість діяльності розпорядників інформації, а також створення умов для конструктивного діалогу «громадськість – влада».

Література

1. Закон України „Про доступ до публічної інформації" від 13.01.2011р. № 2939-VI (за станом на 13.01.2011) // Відомості Верховної Ради України, 2011, № 32, ст. 314.

2. Постанова Кабінету Міністрів України „Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади" від 4.01.2002 р. № 3 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/3-2002-%D0%BF.

3. Постанова Кабінету Міністрів України „Питання системи обліку публічної інформації" від 21.11. 2011 р. № 1277 [Електронний ресурс]. –

Режим доступу: http://www.kmu.gov.ua/control/uk/publish/article%3fshowHidden=1&art_id=244859044&cat_id=244394482.

4. Головенко Р., Котляр Д., Нестеренко О., Шевченко Т. Науково-практичний коментар до Закону України «Про доступ до публічної інформації» / За заг. ред. Д. Котляра / Під ред. А. Шевченка / Коорд. проекту В. Самохвалов. – К.: ГО «Фундація «Центр суспільних медіа»., 2012. – С. 336.

5. [Електронний ресурс]. – Режим доступу: http://www.kmu.gov.ua/control/uk/publish/article?art_id=248753203&cat_id=244316991.

6. Підсумки роботи із запитами на інформацію, що надійшли на адресу Секретаріату Кабінету Міністрів України з 9 травня 2011 року по 31 грудня 2015 року [Електронний ресурс]. – Режим доступу: http://www.kmu.gov.ua/control/uk/publish/article?art_id=248912580&cat_id=245633708.

7. Аналітична довідка за результатами моніторингу інформаційного наповнення веб-сайтів центральних та місцевих органів виконавчої влади [Електронний ресурс]. – Режим доступу: http://pdp.org.ua/images/stories/materials/Analit_Dovid_Sept_2012_WEB.pdf.

8. Єдиний веб-портал органів виконавчої влади України [Електронний ресурс]. – Режим доступу: http://www.kmu.gov.ua/control/pubinfo/search.

9. Система обліку публічної інформації Міністерства юстиції України [Електронний ресурс]. – Режим доступу: http://publinfo.minjust.gov.ua/.

10. Система обліку публічної інформації, яка є у володінні Кіровоградської облдержадміністрації [Електронний ресурс]. – Режим доступу: http://kr-admin.gov.ua/Public_info/.

==========***==========

Д. В. Іванов,
аспірант Міжрегіональної Академії
управління персоналом

СУСПІЛЬНЕ ТЕЛЕРАДІОМОВЛЕННЯ У СПРАВІ ЗАХИСТУ ПРАВ ЛЮДИНИ В УКРАЇНІ

Заважаючи на явно дежавоцентриський акцент дискусії, що точилася під час конференції, слід звернути увагу на проблеми, пов'язані з інституційністю та комплексним підходом у питанні захисту прав людини.

Дежавоцентриський акцент попередніх виступів яскраво демонструє маргіналізацію обговорень ролі громадянського суспільства в питанні захисту прав людини та проблем, що спіткають його на цьому поприщі. Він нівелює цінність обговорень, оскільки звужує питання, які мали б бути охоплені, маргіналізує одні аспекти і робить натиск на інші, спотворюючи реальну картину та перешкоджаючи цілісному обговоренню проблем захисту прав людини в інформаційному суспільстві. Державоцентризм у даному випадку можна розглядати як дволикого Януса – найбільший порушник прав людини виступає найбільшим правозахисником.

Тому акцент потрібно поставити на питанні проблем захисту прав людини, з якими стикаються громадські організації та актори, які можуть відігравати у цьому питання факультативну роль.

Розширення суб'єктів може бути рішенням проблеми обмежених ресурсів для захисту прав людини, про які зазначали попередні доповідачі. Відповідь ця передбачає реалізацію комплексного підходу до питання захисту прав людини. Через розширення кола суб'єктів, впровадження механізмів залучення широкого кола акторів, які зможуть впливати на захист прав, можливою буде реалізація ідеї комплексного підходу у цьому питанні.

Прикладом факультативного елементу захисту прав людини є відповідна робота телерадіомовлення. Роль медіа тут є роллю посередника, має диспозитивний характер – може реалізовуватися, може не реалізовуватися (на розсуд редакційної політики). На прикладі діяльності

інституту суспільного телерадіомовлення автор продемонструє можливість реалізації комплексного підходу та проблему більш глибоку – недооцінку потенціалу суспільного телерадіомовлення законодавцем України.

У 2014 році ухвалено Закон України «Про Суспільне телебачення і радіомовлення України» (надалі - Закон).

Відповідно до частини другої статті 1 Закону Суспільне телебачення і радіомовлення утворюється у формі публічного акціонерного товариства «Національна суспільна телерадіокомпанія України» (далі – НСТУ).

Частина перша статті 1 Закону передбачає, що Суспільне телебачення і радіомовлення створюється з метою залучення громадян до обговорення та вирішення найважливіших соціально-політичних питань. Положення це можна розглядати у контексті реалізації свободи слова, воно ж підкріплюється і нормою пункту 5 частини першої статті 3 Закону, відповідно до якої принципом діяльності НСТУ є вільне вираження поглядів, думок і переконань. Ще одним важливим для дослідження і базовим принципом суспільного мовлення є принцип пріоритету суспільних інтересів над комерційними та політичними.

Слід зауважити, що для реалізації закріплених у Законі мети створення суспільно телерадіомовлення України та наведених вище принципів діяльності НСТУ, у цьому ж Законі повинні бути передбачені відповідні норми, які її (реалізацію) забезпечували. Тобто, згадані декларативні норми повинні бути підкріплені нормами процедурного змісту, або ж нормами, які визначають основні завдання організації та відповідають меті та принципам її діяльності. Це вказувало б на те, що мета створення Суспільного мовлення в Україні - залучення громадян до обговорення та вирішення найважливіших соціально-політичних питань та базові принципи організації - вільне вираження поглядів, думок і переконань, пріоритету суспільних інтересів над комерційними та політичними, насправді реалізуються, а не наявні у Законі виключно як лозунги, що прикрашають зміст акту.

Проте аналіз завдань НСТУ, визначених у статті 4 Закону, дає підстави стверджувати, що згадані декларативні норми дійсно прикрашають зміст Закону. Це пояснюється тим, що єдина можливість реалізації вказаних принципів є опосередкованою.

Аналіз завдань НСТУ вказує на те, що організація реалізує державну інформаційну політику, визначену Парламентом, а єдиним завданням, що гарантує реалізацію принципу вільного вираження поглядів, думок і переконань, є внесена поправками до Закону норма 2015 року щодо забезпечення збалансованого і прозорого доступу суб'єктів суспільно-політичного життя до програм (передач) дискусійного формату, зокрема у вигляді дебатів. Опосередкованість, про яку згадувалося вище, полягає у тому, що, скажімо, народний депутат, представлятиме своє бачення в питанні обговорення суспільно-політичних питань.

Відтак, фактично мова йде про створення Суспільного телерадіомовлення не з метою залучення громадян до обговорення та вирішення найважливіших соціально-політичних питань, але з метою рівного доступу суб'єктів суспільно-політичного життя до можливості нав'язувати громадянам свою наррацію. Це відповідає європейським стандартам, але, на думку автора, вказує на девіацію розвитку суспільного телерадіомовлення, яке у даному випадку виступає яскравим прикладом того, що тенденція змішування суспільних інтересів з державними (здебільшого з політичними) не є найкращим розв'язанням для функціонування демократичних ЗМІ. Згадана девіація демонструє одержавлення того, що мало б бути суспільним.

Щодо зв'язку наведеного вище з питанням захисту прав людини.

Аналізуючи телепрограми приватних мовників на медіаринку України, бачимо, що окремі з них реалізують мету створення в Україні суспільного мовлення - залучають звичайних громадян до обговорення суспільно-політичних питань, чого не реалізує суспільний мовник. Крім того, аналіз телепрограм приватних мовників вказує на ще одну функцію, яку мав би виконувати суспільний мовник, вона ж може розглядатися як елемент

захисту порушених прав людини. Приватні канали сигналізують про проблему масового порушення прав і зазвичай після медіа скандалів Уряд вимушений реагувати на ситуацію.

Інформування комерційним мовником про порушення часто супроводжується відстоюванням чиїхось інтересів, тому не завжди на нього можна покладатися. Натомість суспільний мовник, виконуючи покладені на нього завдання та місію, керуючись приматом суспільного інтересу (блага) повинен реалізовувати сигнальну функцію через надання можливості громадянам повідомляти про те, що не вкладається у рамки державної інформаційної політики і не відповідає політичним інтересам.

Аналіз Закону, а також телепрограм у правозахисному контексті дає підстави до висновків. Суспільне мовлення, як і приватне мовлення, може своєю діяльністю реалізовувати певні елементи з системи заходів захисту прав людини, а саме: моніторинг; повідомлення про порушення прав людини; звітування перед публічністю про перебіг справи щодо усунення порушення органами публічної влади. Такий алгоритм дій може бути прийнятий як елемент функціонування НСТУ зважаючи на мету створення суспільного мовлення та його служіння суспільним інтересам.

Відтак, із зазначеного виникає, що потенціал інституту суспільного мовлення законодавцем недооцінено і, незважаючи на наявні у Законі декларативні норми щодо служіння суспільним інтересам, залучення громадян до обговорення та вирішення найважливіших соціально-політичних питань та реалізації свободи слова, парламентарями не було виписано належним чином завдання суспільного мовлення, які у актуальному Законі в певних аспектах суперечать меті створення суспільного мовлення в Україні та його принципам.

Потенціал цей у контексті захисту прав і свобод людини, тісно переплітається з реалізацією суспільним мовником декларативних положень Закону щодо залучення громадян до обговорення та вирішення

найважливіших соціально-політичних питань, а також реалізації принципу пріоритету суспільних інтересів над комерційними та політичними.

==========***==========

Н. С. Мороховська,
к.ф.н., доцент кафедри
публічного права ФСП НТУУ «КПІ».

ЕТИЧНІ ПРИНЦИПИ КІБЕРПРОСТОРУ ТА ЇХ ІНТЕРПРЕТАЦІЯ ЧЕРЕЗ ПРИЗМУ ПРАВ ЛЮДИНИ

Теоретично в умовах інформаційного суспільства кожен може використовувати технічні засоби, що відкривають небувалі донині можливості по здійсненню прав і свобод людини. Це дозволяє масам людей брати участь у спільному розвитку суспільства і в універсалізації прав і свобод. Але необхідно також брати до уваги згубні чи негативні наслідки й конфлікти інтересів, які здатні поставити під сумнів реалізацію цих нових можливостей, особливо враховуючи стрімкий розвиток сучасних технологій. Зараз існує нагальна необхідність виявити і проаналізувати позитивні й негативні наслідки застосування інформаційно-комунікаційних технологій (ІКТ), а також протиріччя між правами, свободами і цінностями.

Подальшого дослідження вимагають проблеми безпеки і управління інтернетом з метою оптимізації можливостей, що виникають завдяки розширенню доступу до інформації, знанням і культурі, і перетворенню користувачів в активних учасників глобального інформаційного суспільства (за рахунок більшої свободи вираження думок, здібності продукувати контент і створювати соціальні мережі), виходячи при цьому з необхідності захисту окремих користувачів від наслідків неналежного використання інформаційно-комунікаційних технологій.

Етичні аспекти інформаційного суспільства були і залишаються у фокусі уваги фахівців. Зокрема, слід згадати про Всесвітній саміт з інформаційного суспільства (ВСІС), Женева, 2003 р.; Форум з управління Інтернетом, кілька

регіональних конференцій ЮНЕСКО. Продовжується робота у цьому напрямку з боку Ради Європи і Комісії Франції у справах ЮНЕСКО в рамках підготовчого і постпроектного етапів Всесвітнього саміту з інформаційного суспільства. Формується Етичний кодекс ЮНЕСКО.

З етичними аспектами інформаційного суспільства, перш за все, пов'язані такі права людини, як:

- свобода вираження думок;
- право на інформацію, доступ до неї та інтелектуальну власність;
- право на приватне життя і його недоторканність, таємницю онлайн листування;
- культурне і мовне різноманіття інтернет-контенту;
- медіаосвіта.

Навіщо потрібні етичні принципи?

Пітер Фляйшер із компанії «Google» заявляв про те, що, оскільки інфраструктура Інтернету має глобальний характер, необхідно, щоб і сам Інтернет регулювався глобально, навіть якщо це означає саморегуляцію. Ця заява співпадає із заявою «Google» про необхідність створення всезагальної хартії про захист персональних даних. Однак реальність комунікації в спільному просторі така, що кожен виражає власні очікування, переконання та цінності, ризикуючи при цьому вступити в конфлікт, або – ще гірше – *не бути почутим*. Неважко здогадатись, що люди, які будуть незадоволені тим, що їх не поважають чи не чують, залишать простір діалогу. В 1950 р. було простіше проголошувати загальні права людини (зокрема, свободу вираження думки), ніж сьогодні, коли у своїй власній оселі та в своєму приватному житті ми стикаємося з таким різноманіттям уявлень про світ.

Вже зараз існує рух, що пропагує вихід з Інтернету (припинення користування Інтернетом), зокрема в Каліфорнії, одному з місць зародження ІКТ. Є приклад Китаю, де в ім'я державного суверенітету створені технічні

перепони на шляху комунікації, обміну повідомленнями і інформацією. Цей приклад може бути використаний і іншими країнами.

Очевидним є те, що недостатньо проголосити єдність і глобальний характер інфраструктури, щоб уникнути небезпеки її руйнування. Згідно із заявою ВСІС, Інтернет повинен залишатись світовим суспільним ресурсом. А це можливо лише шляхом діалогу, а точніше, шляхом пошуку *загальних етичних принципів,* заснованих на повазі фундаментальних відмінностей людей, груп, співтовариств, країн, і головне – забезпечення дотримання цих принципів (в тому числі законодавчим шляхом).

Про які ж етичні принципи йдеться?

Сучасні дослідження й дискусії в цьому питанні сходяться у визнанні двох основних етичних принципів. **Перший –** це *повага гідності людини і її первинної автономності* (здатності керувати собою, спираючись на власні принципи), тобто здатності до особистого розвитку. **Другий –** полягає в «моральному, навіть юридичному зобов'язанні *солідарності й соціальної справедливості*».

Гідність, виходячи із вчення І. Канта, означає переконання в тому, що людина є самоціллю і що вона ніколи не може бути засобом для досягнення цілі, будь то економіка чи безпека. Саме цей етичний принцип закладено в основу Уставу ЮНЕСКО, зокрема, в преамбулі. Цікаво, що з 1998 р. цей же принцип проголошено в якості однієї з фундаментальних цінностей Конфедерації Європейських асоціацій користувачів комп'ютерів.

Але чи можна говорити про гідність тепер, коли в епоху «інтернету речей», де цінність людини, точніше, її статус в мережах, роботу яких вона не може контролювати, зводиться до статусу оточуючих її речей, з якими вона взаємодіє? Чи можна говорити про повагу до особистості, коли системи функціонують в непрозорому режимі на основі баз даних і метаданих, віддалених від індивідуального «я»?

Солідарність і соціальна справедливість – ще два тісно взаємопов'язаних принципи. Солідарність передбачає зацікавленість у тому,

щоб залучати оточуючих у всі наші дії – індивідуальні, колективні. Однак тут надзвичайно важливим є ввічливе і поважне ставлення до інших, навіть до тих, кого ми не знаємо і не бачимо в процесі комунікації. Здається слушною думка Кароля Якубовича, який зауважував, що в Інтернеті слід висловлюватися так, як би ми говорили зі своєю матір'ю.

Соціальна справедливість у кіберпросторі пов'язується з тим, щоб кожна людина стала членом інформаційного суспільства, мала право на загальний доступ не тільки до інфраструктури, а й до певного значимого контенту, можливість користуватися новими технологіями.

Не дивлячись на критику й негативні відгуки про існуючі етичні кодекси інтернету в пресі, експерти наполягають на розширенні кількості етичних кодексів для тих, кому вони необхідні: **професіоналам** сфери інформаційних технологій, які завдяки таким кодексам і такій деонтології зможуть спонукати компанії замислюватись над тим, на які цінності їм слід орієнтуватись при реалізації технологій; **користувачам** і їх спільнотам, яким кодекси допоможуть усвідомити вразливість інших учасників дискусійних форумів і онлайнових ігор; **віртуальним викладачам і бібліотекарям**, для яких повинен бути очевидним обов'язок бути неупередженим. Робота серверів діалогових чи азартних ігор також повинна підкорятися певним правилам, для того, щоб захистити дітей і підлітків й не допускати ігроманії. Більше того, ставиться питання про **деонтологію онлайнової журналістики** і навіть робототехніки.

Для забезпечення певної міри легітимності цих кодексів необхідно і доцільно, щоб процес їх створення не відбувався всередині закритих груп, а будувався на діалозі з тими, хто зацікавлений у їх створенні, з урахування інтересів кожної сторони. Зміст етичних кодексів повинен відповідати існуючим правовим нормам. Важливо, щоб кодекси були своєрідним доповненням, продиктованим турботою про належне ставлення до фундаментальних етичних принципів – *поваги гідності і автономії особистості, солідарності й соціальної справедливості.*

Існує зв'язок між «етикою» інформаційного суспільства, що формується, з одного боку, і правами людини з іншого. Очевидним є те, що саме етиці судилося привести нас до усвідомлення принципів, на яких слід будувати інформаційне суспільство. Але ці принципи повинні знайти продовження в *утвердженні* тих прав, які вони проголошують і підтримують.

==========***==========

І. В. Казьмірова,
юрисконсульт 1 категорії
відділу претензійно-позовної роботи
юридичного управління НТУУ «КПІ»

ПРАВОВА ІНФОРМАЦІЯ: ПОНЯТТЯ ТА ДЖЕРЕЛА

Поняття «правова інформація» з’явилось ще у 1992 році одночасно з прийняттям Закону України «Про інформацію». До цього часу, закріплене на законодавчому рівні визначення даного поняття жодним змінам та доповненням не піддавалось.

В науковій літературі значна увага приділяється саме поняттю інформації. Натомість, практично відсутні окремі наукові здобутки, предметом яких була б саме правова інформація. В контексті розглядуваної нами теми, можна згадати хіба що О. О. Тихомирова, який досліджував теоретико-правові аспекти правової інформації.

Відтак, вважаємо за необхідне проаналізувати визначення правової інформації, яке міститься у ст. 17 Закону України «Про інформацію» на предмет необхідності внесення змін. Також слід приділити увагу й питанню щодо джерел правової інформації, переліченим у статті 17 згадуваного закону.

Відповідно до ч. 1 ст. 17 Закону України «Про інформацію», правова інформація – будь-які відомості про право, його систему, джерела,

реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо [1].

Як бачимо, О. О. Тихомировим вірно було зазначено, що Закон України «Про інформацію» практично необмежено трактує поняття «правова інформація» [2, с. 30]. І це не випадково, адже на сьогодні правова інформація вбирає в себе значний масив суспільно важливої інформації.

Для порівняння, в Республіці Білорусь правова інформація являє собою тексти та обов'язкові реквізити правових актів, які складають законодавство Республіки Білорусь, в тому числі міжнародних договорів Республіки Білорусь.

Слід розпочати з того, що згадувані в контексті даного визначення реалізація права, юридичні факти та правовідносини в теорії права виступають в якості елементів механізму правового регулювання. Останній, являє собою взяту в сукупності систему правових засобів, за допомогою яких здійснюється правове регулювання суспільних відносин.

У зв'язку з цим, вважаємо за необхідне в ч. 1 ст. 17 Закону України «Про інформацію» слова «реалізація права, юридичні факти, правовідносини» замінити на «механізм правового регулювання».

Також пропонуємо виключити з ч. 1 ст. 17 Закону України «Про інформацію» слова «та їх профілактику», оскільки боротьба з правопорушеннями фактично включає в себе профілактику.

Таким чином, пропонуємо визначити правову інформацію як будь-які відомості про право, його систему, джерела, механізм правового регулювання, правопорядок, правопорушення і боротьбу з ними тощо.

Частина 2 ст. 17 Закону України «Про інформацію», визначає, що джерелами правової інформації є Конституція України, інші законодавчі і підзаконні нормативно-правові акти, міжнародні договори та угоди, норми і принципи міжнародного права, а також ненормативні правові акти, повідомлення засобів масової інформації, публічні виступи, інші джерела інформації з правових питань [1].

На нашу думку, необхідно доповнити даний перелік словами «офіційні друковані видання», виходячи з наступного.

У відповідності до Указу Президента України «Про порядок офіційного оприлюднення нормативно-правових актів та набрання ними чинності», закони України, інші акти Верховної Ради України, акти Президента України, Кабінету Міністрів України не пізніш як у п'ятнадцятиденний строк після їх прийняття у встановленому порядку і підписання підлягають оприлюдненню державною мовою в офіційних друкованих виданнях.

При цьому, нормативно-правові акти, опубліковані в інших друкованих виданнях, мають інформаційний характер і не можуть бути використані для офіційного застосування. Громадяни, державні органи, підприємства, установи, організації під час здійснення своїх прав і обов'язків повинні застосовувати закони України, інші акти Верховної Ради України, акти Президента України і Кабінету Міністрів України, опубліковані в офіційних друкованих виданнях або одержані у встановленому порядку від органу, який їх видав [3].

Таким чином, у науковій літературі майже не приділяється уваги питанням щодо поняття правової інформації та її джерел, що унеможливлює проведення більш ґрунтовного дослідження шляхом співставлення та порівняння різних підходів. Тому, виключно на основі аналізу ст. 17 Закону України «Про інформацію», нами було викладено власне бачення і з наведенням відповідних обґрунтувань запропоновано внести певні зміни та доповнення.

Література

1. Закон України «Про інформацію» від 02 жовтня 1992 р. № 2657-XII // Відомості ВВР України, 1992, № 48, С. 650.

2. Тихомиров О. О. Правова інформація: теоретико-правовий аспект // О. О. Тихомиров / Інформаційна безпека людини, суспільства, держави. - № 1 (8). – 2012. – С. 29 - 35.

3. Указ Президента України «Про порядок офіційного оприлюднення нормативно-правових актів та набрання ними чинності» від 10 червня 1997 р. № 503/97 // Офіційний вісник України, 1997, № 24, С. 11.

==========***==========

А. М. Бежевець,
ст. викладач ФСП НТУУ «КПІ»

ДЕЯКІ АСПЕКТИ ВІДПОВІДАЛЬНОСТІ ЗА ПОШИРЕННЯ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ

Людина являє собою складну соціально сформовану особистість, яка відчуває постійну потребу в спілкуванні. Причому ця потреба не тільки виходить за межі біологічних або професійних потреб, а й нерідко стає переважаючою.

Сучасні технології значно спрощують можливість швидкого обміну інформацією між людьми за допомогою Інтернет-технологій. Щоденно кількість інформації на просторах Інтернету збільшується.

На даному етапі розвитку Інтернет-технологій чітко вбачається все більша спрямованість на соціалізацію. Внаслідок спрощення можливості доступу до мережі Інтернет шляхом постійного збільшення WI-FI точок доступу, впровадження в Україні 3G стандарту зв’язку у людей з'являються величезні можливості для роботи, спілкування і реалізації своїх планів.

Інтернет-комунікації сьогодні можна розглядати як особливе соціальне середовище. У ньому є специфічна мова взаємодії; специфічні норми взаємодії; виборча трансляція соціальних стандартів; своя соціальна ієрархія, в основі якої лежить можливість впливу на хід комунікації. На відміну від звичайної реальності, Інтернет-середовище характеризується набагато більшою соціальною невизначеністю - і в силу своєї динаміки, і в силу принципової безмежності, і в силу наявності більшої різноманітності можливостей комунікацій.

Однією із найпоширеніших форм спілкування на даний час є спілкування в соціальних мережах.

На тлі цієї тенденції в сучасному українському суспільстві найбільш популярними є такі Інтернет - спільноти, як соціальні мережі і різні мікроблоги. Найбільш популярними мережами в світі є Facebook, My space та Twitter, в Україні - «ВКонта́кте» та «Однокла́ссники».

Відповідно до нещодавно проведеного дослідження (станом на жовтень 2015 року) аудиторія соціальних мереж в Україні розподілилась наступним чином:

- «ВКонта́кте» — 13 млн. користувачів.
- «Однокла́ссники» — 8,5 млн. користувачів.
- «Facebook» — 6,9 млн. користувачів.

Зазначеним дослідженням також встановлено, що понад 90 відсотків користувачів «ВКонта́кте» мають свою сторінку в «Однокла́ссники» чи «Facebook».

Таким чином, в Україні виникло, існує та розвивається нове соціальне явище – Інтернет-спільноти.

Однією із основних причин набуття такої популяризації соціальних мереж є те, що вони є не тільки засобом комунікації людей, але й певним механізмом соціального самовираження особистості. Звичайно, не завжди висловлювання своїх думок, настроїв та переконань не порушує права інших осіб або навіть охоронювані державою інтереси.

В сучасних умовах соціальні мережі в Інтернеті використовуються як інструмент швидкого поширення будь якої інформації. Нажаль, нерідко користувачі мережі Інтернет стають жертвами маніпуляцій, обману чи приниження честі і гідності з боку інших користувачів, що призводить до зниження рівня моральності та системного заподіяння шкоди законним правам та інтересам громадян і суспільству, та, навіть, інтересам держави.

Враховуючи масштаби цього явища, підставно зробити висновок, що заходів саморегулювання соцмереж (які притаманні будь-якій спільноті) вже

недостатньо, і воно потребує певного правого регулювання. Іншими словами, кожен користувач має усвідомлювати можливість настання відповідальності за свою безвідповідальну поведінку у соціальних мережах.

Одними з найголовніших функцій держави є охорона і захист конституційного ладу, законності та правопорядку, забезпечення миру, прав, свобод та законних інтересів людини і громадянина.

Відтак держава не може лишатися осторонь зазначеного суспільного явища. Яскравим прикладом на підтвердження необхідності правового регулювання цього соціального явища є кримінальна справа № 591/442/16-к за обвинуваченням громадянина України, уродженця міста Суми, у вчиненні кримінального правопорушення, передбаченого ч.3 ст.109 Кримінального кодексу України (публічні заклики до насильницької зміни чи повалення конституційного ладу або до захоплення державної влади, а також розповсюдження матеріалів із закликами до вчинення таких дій з використанням засобів масової інформації).

Під час розгляду справи було встановлено, що обвинувачений, перебуваючи у власній квартирі, використав свій персональний комп'ютер, підключений до мережі Інтернет, для опублікування на персональній сторінці у соціальній мережі «Вконтакте» під назвою «Богдан Мазепа» публічних, прямих закликів до користувачів соціальної мережі насильно позбавити влади чинний уряд та сформувати в Україні нову державу.

Вироком суду від 02.02.2016 зазначена особа була визнана винною та притягнута до відповідальності за порушення конституційних приписів щодо порядку визначення і зміни конституційного ладу в Україні за допомогою використання сторінок в соціальній мережі.

Слід зазначити, що на законодавчому рівні визначення терміну «соціальна мережа» відсутнє. З аналізу матеріалів вказаної справи вбачається, що до нього застосовано норми, які стосуються засобів масової інформації.

Таким чином, держава повинна створити відповідний правовий інструментарій захисту прав її громадян, вжити заходів щодо нормалізації всіх сфер життя, захисту конституційного ладу, законності та правопорядку.

==========***==========

М. В. Дубняк,
аспірант НДІІП НАПрН України

ПРОБЛЕМИ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНИХ ПРАВ ГРОМАДЯН В МІСЦЕВОМУ САМОВРЯДУВАННІ

Конституція України встановлює, що єдиним джерелом влади в Україні є її народ, тому громадяни мають право брати участь в управлінні державними справами. При цьому народ може здійснювати свою владу як безпосередньо так і через органи державної влади і місцевого самоврядування [1]. Реалізація цього права можлива шляхом безпосередньої участі громадян в процесі прийняття рішень органами місцевого самоврядування (далі - ОМС).

Основною умовою для безпосередньої участі є забезпечення ефективної інформаційної взаємодія всіх суб’єктів ОМС, до яких відносяться громадянин, група громадян, територіальна громада, сільський, селищний міський голова, сільський, селищний староста, представницький орган місцевого самоврядування — Рада, з відповідним складом депутатів та комісій, виконавчий орган Ради [2].

Законодавство України визначає певні форми інформаційної взаємодії для суб'єктів ОМС: для громадян, групи громадян, територіальної громади — подання заяв, скарг, звернень, петицій та формування місцевих ініціатив; для депутатів, депутатських комісій, міських голів та Рад — інформування громади про поточну діяльність, про питання які виносяться на розгляд сесії, щорічні звіти депутатів.

Однак, в законодавстві недостатньо регламентована інформаційна взаємодія громадян з Радою і відповідна інформаційна взаємодія Ради з

громадянами, внаслідок недосконалого визначення прав та обов'язків суб'єктів інформаційних правовідносин. Ці обставини не дозволяють громадянам належним чином приймати безпосередню участь в процесі прийняття рішень, що різко зменшує їх якість. Таким чином, основним недоліком сучасного законодавства в частині забезпечення інформаційної взаємодії суб'єктів ОМС є обмеженість встановлених прав громадян на таку інформаційну взаємодію, а також не встановлення відповідних кореспондуючих обов'язків суб'єктів місцевої влади.

Отже, з метою підвищення спроможності в реалізації прав громадян на участь в місцевому самоврядуванні слід забезпечити ефективну інформаційну взаємодію, шляхом регламентації інформаційних прав та обов’язків для всіх суб'єктів ОМС на всіх етапах вирішення проблемних питань у місцевому самоврядуванні.

Міжнародними документами [3] та Конституцією України закріплено такі інформаційні права громадян, як право створення, поширення, зберігання, використання інформації. Відповідно до цього органи місцевого самоврядування повинні мати обов'язок щодо надання будь-якої інформації про свою діяльність з визначенням відповідальності за порушення інформаційних прав, наприклад, в частині неповноти наданої інформації або відмови щодо її надання. А з іншого боку, суб’єкти владних повноважень місцевого самоврядування повинні нести відповідальність за не опрацювання інформаційних звернень та запитів громадян

Вочевидь, реалізація права громадянина на участь в управлінні державними справами та вирішення питань місцевого значення обумовлюється можливістю на отримання повної, своєчасної, достовірної інформації про діяльність відповідного ОМС. Це право громадянина кореспондує обов'язок ОМС забезпечити надання такої інформації. Але законодавству України бракує детальної регламентації забезпечення інформаційних прав та виконання інформаційних обов'язків суб'єктами ОМС.

Декілька років в Україні діють нормативні акти, які регламентують порядок оприлюднення інформації, в тому числі і на офіційних веб-сайтах [4]. Однак, ці норми стосуються надання лише формальної інформації про організаційну структуру органу, плани робити, нормативні акти та їх проекти тощо. При цьому, не зважаючи на правову регламентацію щодо обов'язку ОМС опубліковувати зазначену інформацію, внаслідок недбалого виконання законодавчих приписів інформованість громадян в цій частині залишається низькою. Наприклад, на сайтах недостатньо інформації про організацію роботи та склад Ради, не забезпечується інформаційна прозорість процесу прийняття рішень з певного питання, звітування депутатів та міських голів про свою діяльність.

Додатково наголосимо, що механізм індивідуальних запитів громадян до ОМС з приводу отримання конкретної інформації, який регламентовано законом України “Про доступ до публічної інформації” [5], не в повній мірі здатен задовольнити інформаційні права та потреби громадян. Оскільки має дуже обтяжений у виконанні механізм звернення, пошуку та надання публічної інформації за запитом. Тому слід розглянути доцільність питання вдосконалення правових механізмів щодо реалізації інформаційних прав громадян.

Сучасність характеризується інтенсивною концентрацією міського населення, що збільшує навантаження на владних суб'єктів місцевого самоврядування. З метою ефективного забезпечення інформаційної взаємодії і як наслідок, підвищення якості прийнятих рішень доцільно впроваджувати нові ІКТ та інтернет-технології. Впровадження ІКТ створює потенційні умови для втілення в життя принципу прямої участі всіх членів громади у вирішенні питань місцевого значення.

Таким чином, вдосконалення правової регламентації забезпечення інформаційних прав та обов'язків всіх суб'єктів місцевого самоврядування є необхідною умовою втілення в життя конституційного припису щодо права народу здійснювати свою владу безпосередньо.

Список використаних джерел:

1. Конституція України : за станом на 15 березня 2016 року / Режим доступу: http://zakon5.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

2. Про місцеве самоврядування : за станом на 01 березня 2016 року / Режим доступу: http://zakon5.rada.gov.ua/laws/show/280/97-%D0%B2%D1%80

3. Конвенція про захист прав людини і основоположних свобод : за станом на 01 червня 2010 року / Режим доступу: http://zakon3.rada.gov.ua/laws/show/995_004

4. Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади : за станом на 01.01.2014 / Режим доступу: http://zakon5.rada.gov.ua/laws/show/3-2002-%D0%BF

5. Про доступ до публічної інформації : за станом на 01 травня 2015 року / Режим доступу: http://zakon5.rada.gov.ua/laws/show/2939-17

==========***==========

Д. О. Маріц,
к.ю.н., доцент кафедри
інформаційного права та права
інтелектуальної власності
ФСП НТУУ «КПІ»

ПРАВО ВИКОНАВЦЯ НА АВТОРСЬКУ ВИНАГОРОДУ ЗА СТВОРЕНИЙ ОБ'ЄКТ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В ПОРЯДКУ СЛУЖБОВИХ ОБОВ'ЯЗКІВ

Прийняття Загальної декларації прав людини (далі - Декларація) щорічно відзначається 10 грудня, та називається Днем прав людини або Міжнародним днем прав людини. Цей нормативний документ було перекладено більше ніж на 300 мов світу, крім того варто відзначити, що цей документ отримав таку високу оцінку у світі, яку не отримував жоден міжнародний документ. Тому, Декларація стала тим підґрунтям, що послужило побудові всієї системи міжнародного права.

Частиною 3 ст. 23 Декларації визначається, що кожний працюючий має право на справедливу і задовільну винагороду, яка забезпечує гідне людині існування, її самої та її сім'ї, і яка в разі необхідності доповнюється іншими засобами соціального забезпечення. Так, трудові відносини можуть виникати у найрізноманітніших сферах життя [1]. Однак предметом дослідження у цій роботі - є саме трудові відносини, які пов'язані зі сферою інтелектуальної, творчої діяльності. Тому актуальним видається питання про захист інтересів осіб, які в рамках своєї трудової діяльності працюють над створенням об'єктів інтелектуальної власності.

Цивільний кодекс України (далі – ЦК України) [2] у ст.... 429 в загальних рисах визначає права сторін на об'єкт права інтелектуальної власності, які виникають у зв'язку з виконанням трудового договору. Так, *особисті немайнові права інтелектуальної власності на об'єкт,* створений у зв'язку з виконанням трудового договору, належать працівникові, який створив цей об'єкт. У випадках, передбачених законом, окремі особисті немайнові права інтелектуальної власності на такий об'єкт можуть належати юридичній або фізичній особі, де або у якої працює працівник. *Майнові права інтелектуальної власності* на об'єкт, створений у зв'язку з виконанням трудового договору, належать працівникові, який створив цей об'єкт, та юридичній або фізичній особі, де або у якої він працює, спільно, якщо інше не встановлено договором. Водночас частиною третьою названої статті визначається, що *особливості здійснення майнових прав інтелектуальної* власності на об'єкт, створений у зв'язку з виконанням трудового договору, можуть бути встановлені законом. Це по суті означає, що в залежності від об'єкту права інтелектуальної власності, який створюється у зв'язку з виконанням трудового договору, необхідно застосовувати спеціальні нормативні правові акти. Зокрема, це можуть бути, Закон України «Про авторське право і суміжні права», ЗУ «Про охорону прав на винаходи та корисні моделі» [3], тощо.

Так, ***винаходом (корисною моделлю)*** є результат інтелектуальної діяльності людини в будь-якій сфері технології. ***Службовим винаходом*** (корисною моделлю) є винахід (корисна модель), створений працівником: у зв'язку з виконанням службових обов'язків чи дорученням роботодавця за умови, що трудовим договором (контрактом) не передбачене інше. З використанням досвіду, виробничих знань, секретів виробництва і обладнання роботодавця (ст. 1 ЗУ «Про охорону прав на винаходи і корисні моделі»).

У зв’язку із створенням об’єкта права інтелектуальної власності, у даному випадку винаходу, в порядку службових обов’язків, постають ряд питань, які потребують вирішення. Зокрема: яким чином врегульовується питання: щодо розрахунків з автором або авторами винаходу, якщо замовником і виконавцем виступають юридичні особи? Так, в першу чергу необхідно виходити з того, які насправді укладаються договори. Першим договором, який опосередковує відносини між двома юридичними особами щодо створення об’єкта права інтелектуальної власності може бути як договір підряду так і договір про створення об’єкта права інтелектуальної власності створений за замовленням. В свою чергу, юридична особа (виконавець) доручає визначеному колу осіб або одній особі, які перебувають у трудових відносинах з цією юридичною особою, провести науково-дослідні та експериментально-конструкторські роботи, щоб вирішити конкретну технічну проблему. Відповідно до ч. 1 ст.. 9 Закону України «Про охорону прав на винаходи і корисні моделі» *право на одержання патенту на службовий винахід (корисну модель) має роботодавець винахідника*. Таким чином, відповідно до зазначеної статті юридична особа, яка виступає замовником за договором підряду не має права на отримання патенту. В тім, виходячи із свободи договору, вважаємо що питання стосовно одержання патенту має вирішуватись у договорі, адже замовником виступає інша особа, а не роботодавець авторів.

Однак це не позбавляє кожного з власників, що використовують патент, обов'язку виплачувати винагороду авторам патенту. Тому в саме у випадку власник, який використовує патент, повинен виплачувати автору саме авторську винагороду (а не ділитися прибутком), у вигляді певного відсотка від прибутку, одержуваного від використання патенту.

Оскільки законом розмір авторської винагороди за використання патенту не визначений, суд може вдатися до висновку експерта-оцінювача, а також врахувати обсяг випуску продукції по патенту, понесені витрати, прибуток та інші показники.

Водночас аналізуючи судову практику, суди притримуються іншої позиції. Так із справи № 2-179/2011 вбачається, що якщо економічний ефект від винаходу відсутній, то це є підставою для відмови у виплаті винагороди автору за використання винаходу [4].

Література

1. Загальна декларація прав людини. - [Електронний ресурс] – Режим доступу : http://zakon2.rada.gov.ua/laws/show/995_015. - Назва з екрана.

2. Цивільний кодекс України // ВВР. - № 40-44. – 2003. – Ст.356.

3. Закон України «Про охорону прав на винаходи і корисні моделі» // ВВР. - № 7. – 1994. – Ст. 32.

4. Єдиний державний реєстр судових рішень – Справа № 2-179/2011. – [Електронний ресурс] – Режим доступу: http://www.reyestr.court.gov.ua/Review/19931943. --- Назва з екрана.

==========***==========

Г. О. Цирфа,
к.і.н., доцент, заступник директора
Навчально-наукового центру інформаційного
права та правових питань інформаційних технологій
ФСП НТУУ «КПІ»

ЕФЕКТИВНА СИСТЕМА ЗАХИСТУ ПРАВ АВТОРІВ ТА ПРАВОВЛАСНИКІВ НА ОБ'ЄКТИ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ: РЕАЛІЇ ТА МОЖЛИВОСТІ

Ефективне забезпечення захисту в галузі інтелектуальної власності залежить від інтеграції у світовий інформаційний простір та законодавчої системи держави. Україна з часів проголошення незалежності перебуває в стані постійних змін і пошуків на шляху до цивілізованих відносин як на національному, так і міжнародному рівнях. Це дало можливість нашій державі у законотворчій діяльності досягти достатньо ефективних механізмів захисту від незаконного використання об'єктів інтелектуальної власності. Однак, в епоху глобалізації, бурхливого розвитку інформаційних технологій, прискорення процесів інформатизації, стрімкого зростання інформаційно-комунікаційного ринку законодавча система держави повинна забезпечити широкий доступ громадян до надбань інтелектуальної власності, що означає створення балансу між правами та охоронюваними законом інтересами всіх учасників відносин у сфері інтелектуальної власності. Такий баланс може бути досягнутий у результаті невідкладного вирішення цілого комплексу питань і проблем, які, наразі, є надзвичайно актуальними з урахуванням вимог інформаційної доби, і в цьому повинні брати участь усі учасники інформаційного суспільства.

В Окінавській Хартії глобального інформаційного суспільства, прийнятій лідерами "Великої вісімки" 22 липня 2000 р., відмічається: «Усі люди без винятку повинні мати можливість користуватися перевагами глобального інформаційного суспільства. Стійкість глобального інформаційного суспільства ґрунтується на стимулюючих розвиток людини

демократичних цінностях, таких як, вільний обмін інформацією та знаннями, взаємна терпимість і повага до особливостей інших людей».[3]

Сьогодні зміни в суспільстві відбуваються незалежно від того хочемо ми цього чи ні, однак, бажаний результат на рівні держави можна досягти тільки за умови, коли всі зацікавлені в цьому процесі особи поводитимуть себе законно, сумлінно, толерантно. У першу чергу, це стосується відносин в Інтернет-мережі, де відбувається переплетіння інтересів величезної кількості користувачів, а обмін інформацією, її обробка і отримання відбувається доволі швидко, просто та дешево або взагалі безкоштовно. Фактично, весь Інтернет являє собою результат інтелектуальної і творчої діяльності, і слід зазначити, що найбільш чутливою до будь-яких раптових змін є сфера авторського права. В результаті розвитку новітніх інформаційних технологій суттєвого впливу зазнають майнові права авторів. Отже, захист авторів і правовласників з одного боку, і підтримка користувачів в мережі Інтернет з іншого боку, вимагає нових підходів, що передбачає розробки нової стратегії управління глобальною мережею.

Таку стратегію було прийнято Комітетом міністрів Ради Європи. «Стратегія управління інтернетом на 2016-2019 роки» має на меті вирішення проблем у сфері прав людини, демократії і верховенства права, що виникають в онлайн-середовищі та дуже швидко розвиваються. Заходи, що заплановано зробити за цим документом, мають глобальний характер і, без сумніву, сприятимуть правомірній і добросовісній поведінці людини в мережі інтернет, що безумовно стосується і поведінки осіб, які безпосередньо мають відношення до інтелектуального продукту. Зокрема, в цьому документі поряд із багатьма важливими напрямами розроблено і стандарти

[3] Див.: Окінавська Хартія Глобального Інформаційного Суспільства. – Режим доступу: http://library.kr.ua/okinawa.html

поведінки інтернет-провайдерів, які також повинні вчитися добросовісній поведінці при наданні відповідних послуг користувачам Інтернету.[4]

Не секрет, що в Інтернеті велику кількість людей приваблює нелегальний піратський контент – фільми, мелодії, ігри, цікаві видання, статті тощо. Не є секретом і той факт, що піратство підтримується суспільством, а окремі користувачі виступають за вільне розповсюдження контенту в Інтернеті. І тут постає безліч питань, зокрема: як добросовісному користувачу убезпечити себе від неправомірного використання прав чужої інтелектуальної власності? Як виявляють і доказують відповідні порушення? Хто на піратстві заробляє? Хто в такому разі виступає об'єктом відповідальності? І яка роль в усьому цьому провайдерів і власників сайтів?

До цього ж, слід брати до уваги, що Інтернет-мережа являє собою глобальний кіберпростір і має міжнародний характер. Тут зберігаються мільйони інформаційних ресурсів, і доступ до цих ресурсів відкритий у будь-якій точці світу. Слід відмітити і засилля в Інтернеті всіляких «посередницьких послуг», на яких окремі особи просто роблять гроші. На міжнародному рівні такою проблемою є монополізація пошукового ринку. Йдеться про пошуковик корпорації Google у Німеччині. Постає питання про виплату авторської винагороди за цитування анонсів - використання пошуковими системами фрагментів новин та інших матеріалів ЗМІ. І, наразі, Єврокомісією всерйоз обговорюються введення на території ЄС виплат авторської винагороди.

Відомо, що всі права на інтелектуальну власність мають монопольну природу і це причина багатьох сучасних проблем в ефективному законодавчому врегулюванні балансу між правами всіх суб'єктів – зацікавлених сторін у сфері інтелектуальної власності. Натомість слід відмітити, що у різні історичні часи захист об'єктів інтелектуальної власності на світовому рівні відбувався за надійними міжнародними стандартами, які і

[4] Див.: Защита и поддержка граждан в Интернете — новая стратегия управления глобальной сетью. – Режим доступу: http://www.coe.int/ru/web/portal/-/protecting-and-empowering-people-on-the-internet-new-internet-governance

сьогодні здатні врегульовувати деякі важливі проблеми. Особливо слід відмітити таке поняття як «копірайт». Можна сказати, що це те найбільше благо, яке створило інформаційну цивілізацію, в яку ми вступаємо зараз. Проте, норми авторського права безнадійно застаріли і в багатьох випадках неефективні при сучасному розвитку технологій. Тож в інформаційному суспільстві є розуміння, що законодавче регулювання відстає від реалій часу, і виклики бурхливого розвитку сучасних технологій спонукають продовжувати вдосконалення та розробку нових світових стандартів, а також відповідних норм на національному рівні, які повинні відповідати новим вимогам інформаційного суспільства.

Минулого року в Україні затверджено план впровадження реформи системи захисту прав інтелектуальної власності. На зустрічі при обговорені цього плану 18 серпня 2015 року, поряд з представниками центральних органів виконавчої влади, були присутні представники Посольства США, Американської торгівельної палати в Україні (АСС), Європейської Бізнес Асоціації (ЕВА), а також представники компанії «Майкрософт Україна» та експерти в галузі інтелектуальної власності. Таким чином, в обговоренні взяли участь усі сторони процесу реформування системи захисту прав інтелектуальної власності. За результатами цієї зустрічі було розроблено п'ять ключових законопроектів, які стануть основою для реформи державної системи захисту інтелектуальної власності. У підготовці законодавчих змін брали участь представники правовласників, бізнесу і представники провайдерів.

Проте, чи можна сподіватись на консолідований результат цього законотворення? На жаль, аналіз законопроектів показує, що не всі нові норми зможуть захистити як правовласників, так і споживачів в мережі Інтернет. Більшість експертів вважають, що норми законопроектів, зокрема законопроекту № 3353, порушують принципове положення Конституції України щодо верховенства права, а також не відповідають вимогам ст. 13 Конституції. Законопроект також не відповідає і нормі в Угоді про Асоціацію

з ЄС, де регламентовано, що блокування контенту можливо тільки за рішенням суду. Та й взагалі, як показала практика, введення жорстких норм не дає відчутних результатів.

Багато експертів вважають, що в законопроектах не прослідковується побудова для всіх визначених в законопроектах учасників – суб'єктів права інтелектуальної власності, збалансованих взаємовідносин. У цих тезах описана тільки верхівка айсбергу проблем, які криються як у зазначених законопроектах, так і в пошуках змін на шляху до цивілізованих відносин у сфері інтелектуальної власності. Отже, сподіваємося, що українські законотворці врахують всі зауваження фахівців і експертів, а також представників бізнесу, з боку яких вносились пропозиції, і остаточний варіант, поданих до Верховної ради законопроектів, у більшій мірі задовольнить авторів і правовласників, провайдерів і творців сервісів і обов'язково інтернет-користувачів - споживачів продукту інтелектуальної власності.

==========***==========

С. Л. Гнатюк,
к. і. н., головний консультант
Національного інституту
стратегічних досліджень України

ОСОБЛИВОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В СУЧАСНОМУ КІБЕРПРОСТОРІ: НОРМАТИВНО-ПРАВОВИЙ ДОСВІД ЄС

1. На даний момент **в країнах Європейського Співтовариства склалася досить однозначна і стереотипна юридично-правова дефініція самого поняття «персональні дані»** (далі в тексті можливе скорочення – ПД – *С.Г.*)**, а також консенсус щодо основних принципів і процедур їх обробки та захисту**. Крім того, накопичений значний практичний досвід. **Для України** та інших демократичних європейських країн, що

запроваджують або модернізують власну систему захисту ПД саме **ця модель слугує певним стандартом і взірцем**.

2. **Захист персональних даних трактується в європейській правовій традиції як одна з неодмінних підстав забезпечення фундаментального права людини на недоторканість її особистого життя, яке в свою чергу, є основоположним для сучасної демократії** з її приматом поваги до прав та гідності людини. **Нині ця точка зору є загальновизнаною у світі**: недоторканість приватного життя, в тому числі особистої інформації людини, як одне з її основних прав закріплене в найважливіших міжнародних актах сучасності, а також в абсолютній більшості національних законодавств світу.

3. **Основи ідеології захисту ПД** в правовій практиці сучасних демократичних держав можна звести до таких двох положень**:** **1) пріоритетним є право особи розпоряджатися** своїми персональними даними; їх використання без дозволу володільця карається згідно з законодавством; 2) для будь-кого, хто здійснює користування персональними даними фізичних осіб, з їх дозволу, встановлено **відповідальність у разі умисного розголошування цих даних третім особам** (якщо тільки фізична особа не дала дозвіл на таке розголошування).*

4. З цих основ випливають основні **права суб'єкта персональних даних**. Суб'єкт має право знати:

- *хто* і *де обробляє* його ПД;
- *кому передаються* його ПД;
- *де зберігаються* його ПД;
- як реалізувати право на *доступ* до своїх ПД (право на доступ як такий також належить до основних);
- *механізми обробки* його ПД (у разі їх автоматичної обробки).

* У рамках національних законодавств, однак, зазвичай є спеціально прописані випадки винятків з цих двох фундаментальних правил.

Крім того, до основних прав суб'єкта відноситься право *вимагати знищення чи виправлення* ПД, якщо вони обробляються незаконно чи є недостовірними.[5]

З означеними пріоритетами й правами прямо корелюють **вісім основних принципів обробки персональних даних**, сформульованих ще 1981 року у Конвенції Ради Європи про захист осіб стосовно автоматизованої обробки даних особистого характеру (статті 5-8).

5. Європейське право включає майже **два десятки загальноєвропейських конвенцій, директив та рекомендацій** з питань захисту персональних даних, хоча кожна країна ЄС має також свої базові нормативно-законодавчі акти, локальні закони щодо обробки персональних даних у медичній, статистичній, державній, журналістській, поліцейській та інших сферах. **При цьому існує низка міждержавних актів, обов'язкових для всіх країн-членів ЄС** та/чи Ради Європи. Основними з них є:

Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних **1981 р.** (учасницею якої є й Україна).

Додатковий протокол 2001 року до Конвенції Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних (прийнятий Україною).

Директива Європейського Парламенту і Ради №95/46/ЄС про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних **1995 р.** (принципи Директиви підтримані Україною).

6. Разом з цим, нині не лише в ЄС, а й практично в усіх країнах та міждержавних об'єднаннях **найбільш проблемною сферою захисту ПД стали ІТ і кіберпростір** як нове специфічне інформаційно-комунікаційне середовище, яке стрімко розвивається і збільшується. **У цій галузі нормативно-правове регулювання хронічно відстає від якісного**

[5] Див.: Козак В. Захист персональних даних: право, практика, нагляд [Електронний ресурс]. - Режим доступу : http://zpd.gov.ua/dszpd/doccatalog/document?id=51760

(технології) та кількісного (продуктивність і поширеність інфраструктур) розвитку.

7. Традиційно захист персональних даних регулюється узгодженими між собою міжнародними правовими актами і національними законодавствами держав, де знаходяться суб'єкт та оператори ПД. Але в **онлайн-середовищах нормативно-правове регулювання захисту персональних даних стає якісно новою проблемою**, пов'язаною зокрема з архітектурою і технічними особливостями Мережі, а також з її глобальним характером. **Цілком нових підходів потребує у кіберпросторі забезпечення недоторканості ПД, ефективного контролю їх збору, обробки, фізичного місцезнаходження, знищення та виправлення, транскордонної передачі персональних даних** і вирішення пов'язаних конфліктів юрисдикцій. Понад те, існують **широкі технічні можливості й безліч способів анонімного незаконного доступу до ПД**, що знаходяться як «в мережі», так і на локальних дисках персональних пристроїв користувача (ПК, планшет, смартфон тощо), якщо ці пристрої підключені до Інтернету. У хмарових сервісах **сумнівним є навіть доступ користувача до своїх власних ПД**, оскільки за технологією об'єктивно не він контролює цей доступ. Цей перелік можна продовжувати.

8. Поряд з цим, глобальне **Інтернет-середовище швидко перетворюється на дійсно всеосяжну, загальнодоступну й абсолютно необхідну для нормальної життєдіяльності людства структуру**.* Зонами (сегментами) сучасного кіберпростору, де зберігається та обробляється найбільша кількість персональних даних, є:

* За даними Міжнародного союзу електрозв'язку станом на липень 2015 року кількість постійних інтернет-користувачів у світі склала 3,4 млрд. осіб (46% людства) і продовжує швидко збільшуватися. Щонайменше 65% цієї аудиторії користуються інтерактивними сервісами (соціальні мережі, Skype тощо), постійно залишаючи там свої персональні дані. Глобальна стратегія розвитку Всесвітньої павутини, що системно й досить успішно реалізується нині провідними дослідницькими ІТ-компаніями та виробничими корпораціями, передбачає створення всеосяжної й максимально автоматизованої/роботизованої Мережі Мереж, яка забезпечує постійний зв'язок між людьми, даними та іншими об'єктами (речами) в тотальному масштабі. Практика свідчить, що в такому середовищі можливості незаконної обробки та збереження персональних даних користувачів багаторазово зростають, а дієвість нормативно-правових механізмів контролю – пропорційно зменшується.

- будь-які електронні бази даних і дата-центри;
- електронний бізнес, банкінг та шопінг;
- інші дистанційні е-послуги: електронна демократія, навчання, медицина, юридичні послуги тощо;
- комунікативні сервіси: електронна пошта, IP-телефонія, Skype, ICQ;
- середовище Web 2.0: блоги, wiki, соціальні медіа, різноманітні мережні спільноти, інтерактивні служби та інші веб-сервіси другого покоління;
- всі онлайн-сервіси на базі хмарових технологій.

Можна сміливо твердити, що вже на даній фазі розвитку Всесвітньої Павутини **в ній обертається та/чи зберігається практично вся зафіксована людиною інформація, включаючи персональні дані.** Основна проблема тут полягає у відсутності ефективних та апробованих адміністративно-правових інструментів, що могли б забезпечити повноцінний і повсюдний захист персональних даних в умовах віртуального середовища (контроль місцезнаходження, транзиту, доступу до своїх даних, можливість відкликати їх тощо).

9. Керівництво ЄС визнає, що в частині регулювання захисту персональних даних у віртуальному середовищі класичне законодавство Євросоюзу є застарілим і малоефективним. **З 2011 року в Європейської Комісії триває робота над глибокою реформою** нормативно-правового поля Співтовариства в сфері захисту персональних даних.

Основними напрямками реформи є:

- забезпечення прав осіб на захист персональних даних;
- економічний вимір захисту персональних даних;
- захист персональних даних у діяльності правоохоронних органів;
- міжнародний вимір захисту персональних даних.

- Єдиний регулятивний акт для всього ЄС на принципах довіри, повної відкритості і Single Digital Market (Єдиний цифровий ринок)

10. 25 січня 2013 року були опубліковані пропозиції Європейської Комісії по реформуванню законодавства про захист персональних даних в Європі – єдині та обов'язкові для всіх країн ЄС **Стандарти захисту персональних даних Євросоюзу (European Data Protection Regulation)**, які мають замінити Директиву № 95/46/ЕС та визначити основні вимоги законодавства ЄС у сфері захисту персональних даних. Після низки належних погоджень та затверджень 14 квітня цього року Стандарти були остаточно прийняті Європейським Парламентом під назвою **General Data Protection Regulation.** Уведення їх в дію триватиме у країнах-членах ЄС протягом двох років до весни 2018 року.

11. Стандарти є спробою правового врегулювання цих питань з урахуванням нових викликів та загроз у кіберпросторі, але **з позиції безумовного пріоритету невід'ємного права особи на недоторканість і вільне розпорядження власними персональними даними**. Акцент у документі робиться на наданні громадянам більших можливостей контролю використання їхніх персональних даних за рахунок вдосконалення адміністративних процедур, розширення їх прав і збільшення контрольованості та відповідальності компаній-операторів в питаннях захисту і обробки персональних даних.

12. Стандартами передбачено також **розширення прав осіб-володільців персональних даних при одночасному посиленні контрольованості та відповідальності операторів ПД**:

- Гарантування *вільного доступу до власних персональних даних* в будь-яких базах даних.
- ***«Право на вільне перенесення персональних даних»***. За новим законодавством громадяни повинні отримати спрощену процедуру передачі своїх персональних даних від одного постачальника послуг до іншого

(мобільність даних). Передбачається, що це підвищить конкуренцію серед постачальників послуг.

- ***«Право бути забутим»*, тобто** полегшення для громадян процедур знищення своїх персональних даних в базах даних із забороною їх подальшого використання, якщо немає законних підстав для їх збереження.

- ***Право на добровільне і відкрите волевиявлення власника персональних даних* щодо певних типів їх обробки.**

- *Розширення повноважень національних контролюючих органів* із захисту персональних даних. Зокрема, передбачене посилення дисциплінарних заходів щодо компаній, які порушують відповідні правила ЄС. В якості санкцій недобросовісному операторові персональних даних може бути виписане попередження за перше порушення, накладений штраф в розмірі від 250 тис євро або 0,5% від обороту за незначні порушення і штраф в розмірі **до 1 млн євро або до 2% від загальносвітового річного обігу компанії** у разі нанесення збитку суб'єктам персональних даних.

- Вводяться загальні принципи і правила по захисту персональних даних задля опитмізації міждержавної співпраці поліції і правоохоронних органів в т.ч. і у кримінальних справах.

Нові правила ЄС повинні прийматися також і нерезидентами ЄС, якщо вони активно працюють на ринку ЄС і надають свої послуги громадянам ЄС.

13. Попри те, що Стандарти ще не прийняті, вони є чітким індикатором сучасних настроїв в Єврокомісії (а, вірогідно, і загалом у керівництві ЄС). **Акцент у документі робиться на наданні громадянам більших можливостей контролю використання їхніх персональних даних за рахунок вдосконалення адміністративних процедур, розширення їх прав і збільшення контрольованості та відповідальності компаній-операторів** в питаннях захисту і обробки персональних даних.

14. У вересні 2012 року Європейська Комісія виступила зі стратегією **«Вивільнення потенціалу хмарних обчислень в Європі» ("Unleashing the potential of cloud computing in Europe")**, що спрямована на прискорення

імплементації та значне розширення використання «хмар» в економіці ЄС. Передбачається, що реалізація цих завдань принесе 2,5 млн робочих місць і 160 млрд євро чистого прибутку щороку. Основними цілями стратегії є:

- Запровадження вже у 2013 році єдиних технічних та інших стандартів задля забезпечення належної мобільності, функціональної сумісності й оборотності даних;
- Підтримка співробітництва з достойними довіри провайдерами «хмарних» послуг в масштабах всього ЄС;
- Розвиток та підтримка моделі «безпечно і справедливо» (“safe and fair”) при укладенні угод на ринку «хмарних» послуг:
- Запровадження спеціальної інституції – Європейського «хмарного» партнерства (European Cloud Partnership – ECP) – за участю країн-членів та представників індустрії задля залучення потенціалу приватного сектора, оформлення європейського галузевого ринку, стимулювання європейських провайдерів з метою підвищення їхньої конкурентоздатності і запровадження оптимальної системи е-урядування.

15. На даний момент ці законодавчі ініціативи оцінюються як **найбільш складні проекти, які коли-небудь опрацьовувались Європейським Парламентом** – євродепутатами було запропоновано близько **4000 поправок та пропозицій**. Є передчасним оцінювати ефективність цих актів, оскільки їх випробування практикою ще, власне, не відбулося. З іншого боку, вони являють собою послідовну спробу **відповіді на нові виклики з традиційних європейських позицій примату демократії та прав людини**, у чому полягає їх безсумнівна цінність.

16. Якщо найближчим часом не буде знайдено ефективного і при цьому демократичного рішення проблеми захисту персональних даних у веб-середовищі – у недалекій перспективі це може призвести до **непередбачуваних і небезпечних переосмислень загальноприйнятих уявлень про приватність, її сенс та межі, а відтак – до перегляду правового змісту самого поняття «персональні дані»**.

17. На думку автора, крім адекватного правового забезпечення та ефективної системи регулювання та нагляду для успішного протистояння викликам, пов'язаним із захистом ПД у кіберпросторі необхідним є: а) розвинений й диверсифікований ринок юридичних послуг; в) грамотні та відповідальні контрагенти – провайдери онлайн-послуг та їх споживачі, суб'єкти та оператори персональних даних. Особливого значення у цьому контексті набуває **системне поширення серед інтернет-користувачів цифрової грамотності і культивування відповідальної поведінки у Мережі**.

==========***==========

С. В. Дубова,
к.і.н.

ДО ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОСОБИ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ (МЕТОДОЛОГІЧНІ АСПЕКТИ)

Сьогодні питання інформаційної безпеки виходять на перший план в багатьох сферах наукових досліджень. В українських реаліях це обумовлено, по-перше, активною інформаційною агресією проти нашої держави, а по-друге, динамічним розвитком сучасних інформаційних технологій, що формують модернове інформаційне суспільство. Водночас, маємо констатувати, що незважаючи на те, що інформаційна безпека традиційно складається з трьох компонентів (безпека людини, суспільства, держави), основна увага дослідників зосереджена лише на двох останніх елементах, в той час як саме людина зазнає чи не найбільше негативних впливів в інформаційному суспільстві (як технологічних так і психологічних). Важливою складовою цієї проблеми є те, що, а ні на науковому, а ні на державному рівні немає чіткого та однозначного розуміння, що власне має захищатись в контексті інформаційної безпеки особи.

Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки», визначає інформаційну безпеку, як «стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації» [1]. Якщо для держави (а до певної міри і для суспільства) такими життєво важливими інтересами, вочевидь, є національні інтереси (які визначені в Законі України «Про основи національної безпеки України» [2]), то що має розумітись як «життєво важливі інтереси особи» не зовсім зрозуміло. У Доктрині інформаційної безпеки України [3], що втратила чинність у 2014 році, такими інтересами визначались:

- забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації;
- недопущення несанкціонованого втручання у зміст, процеси обробки, передачі та використання персональних даних;
- захищеність від негативного інформаційно-психологічного впливу.

Однак, незважаючи на рішення Ради національної безпеки і оборони України [4] розробити нову редакцію такої Доктрини до останнього часу цього так і не було зроблено. А отже, в нормативно-правовому сенсі, життєво важливі інтереси особи досі не визначені. Щоправда, не має однозначності в розумінні їх і серед науковців. Слід зазначити, що в більшості досліджень, які так чи інакше присвячені питанню «життєво важливих інтересів», життєво важливі інтереси особи майже ніколи не виділяються в якості окремої категорії, а розглядаються у сукупності із інтересами суспільства і держави. Більшою мірою науковці доходять висновку, що життєво важливі інтереси особи це передусім захист її конституційних прав та свобод.

Однак, навіть і в такому випадку майже ніде такі «життєво важливі інтереси особи» не розглядаються саме в контексті інформаційної безпеки та інформаційних прав людини. При цьому саме інформаційні права (а в більш широкому сенсі – права людини) піддаються чи не найбільшій деформації в умовах становлення інформаційного суспільства.

Відтак, питання забезпечення інформаційної безпеки особи в інформаційному суспільстві залишається без необхідного науково-методологічного апарату, без чого не можливо сформувати адекватне викликам та загрозам національне (а заразом і міжнародне) законодавство, за якого такі інтереси будуть достатнім чином захищені, а сама особа зможе реалізувати своє право на ефективний особистий (духовний, культурний, інтелектуальний) розвиток.

Література

1. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 9 січня 2007 року №537-V.- [Електронний ресурс].- режим доступу. - http://zakon5.rada.gov.ua/laws/show/537-16

2. Закон України «Про основи національної безпеки України» від 19 червня 2003 року № 964-IV. - [Електронний ресурс].- режим доступу. - http://zakon3.rada.gov.ua/laws/show/964-15

3. Указ Президента України «Про Доктрину інформаційної безпеки України» від 8 липня 2009 року №514/2009.- [Електронний ресурс].- режим доступу. - http://zakon5.rada.gov.ua/laws/show/514/2009

4. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України», від 01 травня 2014 р. №449/2014 – [Електронний ресурс].- режим доступу: http://www.rnbo.gov.ua/documents/347.html

==========***==========

І. В. Солончук,
ст. викладач кафедри
інформаційного права та права
інтелектуальної власності ФСП НТУУ «КПІ»

ІНФОРМАЦІЯ В ЦИВІЛЬНОМУ СУДОЧИНСТВІ

Конституція України гарантує кожному захист прав та свобод у спосіб, визначений законом. Рішення, дії чи бездіяльність органів державної влади, органів місцевого самоврядування, посадових і службових осіб можуть бути оскаржені в суді [1; ч.1 ст. 55]. У порядку цивільного судочинства реалізується судовий захист порушених, невизнаних або оспорюваних прав та інтересів [2; ч.1 ст.55].

Сучасне цивільне судочинство, виконуючи правозастосовну та правозахисну функції, зобов'язане відповідати викликам часу та забезпечувати справедливе вирішення справи згідно Конвенції про захист прав людини і основоположних свобод [7; с.22].

Проблематика цивільного процесу у глобальному контексті вже розглядалась в науковій літературі, зокрема в працях Комарова В. [7], Лукашука І. [8] та в роботах інших авторів. Але динаміка визначеної сфери правовідносин вимагає додаткового дослідження та аналізу.

Стрімкі процеси інформатизації суспільних відносин об'єктивно здійснюють впив на функціонування судової системи та визначають еволюцію процесуальних приписів щодо розгляду та вирішення цивільних справ. Інформація в цивільному процесі посідає важливе та особливе значення: 1) позовна заява містить відомості особистого характеру, які стосуються як позивача, так і відповідача, а інколи і кількох відповідачів; 2) функціонування автоматизованої системи документообігу суду, яка забезпечує централізоване зберігання текстів рішень, ухвал суду, інших процесуальних документів та є джерелом інформації про стан розгляду справи, про вхідну та вихідну кореспонденцію, про статистичні дані роботи суду; 3) про виклик до суду особи, які беруть участь у справі, можуть бути

поінформовані у досить різноманітний спосіб; 4) така процесуальна діяльність як доказування передбачає дослідження, аналіз і оцінку інформації по справі, одержаної з різних інформаційних джерел тощо.

Цивільний процесуальний кодекс України (далі – ЦПК) встановлює ряд вимог щодо форми та змісту позовної заяви до суду [2; ст.119]. У випадку недодержання цих обов'язкових вимог суддя постановляє ухвалу про залишення такої позовної заяви без руху [2; ч.1 ст.121] та надає позивачу можливість усунути вказані недоліки у встановлений строк (не більше п'яти днів з дня одержання позивачем такої ухвали). В позовній заяві обов'язково зазначається особиста інформація про позивача та відповідача: ім'я, місце проживання (перебування) чи місцезнаходження, поштовий індекс, номери засобів зв'язку (якщо такі відомі) [2; п.2 ч.1 ст.119]. Суд в свою чергу після прийняття позовної заяви не пізніше двох днів з дня її надходження звертається до відповідного органу реєстрації місця проживання та місця перебування відповідача щодо надання інформації про зареєстроване таке місце проживання або місце перебування [2; ч.3 ст.122]. Така диспозитивність щодо місця проживання (перебування) чи місцезнаходження особи визначається конституційним правом людини і громадянина на свободу пересування, вільний вибір місця проживання, право вільно залишати територію України, за винятком обмежень, які встановлюються законом [1; ст.33].

Безумовним наслідком розвитку інформаційного суспільства є запровадження з 1 січня 2011 року в судах України автоматизованої системи документообігу суду (далі – АСДС), яка унеможливлює «ручний» розподіл справ головою суду. АСДС є джерелом інформації про стан розгляду справи для осіб, які є її учасниками. Позовна заява реєструється в АСДС в день її подання [2; ч.2 ст.11-1]. Централізоване зберігання процесуальних документів, зокрема текстів рішень і ухвал суду, також забезпечує АСДС.

Інформування осіб, які беруть участь у справі, про необхідність чи необов'язковість їх явки до суду, забезпечується процесуальним інститутом

судових повісток. ЦПК встановлює загальний порядок вручення судової повістки про виклик до суду: така судова повістка вручається під розписку фізичній особі, якій вона адресована [2; ч.1 ст.76]. Але на практиці нерідко відбуваються випадки, коли вручити судову повістку особі не видається можливим, оскільки не відоме її місце фактичного проживання (перебування). В цій ситуації суд здійснює інформування таких осіб про виклик до суду через друковані засоби масової інформації: оголошення про виклик до суду публікується у друкованому засобі масової інформації загальнодержавної сфери розповсюдження та в друкованому засобі масової інформації місцевої сфери розповсюдження за останнім відомим місцем проживання (перебування) на території України відповідача, третіх осіб, свідків [2; ч. 9, 10 ст. 74]. Новелою у сфері застосування інформаційних технологій в організації роботи суду є запроваджений з 1 жовтня 2013 року у місцевих та апеляційних загальних судах порядок щодо надсилання судами учасникам судового процесу текстів судових повісток у вигляді SMS-повідомлень [5]. Для цього учаснику судового процесу потрібно подати до суду, в якому розглядатиметься його справа, заявку про отримання судової повістки у вигляді SMS-повідомлення. На підставі цієї заявки судова повістка у вигляді SMS-повідомлення надсилається учаснику судового процесу на той номер мобільного телефону, який вказаний в заявці.

Особливим чином процес інформатизації цивільного процесу спостерігається в судовому доказуванні. Для встановлення фактичних обставин справи суд досліджує виключно допустимі докази, тобто одержані у встановленому законом порядку. Всі інші докази судом до уваги не беруться. Наприклад, суд не розглядає як доказ у цивільній справі показання свідка, який не може назвати джерела своєї обізнаності щодо певної обставини [2; ст.63].

Якщо аналізувати в широкому історичному контексті розвиток правосуддя в цивільних справах, можемо спостерігати його певну консервативність та адаптованість до конкретних соціально-політичних

чинників. Комаров В. підсумовує, що правосуддя в цивільних справах має деяку міру самостійності та тяжіє саме до еволюційних змін певних процесуальних інститутів [7; с.22-23]. В той же час еволюція інформаційного суспільства накладає свій відбиток, і можемо констатувати – в позитивному напрямку забезпечення захисту прав та свобод людини в цивільному судочинстві. Безумовно прогресивним кроком у даному напрямі є підготовлена Радою суддів України Інформаційно-комунікаційна стратегія як комплекс заходів інформаційного, організаційного, нормативно-правового та іншого характеру, що направлені в тому числі і на об'єктивне висвітлення діяльності судової системи в засобах масової інформації та через веб-ресурси [6].

Враховуючи актуальність наукових досліджень у сфері впливу інформаційних потоків на організацію роботи судової системи та на цивільне судочинство зокрема, слід пам’ятати, що захист прав, свобод та інтересів людини є пріоритетним напрямом діяльності всіх владних органів правової держави. Оперування судом таким широким спектром різноманітної інформації у цивільному процесі має слугувати саме для захисту порушеного, невизнаного чи оспорюваного права і не повинно використовуватись всупереч інтересам особи. Саме в цьому аспекті взаємозв’язок інформаційного суспільства та цивільного судочинства потребує подальшого вивчення та наукового аналізу.

Література

1. Конституція України: Закон України, 28 червня 1996 р. № 254к/96-ВР // Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141.

2. Цивільний процесуальний кодекс України: Закон України, 18 березня 2004 № 1618-IV // Відомості Верховної Ради України, 2004, № 40 - 41, с. 135.

3. Постанова КМУ від 25 січня 2006 р. № 52 «Про порядок визначення друкованого засобу масової інформації, у якому розміщуються

оголошення про виклик до суду відповідача, третіх осіб, свідків, місце фактичного проживання (перебування) яких невідоме, повістки про виклик підозрюваного, обвинуваченого та інформація про процесуальні документи».

4. Висновок № 14 (2011) Консультативної ради європейських суддів «Судочинство та інформаційні технології» // Страсбург, 9 листопада 2011 року. - КРЄС (2011) 2. [Електронний ресурс] – Режим доступу: http://court.gov.ua/mss/.

5. Наказ Державної судової адміністрації України № 119 від 20 вересня 2013 року «Про реалізацію проекту щодо надсилання судами SMS-повідомлень учасникам судового процесу (кримінального провадження). [Електронний ресурс] - Режим доступу: http://dsa.court.gov.ua/dsa/14/asjhdgajhdsgajhsdgutuut/ .

6. Концепція інформаційно-комунікаційної стратегії Ради суддів України. [Електронний ресурс] - Режим доступу: http://court.gov.ua/userfiles/rsu.pdf.

7. *Комаров В. В.* Цивільний процес у глобальному контексті // Право України – 2011. - № 10. – С. 22 – 44.

8. *Лукашук И. И.* Глобализация, государство, право, XXI век. – М., 2000.

9. *Сакара Н. Ю.* Право на справедливий судовий розгляд та національна практика цивільного судочинства // Право України – 2011. - № 10. – С. 63 – 76.

==========***==========

УДК:342.9
Л. В. Секелик,
аспірант НДІІП НАПрН України

ПРОБЛЕМА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПРИ РОЗМІЩЕННІ СУДОВИХ РІШЕНЬ В ЄДИНОМУ ДЕРЖАВНОМУ РЕЄСТРУ СУДОВИХ РІШЕНЬ

Європейська спільнота до якої прагне також увійти й Україна, вимагає не тільки захисту персональних даних, а й здійснення відкритого доступу до всіх судових рішень.

Саме у зв'язку з цим був прийнятий Закон України «Про доступ до судових рішень» від 22 грудня 2005 року N 3262-IV (надалі – Закон № 3262-IV).

Статтею 3 Закону № 3262-IV суд загальної юрисдикції вносить до Єдиного державного реєстру судових рішень: www.reyestr.court.gov.ua (надалі – Реєстр) всі судові рішення і окремі думки суддів, викладені у письмовій формі, не пізніше наступного дня після їх ухвалення або виготовлення повного тексту.

Закон України «Про інформацію» у ст.11 закріплює, що інформація про фізичну особу (персональні дані) – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Фактично поняття інформації про особу ототожнюється у ст.5 Закону України «Про захист персональних даних».

Передумовою нормативної регламентації поняття «інформації по фізичну особу (персональні дані)» в національному законодавстві України стала Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981р., у ст.2 якої також міститься визначення терміна «персональні дані». Під ними розуміють будь-яку інформацію, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною.

Тої ж думки до дотримується й Конституційний Суд України, даючи офіційне тлумачення частин першої, другої статті 32 Конституції України (Рішення Конституційного Суду України від 20.01.2012 р. N 2-рп/2012 у справі за конституційним поданням Жашковского районної ради Черкаської області відносно офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України), вказав, що персональні дані про особу - це будь-які відомості або сукупність відомостей про фізичну особу, яку ідентифіковано або може бути конкретно ідентифіковано, а саме: національність, освіта, сімейний стан, релігійні переконання, стан здоров'я, матеріальне становище, адреса, дата і місце народження, місце проживання і знаходження і т.д., дані про особисті майнові і немайнові стосунки цієї особи з іншими особами, зокрема з членами сім'ї, а також відомості про події і явища, які відбувалися або відбуваються в побутовій, інтимній, товариській, професійній, діловій та в інших сферах життя особа, за винятком даних відносно виконання повноважень особи, що обіймає посаду, пов'язану із здійсненням функцій держави або органу місцевого самоврядування.

Закон № 3262-IV визначає, що не можуть бути розголошені відомості, що дають можливість ідентифікувати фізичну особу. До таких відомостей законодавець відносить:

- імена (ім'я, по батькові, прізвище) фізичних осіб;
- місце проживання або перебування фізичних осіб із зазначенням адреси, номери телефонів чи інших засобів зв'язку, адреси електронної пошти, ідентифікаційні номери (коди);
- реєстраційні номери транспортних засобів, реєстраційні відомості реєстрів нерухомого майна;
- номери банківських рахунків, номери платіжних карток;
- інша інформація, що дає можливість ідентифікувати фізичну особу.

Окрему увагу треба приділити пп.4 п. 2 ст. 7 Закону № 3262-IV: «4) інша інформація, що дає можливість ідентифікувати фізичну особу.».

Таке нечітке формулювання «персональної інформації» призводить до поширення різноманітного тлумачення, які відомості дозволяють ідентифікувати фізичну особу, а які – ні.

Норми п. 1, 2 ст. 7 Закону № 3262-IV фактично суперечать Закону України «Про судоустрій та статус суддів» від 7 липня 2010 року N2453-VI (надалі – Закон №2453-VI) та нормам процесуального законодавства. Відповідно до ст. 11 Закону №2453-VI розгляд справ у судах відбувається відкрито, крім випадків, установленим законом. Ця норма отримує подальший розвиток у процесуальних кодексах. А саме ст. 4-4 Господарського процесуального кодексу України, ст. 6 Цивільного процесуального кодексу України, ст. 12 Кодексу адміністративного судочинства України, ст. 249 Кодексу України про адміністративні правопорушення, ст. 20 Кримінально-процесуального кодексу України та в інших нормах цих кодексів.

Таким чином постає проблема щодо захисту персональних даних та відкритості доступу до судового засідання.

Проте, як показує аналіз судових рішень наявних в Реєстрі, при викладенні судових рішень не здійснюється належний захист персональних даних.

Так, при винесенні рішення від 19.11.2013 року у справі № 385/1287/13-ц щодо поновлення особи на роботі, дійсно були замінені деякі данні, що ідентифікують позивача, а саме: прізвище, ім’я, по-батькові, проте залишені інші ідентифікуючи данні, а саме – посада та найменування роботодавця. Таким чином, за посадою та місцем роботи позивача можна легко ідентифікувати особу.

Чинне законодавство щодо доступу до судових рішень потребує суттєвих змін, оскільки:

- не містить механізмів притягнення до відповідальності уповноважених осіб держави за порушення Закону №3262-IV;
- не регламентує важливі процедури здійснення Закону №3262-IV;

- не вирішує питання протиріччя принципу гласності судового розгляду і видалення персональної інформації з судових рішень.

==========***==========

Т. Ю. Ткачук,
к.ю.н., доцент,
заступник завідувача кафедри
Організації захисту інформації з обмеженим доступом
Навчально-наукового інституту інформаційної безпеки
Національної академії СБ України

ОБМЕЖЕННЯ ДОСТУПУ ДО СЛУЖБОВОЇ ІНФОРМАЦІЇ ОРГАНІВ ПУБЛІЧНОЇ ВЛАДИ УКРАЇНИ: АКТУАЛЬНІ ПРОБЛЕМИ ТА ЙМОВІРНІ ШЛЯХИ ЇХ ВИРІШЕННЯ

Таємниця є інформацією, яка є відомою лише для тих, хто має до неї доступ. Діалектика феномену таємниці проявляється в її подвійному, полярному характері – для володільців цієї інформації вона не таємниця, для осіб, що не мають доступу до неї являється таємницею. Суть механізму таємниці і реалізується через систему доступу до відповідної інформації, який поєднує в собі певні заборони і зобов'язання.

Обмеження доступу до службової інформації, що міститься в державних інформаційних ресурсах, являється основою режиму таємниці.

Ступінь визначеності може бути різним: це може бути абсолютно повний перелік конкретних видів інформації (наприклад, персональних даних про дітей, що залишилися без піклування батьків); відносно повний перелік (наприклад, відомості, що стали відомими працівникові органів РАГСу у зв'язку з реєстрацією акту цивільного стану), дискретно повний перелік (наприклад, правовий режим податкової таємниці відповідно до п. 17.1.3 Податкового кодексу України (маємо на увазі захист комерційної таємниці платником податку) поширюється на будь-які відомості про платника податків, отримані податковими органами).

Порядок доступу до службової інформації, що є послідовним здійсненням певних дій, реалізовуються у технологіях надання доступу. Слід зазначити, що відповідні технології ще тільки розробляються в органах публічної влади і є далеко не в кожному із них. Ця технологія може включати регламентацію об'єму інформації, що надається; регламентацію форми надання інформації; вимоги про звернення за інформацією в певній формі; вимоги про супровід заяви переліком певних документів; регламентацію порядку реєстрації заяви; регламентацію здійснення підтверджувального запиту у структурі інформаційного забезпечення; регламентацію порядку передачі інформації; встановлення термінів передачі інформації; перевірку об'єктивності відомостей, наданих про себе певною особою.

Прикладом технології доступу до службової інформації може служити порядок надання відомостей з інформаційного масиву дактилоскопічної реєстрації. Він включає перелік реквізитів ініціаторів запиту - органів державної влади, мотивування підстав, припущень про те, що дактилоскопічна інформація про особу може знаходитися в інформаційному масиві, реквізити мотивувального листа, додаток дактилоскопічних карт, які підлягатимуть ідентифікації, з наявними даними в інформаційному масиві про дактилоскопічну реєстрацію, наявність належно оформленого запиту і його офіційний напрям. Таким чином, різні елементи порядку обмеження доступу до службової інформації у сфері діяльності державної влади є присутніми в окремих нормативних актах, але не систематизовані і не уніфіковані.

Виходячи із даного зауваження доцільно встановити уніфікований порядок організаційного захисту службової інформації у сфері діяльності державної влади, що включає визначення переліку службової інформації, визначення кола уповноважених осіб на доступ до даної категорії інформації, визначення виду доступу (разовий, періодичний, систематичний), визначення рівня доступу (до усієї службової інформації в органах державної влади, до

окремих її видів), встановлення порядку щодо надання службової інформації особам, які не є суб'єктами державної влади (отримання запиту встановленої форми, його реєстрація, ідентифікація певної особи, верифікація відомостей про нього, реєстрація факту передачі та отримання інформації). Цей порядок може бути закріплений в нормативних актах органів державної влади, що істотно скоротить загрози несанкціонованого доступу, розголошування, просочування службової інформації і сприятиме встановленню кола осіб, винних у порушенні адміністративно-правових режимів службової інформації.

Органи публічної влади і місцевого самоврядування нині реалізують свою регулятивну діяльність багато в чому за рахунок того, що акумулюють і використовують інформацію, отриману з різних джерел, особливо від суб'єктів підприємницької діяльності. Звідси виникає резонне питання: *які правові підстави і механізми захисту в органах публічної влади для відомостей, переданих їм організаціями, де вони захищалися в режимі комерційної або банківської таємниці*? На сьогодні правове регулювання даних відносин відсутнє, оскільки захист вказаної інформації в режимі державної таємниці неможливий за визначенням, оскільки її сфера законодавчо обмежена певним переліком категорій. Інших систем захисту в тому сенсі, в якому ми розуміємо правовий інститут таємниці, в органах публічної влади практично не існує. В той же час безконтрольне поводження з інформацією, що має високу комерційну цінність і внаслідок цього високу «ліквідність» (простіше кажучи, можливість її продажу зацікавленим особам), апріорі породжує зловживання. Тому потрібний механізм контролю і захисту, причому, бажано, єдиний для усієї системи державного управління, щоб держава могла не на словах, а на ділі гарантувати збереження таких відомостей.

Саме ці міркування і примушують запропонувати в якості універсальної моделі системи обмеження в доступі до службової інформації, що отримується органами публічної влади від інших суб'єктів, інститут

службової таємниці, сформувавши його повністю як сукупність підсистем (субінститутів) службової інформації, захисту і санкцій за неправомірне поширення таких відомостей. Втілення запропонованого напряму в правовому регулюванні може мати багато позитивних наслідків, зокрема:

- зміцнення відповідальності держави перед суспільством і окремими його представниками;

- практична реалізація одного з аспектів забезпечення прав і свобод людини і громадянина в інформаційній сфері;

- позитивна дія на зміцнення економічного суверенітету країни і її інформаційної безпеки;

- встановлення дієвого захисту від зловживань окремих посадовців.

Разом з цим ймовірним є те, що легітимація інституту службової інформації сфері діяльності органів публічної влади є складним процесом, оскільки вимагає коректування значного числа законодавчих та інших нормативних правових актів. Тому для формування цього інституту знадобиться прийняття окремого закону, що регулює комплекс цих відносин, а також ряду актів, що вносять зміни в законодавство. Однією з найбільш складних проблем при вирішенні цього питання є встановлення правового балансу між інститутом державної таємниці та інститутом службової інформації. Тому необхідно, щоб вони, за наявності відповідного законодавчого оформлення, могли деякий час діяти паралельно, внаслідок чого правозастосувальна практика сама визначить, які відомості із числа суміжних і похідних захищатимуться в режимі державної або службової таємниці.

==========***==========

І. В. Павленко,
к.ю.н., доцент кафедри публічного права
ФСП НТУУ «КПІ»

ІНФОРМАЦІЙНЕ СУСПІЛЬСТВО І ПРОБЛЕМИ ГАРМОНІЗАЦІЇ КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА ДІЯННЯ В СФЕРІ СУСПІЛЬНОЇ МОРАЛІ

Взагалі визначення поняття «інформаційне суспільство» наразі залишається дискусійним в наукових колах. Так, наприклад, В.А. Ліпкан інформаційне суспільство розглядає як таке, у якому «будь-хто, будь-де й у будь-який час можуть одержати за відповідну плату чи безкоштовно на основі автоматизованого доступу і систем зв'язку будь-яку інформацію і знання, необхідні для їхньої життєдіяльності і рішення особистих і соціально значущих задач» [1, 146]. Різні автори, виводячи власне визначення цього терміну, тим не менше єдині в тому, що роблять акцентуації на базових основних ресурсах інформаційного суспільства – це знання та інформація. Синонімічними щодо інформаційного суспільства є терміни «посткапіталістичне суспільство» (Д. Дарендорф, П. Дрюкер), «постекономічне суспільство» (В. Іноземцев, І Канн), «технотронне суспільство» (З. Бжезінський), «постіндустріальне суспільство» (Д. Белл, Т. Стоунєр) тощо. В усякому випадку слід констатувати, що інформаційне суспільство – це новий еволюційний етап цивілізаційного розвитку суспільства.

У зв'язку з встановленням та впорядкованою побудовою інформаційного суспільства, що сьогодні слід розглядати вже незворотнім шляхом розвитку, одночасно виникають питання охорони прав людини в такому суспільстві, в тому числі й кримінально-правовими засобами.

Предметом нашої доповіді є дотримання прав людини в сфері суспільної моралі, зокрема, що стосується порнографії. Наперед означимо, що ми не ставимо за мету в рамках доповіді розгляд соціальної обумовленості кримінальної відповідальності за різні діяння щодо

порнографічних предметів. Ми відштовхуємось лише від протиправності таких діянь, відповідальність за які встановлена в чинному КК України.

Отже, йдеться про те, що судово-слідча практика зіткнулася з таким діянням як демонстрування оголеного тіла, його частин, імітація статевого акту через веб-камеру в режимі он-лайн з метою заробітку без запису на матеріальні носії.

Вироків, які б набрали законної сили стосовно осіб, які самостійно займаються такою діяльністю, в Україні наразі немає. Проте, є вироки щодо осіб, які організовують такий «бізнес». Судова практика кваліфікує такі діяння за ст. 301 КК України [2, електронний ресурс].

Така кваліфікація є правильною за умови, що інформація, яка йде в режимі он-лайн через веб-камеру – це предмет злочину, відповідальність за який передбачена ст. 301 КК України. Проте, диспозиції ст. 301 КК України чітко вказують на *матеріальність* предмета злочину: 1) твори, зображення або інші предмети порнографічного характеру; 2) кіно- та відеопродукція, комп'ютерні програми порнографічного характеру.

Саме тут і виникає питання: чи має таке діяння ознаки злочину, чи це нова легальна (хоч і аморальна) форма заробітку за допомогою мережі Інтернет. В науковій юридичній літературі це питання піднімалося і його вирішення пропонується розглядати саме з позицій існуючої судової практики [3, с. 119].

Йдеться про *інформацію* як складову інформаційного суспільства і її місце в кримінальному праві. За останні 10-15 років у вітчизняній кримінально-правовій науковій літературі з'явилося чимало обґрунтувань того, що у вченні про склад злочину інформацію слід розглядати як предмет злочину. Так, вже усталеною позицією є те, що в диспозиціях окремих складів злочину їх предметами прямо вказана інформація. Так, в ст. 114 КК України та ст. 328 КК України предметами злочинів є відомості, що становлять державну таємницю, в ст. 231, 232 КК України – відомості, що

становлять комерційну або банківську таємницю, в ст. 232-1 – інсайдерська інформація.

У випадках, коли інформація прямо вказана в диспозиціях конкретних статей питань щодо кваліфікації діянь, як правило, не виникає. Однак, за сучасного стрімкого розвитку комп'ютерних та інформаційних технологій, кримінальний закон не завжди «йде в ногу з часом». Це стосується саме інформації порнографічного характеру, що йде в режимі он-лайн через веб-камеру.

На нашу думку, однозначне віднесення «живого» потоку інформації порнографічного характеру без запису на носії до предмету злочину (ст. 301 КК України), повинно визначатись в площині вирішення наступного принципового нюансу. Демонстрування оголеного тіла, його частин, імітація статевого акту через веб-камеру в режимі он-лайн з метою заробітку – це своєрідна нова форма проституції, назвемо її віртуальною. Чинний кримінальний закон не встановлює кримінальної відповідальності за зайняття проституцією. Відповідно, виникає певний дисонанс в нормах кримінального закону: якщо особа займається проституцією в реальному житті – кримінальне реагування держави виключене, якщо ж через мережу Інтернет – заходи кримінального впливу мають застосовуватись. Виникає логічне запитання – чи не подвійні це стандарти?

Вирішення державою в особі законодавця цього питання має дуже важливе значення. Якщо розглядуване діяння розглядати як проституцію, то відповідно кримінальне реагування є недопустимим.

У зв'язку з наведеним, можна зробити такі висновки. По-перше, оцінка державою в особі законодавця та суду діянь в сфері суспільної моралі, зокрема, проституції і порнографії, має бути однаковою. По-друге, інформаційне суспільство є швидко розвиваючим, а отже, законодавець має «тримати руку на пульсі» і миттєво реагувати відповідно до виробленої послідовної позиції щодо діянь в сфері суспільної моралі.

Література

1. В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. - К.: КНТ, 2006. - 280 с. (Серія: Національна і міжнародна безпека)

2. Вирок Червонозаводського районного суду м. Харкова від 13.05.2011 р. // [Електронний ресурс]. – Режим доступу: http://www.reyestr.court.gov.ua/Review/24687087

3. Радутний О.Е. Інформація, яка надходить в режимі реального часу через веб-камеру, як предмет злочину, що передбачений ст. 301 КК України / О.Е. Радутний // Інформація і право. - №1(10)/2014. – С. 115-119

==========***==========

В. В. Жилін,
доцент кафедри Національної академії
Служби безпеки України
А. І. Дербеденев,
старший викладач кафедри Національної
академії Служби безпеки України

РЕГУЛЮВАННЯ ПРАВОВІДНОСИН У СФЕРІ ОПЕРАТИВНО-ТЕХНІЧНОЇ ДІЯЛЬНОСТІ ЗА ЗАКОНОДАВСТВОМ ФРАНЦІЇ ТА УКРАЇНИ: ПОРІВНЯЛЬНИЙ АНАЛІЗ

З прийняттям Кримінального процесуального кодексу (КПК) України 2012 року настав новий етап правовідносин у сфері оперативно-технічної діяльності. В Україні така діяльність регулюється багатьма законодавчими актами, базовими серед яких можна вважати Закон «Про оперативно-розшукову діяльність», «Про контррозвідувальну діяльність», «Про організаційно-правові основи боротьби з організованою злочинністю», Кримінальний процесуальний кодекс України тощо. Цими законами регулюється і сфера оперативно-технічної діяльності як складової оперативно-розшукової, контррозвідувальної, кримінальної процесуальної діяльності. Слід відмітити, що в дев‘яностих роках двадцятого сторіччя робилися спроби внести окремі різновиди оперативно-технічних заходів до

кримінального процесу («зняття інформації з каналів зв‘язку» - ст. 187 КПК України). Однак на практиці «зняття інформації з каналів зв‘язку» залишався оперативно-технічним заходом. Зрозуміло, що трансформація сфери оперативно-технічної діяльності в процесуальну повинна, з одного боку, розширити можливості слідства у використанні результатів застосування оперативно-технічних засобів як доказів та, з другого, спростити процедуру вказаного використання в кримінальному процесі. Якщо для української правоохоронної системи НСРД є новелою, то в європейських, зокрема у французькій системі подібний підхід існує вже кілька десятиліть. Відомо, що законодавство західних країн не містить норм щодо застосування оперативно-технічних засобів в оперативно-розшуковій діяльності, як складових закону, що регулював би, наприклад, ОРД. Відсутні і закони про ОРД, КРД тощо. Застосування оперативно-технічних засобів регулюється окремими актами, або законами про відповідні правоохоронні органи (Франція, Німеччина). Франція є родоначальницею класичного континентального кримінального процесу, який за її прикладом був введений майже всіма європейськими державами. Французи активно і результативно застосовують технічні засоби для отримання оперативно значущої і доказової інформації в інтересах безпеки, кримінального процесу і розвідки. Тому пропонується розглянути особливості правового регулювання сфери оперативно-технічної діяльності за законодавством Франції на предмет вивчення позитивного досвіду законотворчості французьких колег у вказаній сфері та можливості його запозичення. Аналіз французьких нормативних актів проводився на основі наукових положень, прийнятих в українській правовій науці.

Після того, як Європейський Суд з прав людини дійшов висновку про те, що французькі норми порушують Конвенцію щодо вказаних прав, французький парламент прийняв Закон № 91-646 від 10 липня 1991 р. «Про недоторканість кореспонденції, що передається засобами телекомунікацій», консолідована версія якого датована 10 липня 2004 року за

номером 2004-669. Закон вказує: «… недоторканість кореспонденції, що передається телекомунікаційними каналами, повинна гарантуватися законом, за винятком випадків, згаданих у ст.1 зазначеного Закону». В Законі наводиться опис двосторонньої системи встановлення прослуховування телефонних розмов (в рамках КПК та в інтересах безпеки).

Закон складається з трьох частин. В частині першій викладаються умови, яким повинне відповідати перехоплення телекомунікацій, яке проводиться за дозволом судової влади. Ці положення подібні до вітчизняних, закріплених в законодавчих актах, які регламентують оперативно-розшукову діяльність та кримінальний процес та ґрунтуються на тому, що зняття інформації з телекомунікаційних мереж проводиться тільки при розслідуванні злочинних діянь.

Положення вказаної частини закону увійшло до кримінального процесуального кодексу Франції у вигляді статей 100-100-7.

В частині другій Закону регламентується право урядового органа віддавати розпорядження про проведення у виключних випадках так званого «перехоплення в інтересах безпеки». Дозвіл на таке «перехоплення» дає прем‘єр-міністр на підставі письмового мотивованого подання міністра внутрішніх справ, міністра оборони та міністра, у компетенції якого знаходиться митниця.

Третя частина регламентує проведення перехоплень по відкритих каналах, та відповідальність за незаконні перехоплення.

Застосування оперативно-технічних засобів за французьким законодавством, на відміну від українського, проводиться з дозволу судді тільки в порядку кримінального судочинства.

Перехоплення кореспонденції здійснюється у справах про злочини, а також у справах про правопорушення, якщо передбачене покарання у вигляді ув‘язнення два і більше років. За українським законодавством подібне перехоплення застосовується щодо осіб, які підозрюються у вчиненні

тяжкого та особливо тяжкого злочину, за який передбачене покарання у вигляді позбавлення волі 5 років і більше.

Суддя має право, у випадку, якщо того потребують інтереси слідства, дати вказівку про проведення перехоплення кореспонденції, що передається шляхом телекомунікацій, про її магнітний запис і проведення письмового запису її змісту. Всі ці дії проводяться за його особистою відповідальністю та під його контролем.

Вказівка про перехоплення дається в письмовій формі. Вона не носить характеру судового рішення та не може бути оскаржена. Таким чином, «вказівка» є своєрідним документом, аналога якого немає в українському законодавстві. Нею встановлюється особиста повна відповідальність судді за свої дії, в тому числі цивільно-правова. За українським законодавством відповідальність судді має субсидіарний характер. Повну відповідальність несе держава.

В Україні дозвіл судді на перехоплення телекомунікацій та інші заходи потрібен як в процесі ОРД, так і в процесі кримінального провадження, процедура його отримання подібна. Це вказує на те, що в Україні в частині застосування ОТЗ в ОРД та КРД фактично діють процесуальні норми, що дещо звужує поле діяльності спецслужб України в інтересах безпеки в сфері оперативно-технічної діяльності.

==========***==========

УДК 321.01
О. К. Задувайло,
аспірант відділу інформаційної безпеки
та розвитку інформаційного суспільства
Національного інституту стратегічних
досліджень, м. Київ

Науковий керівник ***Д. В. Дубов,***
к.п.н, с.н.с., завідувач відділу інформаційної
безпеки та розвитку інформаційного суспільства
Національного інституту стратегічних досліджень

ДОСЯГНЕННЯ БАЛАНСУ МІЖ СУСПІЛЬНИМ ІНТЕРЕСОМ І ДЕРЖАВНИМИ СЕКРЕТАМИ НА МІЖНАРОДНО-ПРАВОВОМУ РІВНІ

Спроможність громадян робити запити і отримувати інформацію щодо розробок та діяльності свого уряду має вирішальне значення для прозорості та підзвітності органів державної влади. Та на жаль, значний обсяг такої інформації утримується під грифом секретності, що означає серйозне порушення права на свободу слова гарантованого міжнародним правом. Ця проблема особливо характерна для пострадянських країн, що зберегли традиції культу «секретності» тоталітарного політичного режиму СРСР.

Реалізація людиною права на інформацію передбачає доступ до матеріалів (записів, документів та інших видів інформації), що перебувають у документообігу органів державної влади та суспільних організацій, окрім випадків встановлених національним законодавством: захисту інтересів національної безпеки і міжнародних відносин, недоторканність приватного життя, комерційну таємницю, правоохоронну діяльність та публічний порядок, конфіденційну інформацію, а також переговори з країнами-союзниками та партнерами. Міжнародне право визначає національну безпеку, як законне обмеження свободи слова та інформації, і багато національних законів визначають, яким чином воно повинно застосовуватися, та все ж це залишається одним з найбільш проблемних обмежень, тому що їм регулярно зловживають і використовують в приватних інтересів, що в свою чергу суперечить міжнародним стандартам.

Цілий ряд міжнародних організацій, що відповідають за лобіювання у сфері захисту права людини на доступ до інформації активно вивчають співвідношення інтересів, що складають суспільний інтерес та національну безпеку держави. В першу чергу, акцентується увага на досягненні розумного обмеження сфери дії державної та службової таємниці та неприпустимість зловживання поняттям «національна безпека».

Комітет з правових питань та прав людини ПАРЄ, зазначає: «Надмірно широкі і розпливчасті виключення національної безпеки, що складають суспільний інтерес дозволяють приховувати незаконну діяльність органів державної влади і окремих посадових осіб. Тому всі обмеження з цього права повинні бути чітко визначені в законодавстві та пропорційні цілям, які вони захищають, як необхідна міра існування демократичного суспільства.» [1]

Значним досягненням міжнародної спільноти у вирішенні найбільш спірного питання засекречення інформації в інтересах національної безпеки стало підписання Резолюції № 1954 Національної безпеки та доступу до інформації ПАСЕ. Резолюції має на меті зобов'язати всіх членів ЄС оновити своє законодавство відповідно до вимог, які зазначені в документі «Глобальні принципи національної секретності і права на інформацію» (The Global Principles on National Security and the Right to Information) [2]. Дані принципи узагальнюють підхід до розуміння меж національної безпеки, а також містять дефініції базових визначень: інформація, що складає суспільний інтерес, законний інтерес національної безпеки, торгівельно-промислові підприємства в секторі національної безпеки тощо.

На нашу думку, варто зосередити увагу на декількох з них. Перший принцип, передбачає вимоги до обмеження права на інформація з міркувань національної безпеки. Не може бути накладено жодних обмежень на доступ до інформації з міркувань національної безпеки, якщо уряд не може довести, що обмеження встановлені законодавством і є необхідними у демократичному суспільстві для захисту законних інтересів національної безпеки. Також закон передбачає відповідні гарантії проти зловживань, в тому числі швидкий, повний, доступний і ефективний розгляд обґрунтованості обмеження незалежним органом нагляду. Вузькі категорії інформації, які можуть бути утримані з міркувань національної безпеки повинні бути чітко викладені в законі. Обмеження повинно відповідати принципу пропорційності і визначати адекватні засоби захисту від можливої

шкоди. Інформація про грубі порушення прав людини ні за яких обставин не повинна оголошуватися секретною з міркувань національної безпеки. Інший не менш важливий принцип має назву «Жодних виключень для будь-якого державного органу». В доступі до інформації не може бути відмовлено з міркувань національної безпеки тільки на тій підставі, тому що вона була розроблена, або спільно з іноземними державами, або міжурядовими органами, або конкретним державним органом чи підрозділом в межах своїх повноважень [3].

Дані принципи викликають неоднозначну думку з боку спеціалістів, які вважають, що даний підхід не досить вдалий, адже автори зазначеної концепції спробували максимально конкретизувати обґрунтування державних органів засекречування інформації. Це може привести до виникнення ситуації, при якій детальний опис конкретних причин, конкретних ризиків загрози може само по собі спричинити розголошення таємної інформації.

Та незважаючи на можливі недоліки, на наш погляд, прийняття такої резолюції є дуже важливим етапом у становленні інформаційної відкритості органів державної влади. У цих принципах виражена ідея оптимального підходу до питання співвідношення інформаційної безпеки та доступу до інформації. Дані принципи потребують детального опрацювання та використання для поліпшення українського законодавства в сфері інформаційного права.

Література

1. Doc. 12548 Parliamentary Asambly Електронний ресурс]. – 2011. – Режим доступу до ресурсу: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=13111&lang=en.

2. Резолюция № 1954 Национальная безопасность и доступ к информации ПАСЕ [Електронний ресурс]. – 2013. – Режим доступу до ресурсу:

http://www.coe.int/t/r/parliamentary_assembly/%5Brussian_documents%5D/%5B2013%5D/Oct2013/Res1954_rus.asp.

3. The Global Principles on National Security and the Right to Information [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf.

==========***==========

О. М. Солодка,
к.ю.н., с.н.с НА СБ України

УДОСКОНАЛЕННЯ ІНСТИТУТУ ТАЄМНИЦЬ ЯК ЗАСІБ ЗАБЕЗПЕЧЕННЯ ПРАВА НА ІНФОРМАЦІЮ

В інформаційному суспільстві одним із фундаментальних прав людини і громадянина визнано право на доступ до інформації, що відображено у відповідних документах міжнародної спільноти (передусім у Загальній декларації з прав людини, Міжнародному пакті про громадянські та політичні права, Європейській конвенції про захист прав людини та основоположних свобод). Так, у статті 10 Європейської конвенції йдеться про те, що кожен має право на свободу вираження поглядів, що включає свободу дотримуватися своїх поглядів, одержувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів. Принцип транскордонності є вкрай важливим в умовах інформатизації та глобалізації.

Однак, слід зазначити, що розвиток інформаційного суспільства може мати як позитивні, так і негативні наслідки, а відтак, щоб уникнути цього, держава повинна регулювати процес його формування. І, з одного боку, створювати умови для вільного доступу своїх громадян до інформації, з іншого – захищати ту інформацію, яка належить до секретної, що відображатиметься у встановленні необхідного балансу між потребою у вільному обміні інформацією і припустимими обмеженнями її поширення.

Правовий режим таємниці є одним із важливих інститутів права, що дає змогу встановити міру інформаційної захищеності, оптимально співвіднести інтереси людини, суспільства й держави, захистити основні права людини і громадянина, визначити межі дозволеного втручання у сферу приватного інтересу, не порушуючи закон. Результативність та ефективність заходів, що реалізуються державою у сфері охорони таємниці, безпосередньо залежать від нормального функціонування державно-правових інститутів, зокрема й від правового регулювання інформаційних відносин. Разом із тим, статус таємниці обмежує фундаментальне право особи на інформацію, що в умовах інформаційного суспільства виносить на порядок денний питання про необхідність трансформації правових режимів таємниць відповідно до реалій сьогодення.

Відтак, об'єктивні передумови трансформації правових режимів таємниць в умовах інформаційного суспільства вимагають вирішення таких питань:

- адаптацію законодавства України у сфері обігу інформації з обмеженим доступом до вимог НАТО і ЄС з урахуванням досвіду проведення АТО та особливостей ведення гібридної війни, скорочення обсягу таємної інформації, визначення процедур переходу таємної інформації з одного виду в інший (перегляд грифів в умовах її швидкого старіння);
- конкретизація визначення поняття «службова інформація», визначення та уніфікація на державному рівні критеріїв віднесення відомостей до даного виду інформації;
- правове врегулювання питань захисту персональних даних в інформаційних мережах, що передбачає практичну реалізацію принципу екстериторіальності правових норм у цій сфері, встановлення контролю особою за власними персональними даними;
- трансформація режиму банківської таємниці у сукупність взаємопов'язаних правових механізмів, які, з одного боку, дають змогу забезпечити запобігання розголошенню та неправомірному

використанню банківської таємниці, а з іншого – надають достатні можливості представникам уповноважених органів для виявлення, попередження та попередження злочинних діянь.

Разом із тим, на нашу думку, процесу трансформації правових режимів таємниць мають сприяти вже напрацьовані принципи забезпечення доступу громадян до інформації, які в умовах інформаційного суспільства повинні бути покладені в основу процедури обмеження доступу до інформації, а саме: максимальне розкриття; обов'язок публікувати; відкритий уряд; вичерпний перелік винятків; сприяння доступу; прийнятний рівень витрат; відкритість для громадськості засідань державних органів; першочергове значення відкритості інформації; захист інформаторів. Більшість з них сьогодні лише частково відображені у національному інформаційному законодавстві.

Крім цього, для того, щоб інформація правомірно обмежувалась у доступі, вона, згідно із трискладовим тестом, повинна відповідати трьом вимогам, а саме: повинна стосуватися легітимної мети, визначеної законом; оголошення такої інформації повинно загрожувати завданням суттєвої шкоди визначеній законом меті; шкода, яка може бути заподіяною цій меті повинна бути вагомішою, ніж суспільний інтерес в отриманні інформації.

Легітимна мета повинна бути виправдана визначеним в законі вичерпним переліком правових підстав для обмеження доступу до інформації. Ці підстави, як правило, зумовлені інтересами національної безпеки, територіальної цілісності або громадського порядку, необхідністю запобігання заворушенням чи злочинам, охорони здоров'я населення, захисту репутації або прав інших людей, запобігання розголошенню інформації, одержаної конфіденційно, підтримання авторитету і неупередженості правосуддя.

Хоча, наприклад, відповідно до положень Конституції України 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, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя. Відтак, з одного боку, Конституцією України передбачено вичерпні підстави можливого правомірного втручання в особисте та сімейне життя особи, а з іншої – поза правовим полем залишаються питання конкретизації інтересів національної безпеки, як і власне законодавчого визначення змісту цього поняття.

Тема суспільної значущості інформації актуалізується щоразу, коли є легітимні підстави обмеження доступу до певної інформації та з'являється потреба застосування права громадськості дізнатися про неї. Визнання інформації суспільно необхідною має бути безперечним юридичним фактом, що дозволяв би ставити питання про поширення такої інформацію без згоди її власника.

Предметом суспільного інтересу вважається інформація, яка свідчить про загрозу державному суверенітету, територіальній цілісності; забезпечує реалізацію конституційних прав, свобод і обов'язків; свідчить про можливість порушення прав людини, введення громадськості в оману, шкідливі екологічні та інші негативні наслідки діяльності (бездіяльності) фізичних або юридичних осіб тощо, тобто у кожному конкретному випадку необхідно встановити, яка інформація є суспільно необхідною.

При розгляді питання шкоди слід звертати увагу на такі аспекти, як переваги відкритого використання відомостей, що підлягають віднесенню до таємниці, а також витрати на захист таких відомостей у порівнянні із збитками, що можуть бути завдані, у разі їх розголошення.

Із розвитком сучасних інформаційних і комунікаційних технологій та їх застосуванням в усіх сферах життя, із збільшенням кількості та якості

інформації, визнання права на інформацію одним із фундаментальних прав людини в інформаційному суспільстві зумовлює необхідність трансформації правових режимів таємниць, що має враховувати прогалини та колізії правового регулювання обігу таємної інформації не лише в масштабах однієї держави, а й на міждержавному рівні, фактори інформатизації сучасного суспільства та основоположні принципи свободи доступу до інформації.

==========***==========

Ю. Б. Ірха,
науковий консультант судді
Конституційного Суду України

АНОНІМНІСТЬ ЯК ФАКТОР ВИКОРИСТАННЯ МЕРЕЖІ ІНТЕРНЕТ В ЕКСТРЕМІСТСЬКИХ ЦІЛЯХ

Свобода інформації є одним із визначальних факторів утвердження демократичного суспільства. Вона сприяє вільному формуванню особистості, самореалізації індивідів, налагодженню між ними контактів та взаємодії, об'єднанню їх у групи, запровадженню комунікації між громадянським суспільством і державою, цивільному контролю за діяльністю посадових та службових осіб органів публічної влади тощо. У широкому розумінні саме свобода інформації забезпечує духовний, економічний, культурний, моральний, науково-технологічний, політичний, соціальний розвиток суспільства.

Гарантування і захист таких фундаментальних прав і свобод людини і громадянина, як право на свободу слова, право на інформацію, право на приватність, право на свободу творчості, а також недопущення цензури, ідеологічної та політичної диктатури є одними із першочергових кроків на шляху побудови правової держави. Свобода інформації не є абсолютною категорією, її реалізація має відбуватися у межах розумного і справедливого балансу між приватним та публічним інтересами. При цьому загальновизнано, що обмеження прав і свобод, які є складовими

названої категорії, має відбуватися виключно на підставі закону. Ці обмеження є необхідними для функціонування демократичного суспільства та повинні запроваджуватися в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для охорони публічного порядку для запобігання заворушенням чи злочинам, для охорони здоров'я чи моралі, для захисту репутації чи прав інших осіб, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету і безсторонності суду тощо.

Еволюція суспільства та правової думки постійно оновлює зміст і обсяг існуючих прав і свобод людини і громадянина, підходи до їх розуміння, а також формує нові права і свободи.

В епоху відкритого інформаційного суспільства одним із важливих елементів права на приватне життя стало право на анонімність, яке, як стверджує В. Серьогін, полягає у тому, що людина не може бути примушена розкрити свою ідентичність і має право вчиняти дії, спрямовані на те, щоб її не могли ідентифікувати оточуючі. Право на таку автономію приватного життя фактично передбачає знеособлення людини для того, щоб вона почувалася вільно й розкуто, не ризикуючи стати об'єктом пліток, пересудів, критичних оцінок чи навіть громадського осуду. За таких умов анонімність є ширмою, а то й щитом, що захищає внутрішній світ людини, дає їй змогу вільно розвиватися, самовиражатися, налагоджувати стосунки з іншими [1, с. 157].

Технологічний прогрес значно ускладнив реалізацію та захист права на анонімність, адже у розвинутому соціумі особу можна ідентифікувати за 2D- та 3D-зображеннями, голосом, ДНК, відбитками пальців рук, сітківкою ока, унікальним малюнком вен на долонях. Використовуючи мобільний телефон, розраховуючись банківською карткою, індивіди прямо чи опосередковано оприлюднюють про себе значний обсяг інформації, аналіз якої дозволяє сформувати відповідний профіль особи. На сьогодні держави мають значні

можливості для ідентифікації громадян у повсякденному житті, контролю за їх поведінкою, впливу на їх свідомість.

У недемократичних країнах влада, як правило, не зважає на необхідність максимально повної реалізації міжнародних стандартів гарантування і захисту свободи інформації та права на анонімність, тому доступ громадян до об'єктивних, неупереджених і достовірних даних про стан справ у таких державах суттєво обмежено, а їхня участь в управлінні державними справами є номінальною. У демократичних країнах втручання у свободу інформації та у реалізацію права на анонімність регламентовані та відбуваються, як правило, під судовим контролем. Зазначене не убезпечує інформаційну діяльність від запровадження державою надмірних обмежень, однак індивіди мають доступ до ефективних механізмів поновлення та захисту своїх прав і свобод.

Швидкий розвиток інтернет-технологій спричинив появу нових можливостей передачі інформації, які змінили природу спілкування та самовираження індивідів. На сьогодні мережа Інтернет стала універсальним способом і засобом передачі та зберігання, у тому числі анонімно, різноманітних відомостей. Екстериторіальний принцип її побудови, відсутність єдиного «власника», централізованого місця зберігання даних, універсального правового регулювання функціонування сформували віртуальний простір, який вважається вільним від державного втручання. Саме завдяки анонімності ця мережа стала шалено популярною та має значну кількість користувачів, особливо молоді.

Анонімність у мережі Інтернет стала цінністю, яка визнається та захищається на міжнародному рівні. Так, у Декларації про свободу комунікацій в Інтернеті Комітет міністрів Ради Європи наголосив, що з метою забезпечення захисту від стеження он-лайн і сприяння вільному вираженню інформації та ідей країни-члени Ради Європи поважатимуть бажання користувачів Інтернету не розкривати свою особистість (принцип 7) [2].

Спеціальний доповідач Ради Організації Об’єднаних Націй з прав людини Девід Кей зазначає, що анонімність та шифрування даних у мережі Інтернет (самостійно або у сукупності) створюють для індивідів зону приватності, у якій вони можуть безперешкодно формувати свої думки, виражати погляди та переконання. У випадках незаконної цензури анонімність та шифрування даних дають людям можливість обійти встановлені бар’єри й отримати вільний доступ до інформації та ідей, вони забезпечують конфіденційність і безпеку, які є необхідними для реалізації права на свободу вираження поглядів і переконань в епоху цифрових технологій [3].

Незважаючи на важливість інституту анонімності у становленні та розвитку людини, його все більш інтенсивно використовують для розповсюдження інформації у протиправних цілях, особливо в мережі Інтернет. Сучасні технології дозволяють приховувати діяльність у Всесвітній павутині. Цим користуються, зокрема, екстремісти для планування своїх акцій, вербування адептів, поширення відповідних матеріалів з метою пропаганди екстремістських ідеологій та залякування населення.

Надмірна анонімність у віртуальному середовищі породжує у людей почуття безкарності та вседозволеності, вона перетворює свободу інформації на інформаційний хаос. У мережі Інтернет анонімність сприяє не тільки самоствердженню екстремістів, але й уникненню ними відповідальності за посягання на права і свободи людини, суспільства та держави. Екстремізм і така його крайня форма прояву, як тероризм, стали реальними загрозами для миру та безпеки людства у XXI столітті. На нашу думку, держава та громадянське суспільство мають виробити демократичні механізми перешкоджання деструктивній діяльності екстремістів у мережі Інтернет та цивільного контролю за функціонуванням органів публічної влади у цій сфері.

Література

1. Серьогін В.А. Право на анонімність як елемент прайвесі [Текст] / В.А. Серьогін // Науковий вісник Ужгородського національного університету. Серія „Право“. – Ужгород, 2014. – Вип. 24. – Т. 1. – С. 154–159.

2. Декларація про свободу комунікацій в Інтернеті : Декларація, затверджена Комітетом Міністрів Ради Європи на 840-му засіданні заступників міністрів, (28 травня 2003 р., м. Страсбург) [Електронний ресурс]. – Режим доступу : http://medialaw.org.ua/library/deklaratsiya-pro-svobodu-komunikatsij-v-internet/.

3. David Kaye. Encryption, anonymity, and the human rights framework : Report of the Special Rapporteur of the United Nations Human Rights Council on the promotion and protection of the right to freedom of opinion and expression, 22.05.2015, № A/HRC/29/32 [Електронний ресурс]. – Режим доступу : http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx.

==========***==========

Л. В. Ковальчук,
2 курс, ІПСА, НТУУ “КПІ”
Науковий керівник:
Н. В. Ніколаєнко,
к.ф.н., доцент, ФСП НТУУ ”КПІ”

ВПЛИВ ІНФОРМАЦІЙНИХ ЧИННИКІВ

На сьогодні головними інформаційними каналами впливу на свідомість та на формування ідентичності є телебачення, преса, Інтернет та кіногалузь.

Особливе місце займає саме мережа, яка зазнала неймовірних змін за останнє десятиліття. Інформаційні системи і мережі, які вона в собі містить, виступають як підсилюючий соціальний, науковий, технічний засіб. У той же час вони виступають послаблюючим фактором, оскільки стають основним засобом в економічній, політичній, у військовій боротьбі, будучи при цьому вразливим місцем.

Нині соціальна сфера тісно переплітається з інформатикою. Користувачі Інтернету вже не уявляють своє життя без соціальних мереж та

додатків, за допомогою яких можна пересилати повідомлення. Створення робочих чатів є невід'ємною частиною у навчанні, на роботі , у звичайному побутовому спілкуванні. Також, таким чином можна здійснювати обмін важливими файлами, фотографіями, рефератами, домашнім завдання, жартами та ін. речами. Буквально за останній рік з'явилося багато мобільних додатків-месенджерів, які жорстко конкурують між собою. Яскравим прикладом є Viber, WhatsApp, Телеграм, Slack, Trello. Деякі з них повністю адаптовані під обговорення робочих процесів. Перехід до цих новинок надзвичайно полегшує трудові будні.

Розширення застосування засобів обчислювальної техніки, розширює горизонти наукових та практичних пізнань, стимулюючи процеси вдосконалення інформаційних технологій. І так, маючи доступ до мережі ти можеш швидко отримати інформацію, яка знаходиться в книгах, які не завжди є доступні, або знаходяться за тисячі кілометрів від тебе. Це обумовлює стрімкий розвиток всієї інформаційної структури суспільства. Адже рух до інформаційного суспільства — загальна тенденція для розвинених держав і країн, що розвиваються. Фоміних Н.Ю. вважає, що завдяки інформатиці відбувається інтелектуалізація суспільства [1].

Інформаційне суспільство, до якого неминуче прямує Україна, змінює статус інформації (відомостей, даних, знань) як каталізатора позитивних зрушень соціального буття. Інформаційні технології дають нові можливості тим, хто знає їх, володіє ними, вміє ними користуватися і вміє від них захищатися. Розвиток інформаційних технологій сьогодні стає домінуючим фактором, який впливає на прискорення соціальних змін сучасного суспільства. Нові технології створюють нові можливості, нові горизонти для розвитку особистості, розширюють діапазон вибору окремої людини. Згідно з думкою Фоміних Н.Ю., найвищу цінність у суспільстві має інформація, яка є атрибутом та істотною властивістю всіх життєвоважливих процесів [1].

Водночас обмеження на концентрацію засобів масової інформації і комунікації може реально призвести до маніпуляції масовою свідомістю, контролю за особистістю з боку або державних, або просто навіть тією категорією людей, які краще володіють цими технологіями.

Інформаційне суспільство – це принципово новий рівень в історії цивілізації, його основою виступають теоретичні знання, інформація та інформаційні технології. Саме вони є провідними цінностями майбутнього розвитку суспільства. Спроможність чи неспроможність суспільства керувати технологією, особливо стратегічними технологіями, значною мірою формує долю суспільства.

Література

1. Фоміних Н.Ю. Філософські й соціальні засади інформатизації іншомовної освіти, [електронний ресурс] - режим доступу: http://www.narodnaosvita.kiev.ua/?page_id=881.

==========***==========

І. О. Богініч,
доцент кафедри Національної
академії Служби безпеки України

І. О. Моргун,
доцент кафедри Національної
академії Служби безпеки України

ОСОБЛИВОСТІ ПОПЕРЕДЖЕННЯ НЕЗАКОННОГО ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ТЕХНІЧНИХ ЗАСОБІВ НЕГЛАСНОГО ОТРИМАННЯ ІНФОРМАЦІЇ

Конституцією України кожному громадянину гарантується недоторканність житла, таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. При цьому не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу

без її згоди, крім випадків, визначених законом, що стосуються, виключно, інтересів національної безпеки, економічного добробуту та прав людини.

Згідно із діючим законодавством України спеціальні технічні засоби негласного отримання інформації (далі – СТЗ) застосовуються при проведенні оперативно-розшукової, розвідувальної, контррозвідувальної діяльності, реалізації заходів із боротьби з тероризмом правоохоронними, іншими державними органами.

Нормативно-правовими актами використання СТЗ у цивільному обігу заборонено. Замовляти та використовувати СТЗ у випадках, визначених законом, можуть тільки правоохоронні, інші державні органи, які виступають суб'єктами оперативно-розшукової діяльності. Господарська діяльність з розроблення, виготовлення та торгівлі СТЗ повинна підлягати ліцензуванню.

Неконтрольоване зростання кількості СТЗ, удосконалення їх характеристик, технічних можливостей та постійне розширення сфери потенційного використання обумовлюють необхідність застосування кримінально-правового реагування на відповідні соціально небезпечні процеси. Так, на теперішній час у Кримінальному кодексі України (далі – КК України) діє ст. 359, відповідно до якої встановлюється кримінальна відповідальність за незаконне використання, збут та придбання СТЗ.

При цьому у нормативно-правовій базі України існують деякі невизначені у повній мірі питання теоретичного та прикладного характеру, пов'язані із кримінальними посяганнями, в яких використовуються СТЗ. Вони мають бути обговорені та потребують невідкладного розв'язання. Зокрема, на теперішній час відсутні усталені уявлення щодо характеру та змісту попереджувальних заходів щодо незаконного використання СТЗ, що обумовлює актуальність проведення відповідних наукових досліджень.

Відповідно до ст. 359 КК України незаконне використання СТЗ "карається штрафом від двохсот до тисячі неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до чотирьох років, або позбавленням волі на той самий строк". Ті ж самі дії, якщо вони вчинені повторно, за попередньою змовою групою осіб або організованою групою, або заподіяли істотну шкоду охоронюваним законом правам, свободам чи інтересам окремих громадян, державним чи громадським інтересам або інтересам окремих юридичних осіб, – "караються позбавленням волі на строк від семи до десяти років". При цьому об'єктом злочину виступає встановлений певний порядок використання СТЗ, який забезпечує дотримання конституційних прав людини і громадянина і законних інтересів юридичних осіб. З об'єктивної сторони злочин полягає у суспільно небезпечних діях – незаконному використанні вказаних технічних засобів. З суб'єктивної сторони даний злочин характеризується прямим умислом.

Під використанням СТЗ розуміється застосування їх у залежності від конкретного виду, за прямим призначенням. Використання СТЗ в Україні дозволяється тільки відповідним оперативним підрозділам на підставах і за умов, визначених законом. У будь-якому іншому випадку їх використання є незаконним.

Незаконна діяльність (контрабанда), пов'язана з переміщенням "через митний кордон України поза митним контролем або з приховуванням від митного контролю" СТЗ, за відповідних підстав кваліфікується за ч. 1 ст. 201 КК України "позбавленням волі на строк від трьох до семи років", а якщо ця "дія, вчинена за попередньою змовою групою осіб або особою, раніше судимою за злочин, передбачений цією статтею, або службовою особою з використанням службового становища – за ч. 2 ст. 201 КК України "карається позбавленням волі на строк від п'яти до дванадцяти років з конфіскацією майна".

Кваліфікованими видами злочину є незаконне використання СТЗ вчинене: 1) повторно; 2) за попередньою змовою групою осіб; 3) організованою групою; 4) таке, що заподіяло істотну шкоду охоронюваним законом правам чи інтересам окремих громадян, державним чи громадським інтересам або інтересам окремих юридичних осіб.

Поняття щодо повторності злочинів, вчинення злочину за попередньою змовою групою осіб, вчинення злочину організованою групою та злочинною організацією розкривається, відповідно, у ст. 32 і ст. 28 КК України. Істотною шкодою у ст. 359 КК України вважать шкоду, яка полягає, наприклад, у порушенні конституційних прав людини на недоторканність житла чи іншого володіння особи, таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції, на заборону втручання в особисте і сімейне життя людини, на свободу думки і слова, світогляду і віросповідання, на приватну власність або у порушенні інших прав людини і громадянина, у заподіянні значної матеріальної шкоди юридичній чи фізичній особі тощо.

Діючим законодавством визначено, що тільки оперативні підрозділи уповноважених правоохоронних органів України мають право використовувати різноманітні технічні засоби отримання інформації для попередження та розкриття злочинів у сфері національної безпеки, захисту державного суверенітету, конституційного ладу, територіальної цілісності, економічного, науково-технічного і оборонного потенціалу України, законних інтересів держави та прав громадян від розвідувально-підривної діяльності іноземних спеціальних служб, посягань з боку окремих іноземних організацій, груп та осіб, забезпечення охорони державної таємниці, захисту державних кордонів, а також розшуку підозрюваних осіб, які ухиляються від кримінального покарання, переховуються від органів розслідування, судових та інших установ державної влади. Тому СТЗ повинні спеціально створюватися, розроблятися, модернізуватися, програмуватися та

пристосовуватися лише для виконання завдань з негласного отримання інформації під час здійснення оперативно-розшукової, контррозвідувальної та антитерористичної діяльності органів і підрозділів Служби безпеки, розвідувальних органів України.

Дослідивши аспекти кримінального попередження незаконного використання СТЗ, необхідно визнати, що такі заходи у своїх правових та організаційних межах можуть бути розподілені на декілька форм. Наприклад, загальне попередження може виявлятися у встановленні механізмів захисту інформації в інформаційних мережах від незаконного втручання, розробленні та здійсненні заходів щодо перешкоджання та запобігання скоєнню злочинів у цій сфері. Повноваження у цьому напрямку розподілені між правоохоронними структурами (СБ України та ДССЗЗІУ), іншими державними установами у сфері зв'язку. Попередження на галузевому рівні полягає у регулюванні механізмів виготовлення, реалізації та імпорту СТЗ за допомогою ліцензування та контролю за виконанням ліцензійних умов, яке здійснює СБУ спільно із митними, податковими та іншими державними органами. Попередження також повинно здійснюватися правоохоронними органами адміністративної практики згідно ст. 164, ст. 195-5 Кодексу України про адміністративні правопорушення.

Враховуючи вищезазначене, запровадження відповідних дій полягає як у виконанні процесуальних заходів СБ України щодо попередження незаконного використання, придбання, збуту СТЗ, так і у створенні необхідних діючих механізмів судового контролю за застосуванням СТЗ правоохоронними структурами. У подальшому, аналіз накопичення статистичних даних відповідно до сучасної нормативної бази щодо створення, розроблення, удосконалення СТЗ в Україні, у тому числі іноземного виробництва, має прикладне значення для проведення оперативно-розшукових заходів правоохоронними органами України, що у свою чергу, дозволить з нових позицій оцінити та дослідити відповідні

аспекти попередження кримінальних злочинів та правопорушень у даній сфері.

==========***==========

І. Ф. Корж,
д.ю.н., с.н.с., завідувач науковим сектором
НДІ ІП НАПрН України

СУЧАСНІЙ УКРАЇНІ – СУЧАСНИЙ ВОЄННИЙ СТРАТЕГІЧНИЙ ДОКУМЕНТ

Ознайомившись із попередніми матеріалами заходу (пропозиції та висновки, надані Вадимом Тютюнником, Валентином Горовенком, Ігорем Лісодідом, Віталієм Лазоркіним), і підтримуючи більшість з них, у своєму виступі торкнуся такого аспекту із загального масиву проблем, пов'язаних із напрацюванням згаданого доктринального документу, як ефективності державного управління та дієвості механізмів впровадження у цій царині.

Як показують реалії сьогодення, Україна потребує нагальної побудови сучасного типу сектору безпеки і оборони в частині забезпечення воєнної безпеки, що передбачає:

- проведення воєнно-політичного та воєнно-стратегічного аналізу та усвідомлення реальних та можливих джерел, причин, цілей і характеру сучасних війн та воєнних конфліктів, включаючи нинішню гібридну війну Російської Федерації проти України; дослідження проблем запобігання виникненню сучасних війн і воєнних конфліктів та воєнно-політичних шляхів їх вирішення;
- обґрунтування та напрацювання воєнно-технічних шляхів запобігання війн та воєнних конфліктів.
- розробки методологічних основ оцінки та прогнозування воєнно-політичної обстановки, визначення науково-обгрунтованих рівнів воєнної небезпеки;

- розробки доктринальних основ та обґрунтування завдань, складу і побудови системи забезпечення воєнної безпеки держави, організації управління та взаємодії суб'єктів забезпечення на різних етапах її функціонування;
- обґрунтування концептуальних шляхів розбудови сектору безпеки і оборони, розвитку теорії воєнного мистецтва;
- обґрунтування реальних різнобічних шляхів зміцнення воєнної безпеки держави;
- напрацювання воєнних аспектів забезпечення безпеки держави в технічній та інформаційній сферах;
- напрацювання сучасної форми оцінювання стійкості та ефективності системи забезпечення воєнної безпеки та шляхів їх вирішення.

Для реалізації зазначеного необхідна, насамперед, наявність політичної волі з боку керівництва держави, а також, що не маловажно, здійснення ефективного контролю за реалізацією зазначеного з боку громадянського суспільства.

Розбудову даного сектору та напрацювання відповідних доктринальних та стратегічних документів, на наше переконання, мають здійснювати насамперед громадяни-патріоти, громадяни з наявністю сучасного стратегічного мислення, професіонали, компетентні у зазначених питаннях. А для цього державною владою має проводитися належна кадрова політика, має функціонувати мережа наукових аналітичних центрів, в яких би напрацьовувалися відповідні доктринальні та стратегічні документи.

Загальновідомо що існуюча система таких центрів (Національні інститути проблем міжнародної безпеки та проблем національної безпеки, державної безпеки) у свій час за відповідною указівкою була «успішно» знищена у 2010 та 2011 роках 5-ю колоною нинішнього агресора, яка цинічно прикривала свої дії необхідністю оптимізації діяльності з розроблення наукових засад національної безпеки України (Указ від 2 квітня 2010 р. № 471/2010). Внаслідок цього була підірвана наукова основа системи

забезпечення національної безпеки, розпорошена значна кількість наукових кадрів, фахівців-теоретиків і фахівців-практиків у даній сфері, що і уможливило нівелювання наукових напрацювань щодо можливого прогнозування сумнозвісних подій в Україні 2014-2015 років, впровадження яких змогло б, на нашу думку, їх не допустити.

Як свідчить аналіз правових документів, з якими приходилося мати справу протягом останніх років і які вносилися до парламенту для науково-правової експертизи, проблема кадрового підбору та їх розстановки у секторі безпеки і оборони, як була актуальною, так і залишається такою, що говорить про відсутність належної політичної волі для виправлення ситуації у даній царині. Як розставлялися у державній владі люди за принципом особистої відданості та партійної (корпоративної) належності, так і продовжують розставлятися. Принципи професійності і компетенції практично застосовуються лише до громадян, які призначаються на посади, на яких не приймаються політико-значимі рішення, тобто працівники для виконання завдань технічного характеру.

Для підтвердження зазначеного можна навести приклад подання до парламенту законопроекту (Про СЗРУ -2005 р.) під грифом «секретно», що вказує на фаховий рівень осіб, які це питання готували та санкціонували в Адміністрації Президента України. Або ж видання Указу ПУ «Про деякі заходи з оптимізації системи центральних органів виконавчої влади» від 24 грудня 2012 року № 726/2012, куди внесені явно не конституційні положення, якими розбалансовувалася система державного управління сектору безпеки і оборони (відповідно діяльність Адміністрації ДПСУ спрямовувалася і координувалася через Міністра внутрішніх справ України, а Державної служби України з надзвичайних ситуацій – через Міністра оборони України: п. п. 2 і 8 Розділу IV – зміни до Указу ПУ «Про оптимізацію системи центральних органів виконавчої влади від 9 грудня 2010 р. № 1085/2010). Зазначене хоча і було здійснено формально до положень ст.116 Конституції України щодо спрямування та координації

КМУ роботи ЦОВВ, однак було явно направлено на ослаблення функціонування МО і ДПСУ, які забезпечували воєнну безпеку держави. Водночас, спрямування та координація МВСУ функціонування ДПСУ, явно не відповідало положенням ст.106 Конституції, за якою ПУ, забезпечуючи державну незалежність, національну безпеку, здійснюючи керівництво у сферах національної безпеки і оборони держави, – не може передавати свої повноваження іншим особам або органам. Крім того, відповідно до положень ст. 107 КУ, РНБОУ є координаційним органом з питань національної безпеки і оборони при Президентові України. Саме на неї покладено координацію і контроль за діяльністю органів виконавчої влади у сфері національної безпеки і оборони.

Необхідно зазначити, що за здійснених у країні конституційних змін 2014 року (повернення КУ до редакції 1996 р.), пов'язаних і революцією гідності, у даній сфері хоч і відбулися певні зміни, однак відповідні недоліки, які були притаманні попередньому періоду, залишилися, а в деяких моментах навіть появилися нові з них. Так усе суспільство було свідком «дивних» на перший погляд прийняття кадрових рішень як у секторі безпеки і оборони, так і в інших сферах життєдіяльності (в Уряді, МО, СБУ, Генеральній прокуратурі, МОЗ тощо). За наявності в країні значної кількості професійного, компетентного, патріотично-налаштованого, військово- та спеціально- навченого особового складу, на керівні посади призначалися особи, які були далекі від відповідності цим критеріям, і за період діяльності яких держава понесла певні людські, матеріальні, політичні, іміджеві тощо втрати. Можна навести свіжі приклади зазначеного: щодо недавніх кадрових подій навколо Луганської ОВЦА, що має стати показовим для президента. Адже, це не перше публічне непорозуміння, пов'язане із розстановкою людей з обойми Януковича на найвищі посади у державі. Тут варто згадати і скандальне призначення Костянтина Бриля, який вважається людиною Сергія Льовочкіна, головою Запорізької ОДА, а також губернатора Кіровоградщини Сергія Кузьменка, близького до одного з керівників Адміністрації Януковича

Сергія Ларіна. Тож, м'яко кажучи, є очевидним, що хтось із АП опікується такими призначеннями.

І в даній ситуації належну громадянську позицію проявило українське суспільство, яке через громадські організації, активістів різних рухів і просто небайдужих громадян через механізми здійснення контролю за згаданим процесом здійснюють активний супротив дивним кадровим призначенням, викриваючи у владі перевтілених представників минулого режиму.

І саме в цьому проявиляється активна участь громадськості в організації та здійсненні цивільного контрою за функціонування воєнної сфери держави, вже не говорячи про вирішальну роль громадянських активістів і добровольців у перші дні та тижні агресії Росії проти України. Тому роль цивільної складової у здійсненні контролю за функціонування державної влади, насамперед у секторі безпеки і оборони, у прийняті безпосередньої участі в управлінні державними справами в нинішніх умовах є дуже важливою, якщо не вирішальною.

Важлива роль у зазначеному мала б належати функції здійснення парламентського контролю за сектором безпеки і оборони. Однак і у цій сфері мають місце кричущі недоліки, які не сприяють покращенню ситуації в ній. У такий важкий і відповідальний для країни час до комітету прийшов депутатський корпус, який не має відповідного досвіду і уміння. В цих умовах важливу роль у наданні їм належної професійної, компетентної допомоги для їхнього професійного становлення, як це передбачено у багатьох аналогічних комітетах парламентів світу, мали б зіграти працівники секретаріату комітету. Однак зазначене можливо за умови збереження колективом своєрідної «генетичної» кадрової пам'яті, в сенсі професіоналізму і компетенції. Цього ж у комітеті на сьогодні немає, оскільки відбулося, буду говорити прямо, витіснення професійної складової попереднього складу секретаріату – компетентних, належним чином підготовлених, з відповідним досвідом працівників, і заміни їх, всупереч вимог професійно-кваліфікаційних характеристик для цих посад, на нових,

непрофесійних, некомпетентних осіб, які фактично не мають ні відповідного уміння, ні відповідного досвіду, ні відповідної підготовки. Сьогодні у складі секретаріату немає жодної особи, яка б мала відповідну освіту і належний практичний досвід відповідно до предмету відання комітету. І що вражає, що при цьому відкидаються пропозиції представників громадянського суспільства щодо розгляду комітетом професійно підготовлених і компетентних кандидатів на зайняття відповідних посад.

Зазначений негатив усугубляється і тими політичними скандалами навколо керівництва комітету (публікації у мас-медіа питань звинувачень у рейдерстві, корупції, превалюванні політичних корпоративних інтересів над суспільними тощо), що мають місце в недалекому минулому і нині. Можна навести і розгляд на комітеті 28 лютого 2016 р. та опублікування у пресі стислої розсекреченої стенограми закритого засідання РНБОУ від 28 лютого 2014 року щодо ситуації в Криму. Зазначене, на думку багатьох аналітиків, має в собі політичний підтекст «обілити» одних, і «очорнити» інших. Тому говорити про можливість здійснення належного ефективного парламентського контролю за сектором безпеки і оборони у сучасних умовах, на моє переконання, не приходиться, оскільки тут превалює вузько-корпоративний інтерес, а не загальносуспільний.

Щодо самого документу, то на наш погляд, за наявності таких концептуальних документів, як: Закон України «Про основи національної безпеки України» від 19.06.2003 р., який визначає основні засади державної політики, спрямованої на захист національних інтересів і гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз в усіх сферах життєдіяльності; Стратегії сталого розвитку «Україна – 2020» (Указ ПУ від 12.01.2015 № 5/2015), яка визначає мету, вектори руху, дорожню карту, першочергові пріоритети та індикатори належних оборонних, соціально-економічних, організаційних, політико-правових умов становлення та розвитку України, а також прийняту на виконання зазначеної Стратегії та Угоди про асоціацію між Україною та ЄС, ратифікованою

Законом України від 16.09.2014 р., Стратегію національної безпеки України, затверджену Указом ПУ від 26.05.2015 р. № 287/2015 р. як відповідного плану дій щодо захисту таких фундаментальних цінностей, як незалежність, територіальна цілісність і суверенітет, гідність, демократія, людина, її права і свободи, верховенство права, забезпечення добробуту, мир та безпеку, логічно було б напрацювання не Воєнної доктрини, як декларативний документ про державну воєнну політику, а Стратегії воєнної безпеки, як стратегічного плану 2-го рівня по відношенню до Стратегії національної безпеки України як документу вищого рівня.

Однак, оскільки вже напрацьовано саме Воєнну доктрину, то пропоную до неї зауваження і пропозиції, які були надані від Інституту.

==========***==========

К. С. Мельник,
здобувач наукового ступеня к.ю.н.
НДІІП НАПрН України,
експерт з питань захисту персональних даних

НОВІТНІ ТЕНДЕНЦІЇ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В ЄВРОПЕЙСЬКОМУ СОЮЗІ: ДОСВІД ДЛЯ УКРАЇНИ

Постановка проблеми. Використання передових інформаційних технологій і досягнень науково-технічного прогресу надало людству неабиякі можливості для спілкування. Технологічні зміни у сфері інформаційних технологій, зокрема створення міжнародних просторових інформаційних систем обігу інформації, зумовили необхідність докорінних законодавчих змін в Європейському Союзі (далі – ЄС) у сфері захисту персональних даних.

З огляду на поступову тенденцію до вдосконалення положень про захист приватного життя на міжнародному рівні, важливим вбачається розгляд новітніх тенденцій захисту персональних даних в ЄС, пошук

найоптимальніших шляхів врегулювання цих питань у вітчизняному правовому полі.

У вітчизняній юридичній літературі дослідженню окремих питань цієї проблематики в різні часи приділяли увагу такі фахівці, як О. Баранов, В. Брижко, М. Різак, В. Панченко, М. Швець, О. Сидєльніков, А. Гевлич, О. Рогова, О. Радкевич та інші. Розгляд цього питання здійснюється і зарубіжними вченими – І. Вельдер, А. Міллер, Р. Холлборг. Багато аспектів правового регулювання у сфері захисту персональних даних в ЄС нині залишаються малодослідженими чи дискусійними, особливо в контексті постійного становлення законодавства у цій сфері. Більшість досліджень за даною тематикою здійснювались в рамках певних наукових, аналітичних статей.

Метою доповіді є комплексний аналіз новітніх тенденцій захисту персональних даних в Європейському Союзі, пошук найоптимальніших шляхів врегулювання та вирішення цих питань у вітчизняному правовому полі.

Виклад основного матеріалу. Інформація якою наші інформаційні системи в автоматичному режимі обмінюється з віддаленими серверами, є такими, за якими *«особа може бути конкретно ідентифікованою»*, тобто, відповідно до українського законодавства та права ЄС, така інформація фактично є «персональними даними», які, в свою чергу, є невід'ємною складовою приватного життя людини [1-2].

Сучасне право ЄС містить низку як спеціалізованих правових актів у сфері захисту персональних даних так і актів Ради Європи, установчих документів ЄС, актів «вторинного» законодавства у різних галузях. Загальна структура виглядає наступним чином:

- Директива 95/46/ЄС Європейського Парламенту і Ради "Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних" від 24 жовтня 1995 року (далі – Директива 95/46/ЄС) [3];

- Регламент (ЄС) № 45/2001 про захист фізичних осіб при обробці персональних даних інститутами і органами Співтовариства і про вільне переміщення таких даних (Регламент інститутів ЄС щодо захисту персональних даних);

- Директива 2002/58/ЄС «Про обробку персональних даних та захист таємниці у секторі електронних комунікацій (Директива про секретність та електронні комунікації);

- Рамкове рішення Ради ЄС № 2008/977/JHA про захист персональних даних, що обробляються в рамках поліцейського та судового співробітництва у кримінальних справах (Рамкове рішення про захист персональних даних);

- Акти Ради Європи, установчі документи ЄС, акти «вторинного» законодавства у різних галузях.

Призначенням базового, на сьогодні, правового акту ЄС - Директиви № 95/46/ЄС - є «забезпечення однакового рівня захисту прав і свобод особи при обробці персональних даних в усіх державах-членах ЄС». При цьому, «процес адаптації національного законодавства, яке діє у цій сфері, не повинен призводити до зменшення передбачуваного ним захисту, а навпаки, повинен намагатися гарантувати високий рівень захисту в ЄС». Саме тому, «гармонізація національного законодавства не повинна обмежуватися мінімальними заходами, а повинна бути повною» [3].

У січні 2012 року Європейська комісія, заявивши про необхідність модернізації існуючих норм захисту персональних даних у світлі стрімких технологічних змін та глобалізації, запропонувала пакет реформ у сфері захисту персональних даних.

До пакету реформ було включено:

- пропозиції щодо заміни Директиви 95/46/ЄС *Генеральним регламентом про захист персональних даних*, а також

- підготовки нової *Генеральної директиви про захист персональних даних*, у якій би передбачалось забезпечення захисту даних у таких сферах,

як поліцейське та судове співробітництво, спрямоване на подолання злочинності.

На сьогодні обговорення пакету реформ все ще триває на рівні громадськості та органів наднаціонального права ЄС.

Проект *Генерального регламенту про захист персональних даних* [4] містить низьку ключових моментів, які підлягають висвітленню з огляду на їх важливість в контексті нововведень:

- приведення законодавства у сфері захисту персональних даних у відповідність до «первинного» права ЄС;

- посилення права особи на захист своїх даних за усталеною схемою: «обробка контролером – контроль органу нагляду – можливість оскарження рішення органу нагляду»;

- забезпечення високого рівня охорони персональних даних у всіх сферах життєдіяльності, а також належного дотримання правил, введених з цією метою, у спрощенні процесу міжнародного переміщення персональних даних, та впровадженні єдиних стандартів з їх захисту.

Відмінність майбутнього Генерального регламенту про захист персональних даних від базової Директиви 95/46/ЄС полягає насамперед у юридичній силі цих документів. Регламент – акт прямої дії, є обов'язковим для виконання всіма державами-членами ЄС. В свою чергу, Директива потребує додаткових імплементаційних заходів з боку національних органів.

Інша відмінність вищезгаданих документів полягає у чіткому визначенні на рівні проекту Генерального регламенту сутності фундаментального права фізичної особи у сфері захисту персональних даних - "права бути забутим" (right to be forgotten) та меж його дії та підстав реалізації. Варто нагадати, що «право бути забутим» існувало в Європі з 1995 року в усіх країнах-членах ЄС (з прийняттям базової Директиви 95/46/ЄС). Сутність цього права: кожна людина може вимагати видалити свої дані у будь-який момент з будь-якого джерела їх обробки. Звичайно, існують і певні обмеження, наприклад, якщо дані використовуються з метою забезпечення свободи самовираження у

засобах масової інформації, а також, якщо держава або приватна компанія має право обробляти ці дані відповідно до визначеної законної мети їх обробки. Тож хоча обмеження й існують, в цілому «право бути забутим» має бути гарантованим, якщо немає підстав для подібних обмежень [3-4].

Стаття 17 проекту Генерального регламенту передбачає спеціальні сфери, в межах яких особи можуть вимагати виключення своєї персональної інформації з баз даних, куди вона була внесена: електронні комунікації, включаючи Інтернет; правоохоронна сфера; охорона здоров'я; клінічні дослідження; освіта.

Підстави для реалізації «права бути забутим» викладені наступним чином:

- дані більше не є необхідними для цілей, у яких здійснювалося їхнє одержання чи обробка;

- суб'єкт даних відкликає згоду, на підставі якої здійснюється обробка, або строк зберігання даних сплив, а інших правових підстав для обробки даних немає;

- суб'єкт даних заперечує проти обробки персональних даних згідно зі статтею 19 Регламенту («профілювання» без відома особи).

«Праву бути забутим» приділено чималу увагу у проекті Генерального регламенту ЄС із захисту персональних даних, зокрема від контролера даних (володільця персональних даних – українське законодавство) вимагається вироблення чіткого, послідовного правового і технічного механізму реалізації цього права [4].

Не зайвим буде згадати в цьому відношенні нещодавнє рішення Суду ЄС від 13 травня 2014 року. Так, Суд ЄС прийняв рішення у справі за позовом Національного агентства із захисту даних Іспанії в інтересах гр. Mario Costeja González проти дочірньої корпорації Google Іспанії та материнської компанії Google Inc. *(Google Spain SL, Google Inc. vs. Agencia Española de Protección de Datos)*, визнавши, що за певних обставин Google (як і інші пошукові сервіси) «зобов'язані вилучати з результатів пошуку

посилання на окремі статті, судові рішення чи інші документи, які містять персональні дані особи. Цим забезпечується «право бути забутим», за яким користувачі повинні отримати можливість звертатися до Інтернет-компаній з проханням знищити певну інформацію про них у мережі Інтернет» [5]. Свою позицію Суд ЄС обґрунтовує, зокрема, тим, що можливість отримати інформацію про фізичну особу за допомогою введення її імені в пошукову систему, значно спрощує доступ до неї для будь-якого Інтернет-користувача, і цим самим може відігравати суттєву роль в поширенні такої персональної інформації, а отже - становити більше втручання в фундаментальне право особи на приватність, ніж просто оприлюднення персональної інформації на окремій веб-сторінці [6-7].

Важливим нововведенням вищезгаданого проекту Генерального регламенту є також впровадження *права на перенесення даних*, тобто переміщення даних із однієї системи електронної обробки в іншу без будь-якого перешкоджання з боку контролера. Генеральний регламент встановлює право особи на отримання від контролера зазначених даних у структурованому та поширеному електронному форматі як передумову для цього та задля подальшого поліпшення доступу фізичних осіб до своїх персональних даних[4].

Питанню запобігання «профілюванню» без відома особи присвячена стаття 19 проекту Генерального регламенту. Забезпечення права суб’єкта даних не бути предметом заходів, які ґрунтуються на профілюванні, розвиває (з відповідними змінами та додатковими запобіжними заходами) положення частини 1 статті 15 Директиви 95/46 про автоматизовані індивідуальні рішення та враховує численні рекомендації Ради Європи щодо запобігання профілювання.

Важливими є також організаційно-правові нововведення. Це, насамперед, стосується створення посад “службовців” із захисту персональних даних (service persons). Ці службовці мають обов’язково бути наявними у компаніях, де кількість персоналу перевищує 250 осіб, а також у

державних установах. Вони будуть здійснювати спостереження за виконанням положень Регламенту на рівні компаній, та забезпечуватимуть досягнення необхідних результатів.

На сам кінець, слід розглянути питання *реформування органів нагляду за дотриманням права на захист даних*. Держави-члени ЄС можуть утворювати по декілька наглядових органів з урахуванням власної конституційної, організаційної та адміністративної структури. Якщо Держава-член утворює декілька органів нагляду, вона має встановити законом механізми забезпечення результативної участі цих органів нагляду у функціонуванні узгоджувального механізму. Держава-член повинна визначити орган нагляду, який виконує функції "єдиного вікна" для забезпечення дієвої участі зазначених органів нагляду в функціонуванні механізму, оперативної та безперешкодної співпраці з іншими органами нагляду, Європейською радою з захисту даних та Європейською Комісією. Кожний орган нагляду має бути забезпечений достатніми фінансовими та кадровими ресурсами, приміщенням та інфраструктурою, необхідними для дієвого виконання покладених на нього завдань, включаючи завдання у сфері взаємної допомоги та співробітництва з іншими органами нагляду в межах усього ЄС. Рішення наглядового органу можуть бути оскаржені в суді (фактична можливість) [4].

Висновки. Комплексний аналіз новітніх тенденцій захисту персональних даних в Європейському Союзі, пошук найоптимальніших шляхів врегулювання цих питань у вітчизняному правовому полі свідчить про необхідність інтенсифікації вироблення підходів до вирішення цих питань державою, суспільством, науковим середовищем.

Пошук шляхів врегулювання та вирішення цих питань може мати місце у 3х напрямах:

1. Запровадження дієвого механізму захисту прав людини на власні персональні дані, враховуючи новітні тенденції ЄС, обговорення доцільності внесення змін у вітчизняне законодавство (в контексті

реалізації «права бути забутим», права на перенесення даних, запобігання “профілюванню”).

2. Запровадження дієвого механізму функціонування інституту відповідальних осіб/структурних підрозділів, відповідальних за обробку та захист персональних даних, на підприємствах, установах, організаціях (як пропозиція – на рівні підзаконного нормативно-правового акту).
3. Вирішення питання можливості оскарження рішень вітчизняного уповноваженого органу з питань захисту персональних даних в суді.

Перспективи подальших досліджень, на думку автора, пов’язані із необхідністю вивчення нових тенденцій цієї проблематики в Європейському Союзі та пошуком можливостей впровадження найкращого європейського досвіду в законодавство України.

Література

Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI // Офіційний вісник України від 09.07.2010, № 49, с. 199

1. Конвенція Ради Європи про захист осіб у зв’язку з автоматизованою обробкою персональних даних // Офіційний вісник України. – 2011. – № 1. – С. 701.
2. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних: Директива Європейського парламенту і Ради № 95/46/ЄС. – Режим доступу: //www.zakon.rada.gov.ua/laws/show/994_242.
3. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [Електронний ресурс]. – Режим доступу: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
4. Judgment of the Court (Grand Chamber) of 13 May 2014. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and

Mario Costeja González. Case C-131/12 [Електронний ресурс]. – Режим доступу: http://curia.europa.eu/juris/liste.jsf?num=C-131/12

5. Рекомендації Комітету Міністрів державам-членам Ради Європи № R (99) 5 по захисту недоторканності приватного життя в Інтернеті [Електронний ресурс]. – Режим доступу: http://www.medialaw.kiev.ua/laws/laws_international/105/

6. Радкевич О.П. Конфіденційність персональної інформації в соціальних мережах / О.П. Радкевич // Вісник Вищої ради юстиції № 3 (11), 2012. - С. 215 – 224.

==========***==========

Підп. до друку 16.05.2016. Формат 60×84 1/16. Папір офс. Гарнітура Times.
Спосіб друку – ризографія. Ум. друк. арк. 8,83. Обл.-вид. арк. 14,69. Наклад 100 пр. Зам. № 16-78.

Національний технічний університет України

«Київський політехнічний інститут»

Видавництво «Політехніка»
Свідоцтво ДК № 1665 від 28.01.2004 р.
03056, Київ, вул. Політехнічна, 14, корп. 15
тел. (44) 204-81-78