

ПРАВОВІ ПРОБЛЕМИ ПРОТИДІЇ ВИКЛИКАМ НОВІТНЬОЇ ЗЛОЧИННОСТІ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Савінова Н. А.

кандидат юридичних наук, т.в.о. ученого секретаря Науково-дослідного інституту інформатики і права НАПрН України

Сприймаючи у якості правових проблем протидії негативним впливам, що трансформується, або виникає під впливом розвитку інформаційного суспільства (новітня злочинність), слід сприймати ті вади політико-правових та суто правових підходів, які унеможливають або гальмують ефективність такої протидії.

У цьому контексті такі проблеми у галузі протидії саме злочинності доцільно поділяти на проблеми загальноправові - ті, що належать до сфери правової політики на практиці та до питань загальної теорії права в науці, а також кримінально-правові - ті, що належать до компетенції регулювання кримінально-правовою політикою і кримінальним правом.

В цілому правові проблеми протидії новітній злочинності можна визначити як:

Загальноправові проблеми:

- 1. Втрачений час сприйняття інформаційної безпеки на державному політико-правовому рівні.*
- 2. Сприйняття інформаційної безпеки як окремої складової національної безпеки.*
- 3. "Точковість" протидії загрозам інформаційній безпеці на рівні правових тактико-стратегічних заходів.*

та кримінально-правові проблеми:

- 1. Невизначеність на рівні науки кримінального права, та, відповідно, на рівні Закону про кримінальну відповідальність*

можливості кримінальної відповідальності за посягання на свідомість індивіда, групи, суспільства.

2. Несприйняття наукою кримінального права рівня уразливості різних джерел та сфер життєдіяльності від дистанційних комунікаційних впливів.

3. Здійснення кримінально-правової протидії лише фактам, та відсутність реальної протидії загрозам, які породжують виникнення таких фактів.

Відповідно до сфери регулювання ці проблеми можна поділити на загальноправові та спеціально-правові - кримінально-правові. Дослідимо кожну з них.

Загальноправова проблема № 1: втрачений час сприйняття інформаційної безпеки на державному політико-правовому рівні. Після закінчення Другої світової війни суспільство жадало миру і готове було іти на все, аби убезпечити себе від мілітаристських та інших небезпечних впливів. Теорія суспільного договору Ж.-Ж.Руссо (теорія суспільної безпеки Арістотеля) повною мірою трансплантується на сучасні міждержавні об'єднання, суб'єкти яких консолідувалися з метою - забезпечення безпеки. Цей процес розпочався у 1945 році з визначення основ безпеки усього суспільства планети Земля, як спільна мета вони були закріплені у ч. 1 ст. 1 Статуту ООН. У цьому ж контексті слід згадати пізніші утворення Ради Європи, НАТО, Ліги арабських країн та ін.

В період з 1975 по 2000 р. бурхливі процеси глобалізації, інформатизації, розвитку комунікаційної інфраструктури почали перекидати старі схеми забезпечення безпеки через переорієнтацію суспільства на інші цінності та способи їх використання. Фактично, всі суспільні відносини переходять на "рейки" комунікаційної інфраструктури.

У той же час, у суспільстві того часу продовжували діяти принципи безпеки, орієнтовані на убезпечення інших, попередніх умов життя людей. Період "холодної війни" між СРСР та США, протистояння соцтабору капіталістичними країнами обумовлювали сприйняття явища безпеки насамперед, як безпеки однієї країни - національної безпеки. У СРСР національна безпека сприймалася переважно як безпека від зовнішнього мілітаристичного втручання.

Зникнення СРСР, демократичні перетворення у країнах на його теренах та інших країнах соціалістичного табору та нова політика дружніх стосунків з США та розвиненими країнами Європи і Азії обумовили швидкий прихід на територію України та інших країн глобальної мережі Internet, програмних продуктів, стільникового зв'язку та багатьох інших технологій, які забезпечили покриття комунікаційною інфраструктурою фактично всієї території і запровадження комунікаційної складової в усі сфери життя суспільства і інфраструктури держави.

У той же час поняття "національна безпека" нібито заморозилося: воно описувало й охоплювало переважно протидію мілітаристичним, економічним та соціальним загрозам, лишаючи інформаційні загрози сферою законодавчо невпорядкованою.

Загальноправова проблема № 2: сприйняття інформаційної безпеки як окремої складової національної безпеки. З запровадженням ІКТ можливість транскордонного обміну інформацією, питання безпеки набуло нової якості, і у суспільстві, яке використовувало нові технології, виникла життєво важлива необхідність - забезпечення відносин, які здійснюються при посередництві ІКТ. Інформаційна безпека у такому суспільстві сприймалася лише як елемент цілковитої безпеки, а остання сприймалася виключно як безпека національна. Фактично безпека суспільних відносин від інформаційних загроз і на новому етапі - розвитку інформаційного суспільства приймалася не як безпека від посягань як щодо основних ресурсів інформаційного суспільства, так і від таких, а цілковито як безпека інформації та ІКТ. Безпека від посягань на інформацію, по суті ж і становила сутність підходів до визначень інформаційної безпеки та її співвідношення з поняттям "національна безпека" у вітчизняній науці.

Здебільшого, вітчизняними науковцями інформаційна безпека пов'язується саме з національною безпекою як частина з цілим: її визнають як функціональну сферу національної безпеки, або невід'ємну складову національної безпеки, чи самостійний напрямок національної безпеки. Логічне пояснення цьому одне: похибка міститься саме у тому, що глобальне інформаційне суспільство обумовлює розвиток комунікацій до такого рівня, що вони нібито

пронизують всі суспільні відносини, стан забезпечення яких від загроз визнається комплексною безпекою суспільства. Остаточно доводить вірність цієї ідеї той факт, що суспільні відносини, на які спрямовується комплексна безпека, переорієнтовуються на інші ресурси - інформація, знання та ІКТ, комунікації в цілому стають тими цінностями, на виробництво яких направлені і економіка, і політика, і які, відповідно, стають продуктами користування і споживання населення.

На підтвердження цього тут слід навести визначення інформаційної безпеки, яке являє собою спільну позицію країн-членів ЄС, висловлене представником Швеції при обговоренні питань міжнародної інформаційної безпеки на 56-й сесії Генеральної Асамблеї ООН: "Інформаційна та мережна безпека означає захист особистої інформації про відправників і одержувачів, захист інформації від несанкціонованих змін, захист від несанкціонованого доступу до інформації і створення надійного джерела постачання обладнання, послуг та інформації. Інформаційна безпека також охоплює захист інформації, що стосується військового потенціалу та інших аспектів національної безпеки. *Недостатній захист життєво важливих інформаційних ресурсів і інформаційних та телекомунікаційних систем може створити загрозу для міждержавної безпеки*" [1].

У інформаційному суспільстві інформаційна безпека є невід'ємною складовою комплексної безпеки, а їх конфігурації повністю співпадають, і інформаційна складова повинна включатися у зміст поняття комплексної безпеки.

Загальноправова проблема № 3: "точковість" протидії загрозам інформаційній безпеці на рівні правових тактико-стратегічних заходів. Ані у Законі України "Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" [2], ані у відповідній стратегії, навіть, на рівні її обговорення [3] не міститься вказівок щодо необхідності розробки та запровадження комплексних тактичних та стратегічних заходів протидії новітній злочинності. Захисні дії держави у цій сфері обмежуються перманентним внесенням змін до окремих положень КК України, переважно відносно відповідальності саме (чомусь!) за злочини, передбачені Розділом XVI КК.

У той же час, у ст. 5 Закону України "Про основи національної безпеки" загрози у інформаційній сфері виділені окремим рядком і повною мірою відділені від загроз безпеці державній, до переліку яких віднесена корупція, організована злочинність, кіберзлочинність та кібертероризм.

І при цьому - жодного слова про трансформацію злочинності, видозмінення її під впливом можливостей дистанційних комунікацій, можливості тотальних впливів на свідомість через ЗМІ та соціальні мережі тощо. *Концептуальні акти законодавства, не враховуючи особливостей сучасних загроз новітньої злочинності, визначають окремі "точкові" необхідності протидії, лишаючи поза полем зору тотальні, системні виклики злочинності національній безпеці.*

Суто кримінально-правові проблеми дещо схожі з загально-правовими. Насамперед - застаріле бачення науковцями і практиками можливостей злочинності в нових умовах, яка призводить не лише до змін способів вчинення, а й до виникнення нових суспільно небезпечних діянь, які не могли вчинюватися за відсутності дистанційних комунікацій.

Розкриємо зміст цих проблем.

Невизначеність на рівні науки кримінального права, та, відповідно, на рівні Закону про кримінальну відповідальність можливості кримінальної відповідальності за посягання на свідомість індивіда, групи, суспільства (кримінально-правова проблема № 1). Хоча у ч. 1 ст. 1 КК України і міститься повний, на думку сучасного вітчизняного законодавця, перелік об'єктів кримінально-правової охорони, він є достатньо старим з точки зору необхідності врахування особливостей здійснення суспільно небезпечних посягань на свідомість. Такі посягання мали місце і раніше, деякі з них були криміналізовані (наприклад, злочин, передбачений ст. 190 КК Шахрайство). Можливість вчинення "обману" або "зловживання довірою" "з використанням електронно-обчислювальної техніки" також визнається сьогодні злочином (ч. 3 ст. 190 КК України). Аналогічно, стосовно "розповсюдження матеріалів" із закликами до насильницької зміни або повалення конституційного ладу або захоплення державної влади (ч. 2 ст. 109 КК України).

Однак цим, фактично, обмежується усвідомлення можливостей вчинення впливів на свідомість. Свідомість же сама, як об'єктивне явище, КК у якості об'єкта кримінально-правової охорони та безпосередньо предмета злочину не оцінюється.

У жодному з науково-практичних коментарів КК України термін "свідомість", як об'єкт посягання чи то об'єкт кримінально-правової охорони не визначається. Він використовується виключно при характеристиках інтелектуального моменту суб'єктивної сторони складу злочину.

Відсутнє бачення як науковцями-кримінологами, так і законодавцем того факту, що ми живемо у нову добу, коли свідомість стає наріжним каменем всіх суспільних змін, революцій, економічних та соціальних переворотів, незадоволеності владою, причиною насилля тощо.

Абсурдність такого небажання бачити очевидні речі підсилюється тим, що КК України, як і вказувалося стосовно двох попередніх випадків, містить, якнайменше, один склад злочину, безпосереднім об'єктом якого є свідомість людини. Це - передбачене ст. 120 "Доведення до самогубства". Об'єктивну сторону цього діяння утворюють діяння з жорстокого поводження з людиною, її шантажу, примусу до протиправних дій або систематичного приниження людської гідності, внаслідок яких відбувається самогубство або замах на нього. Тобто, йдеться про прямий вплив саме на свідомість людини, на її ставлення до цінності власного життя, розуміння своєї значимості. Впливи на свідомість мають місце і при вимаганні, і при впливі на виборців, і при вимаганні чи провокації хабара, зловживанні становищем в службових злочинах, яке здійснюється шляхом тиску на залежних осіб, тощо. Хоча безпосереднім об'єктом в таких випадках мають визнаватися суспільні відносини, яким завдається шкода, свідомість має оцінюватися як предмет злочину, адже саме на неї здійснюється злочинний вплив.

Кримінально-правовою проблемою (№ 2) протидії викликам новітньої злочинності в сучасних умовах є несприйняття наукою кримінального права рівня уразливості різних джерел та сфер життєдіяльності від дистанційних комунікаційних впливів.

Сучасною наукою кримінального права не визнаються можливості вчинення посягань на життя людини, її честь, гідність, основні людські права і свободи та на інші групові та родові об'єкти злочинів, у тому числі такі, здавалось би, недосяжні для новітніх технологій, як правосуддя чи військові злочини.

З використанням дистанційних комунікацій, побудованих на використанні сучасних ІКТ, можуть здійснюватися злочини, передбачені більш ніж третиною статей КК України. І хоча спосіб таких діянь переважно лишається факультативною ознакою, відповідно спосіб дистанційних комунікацій не перешкоджає правильній кваліфікації відповідних діянь, на жаль, на практиці, вірної кваліфікації майже не відбувається. Це обумовлюється тим, що практичні працівники не усвідомлюють таких нових можливостей злочинців, а на рівні коментарів та постанов Вишого спеціалізованого суду з розгляду цивільних та кримінальних справ України таких необхідних роз'яснень нема.

За наявності визначення превентивної функції кримінального права, зокрема, у цитованій раніше ч. 1 ст. 1 КК України, *здійснення кримінально-правової протидії сьогодні відбувається лише щодо фактів злочинів, за відсутності реальної протидії загрозам, які породжують виникнення таких фактів. Це зазначена вище кримінально-правова проблема протидії новітній злочинності № 3.*

У теорії кримінального права сьогодні фактично відсутні дослідження з оцінки потенційних загроз, необхідності упереджувальних дій щодо трансформованої злочинності або нових видів суспільно небезпечних діянь, що виникають під впливом нового середовища - інформаційного суспільства.

По суті, явища, які б мали розцінюватися наукою як кримінально-правові ризики - негативні явища, які набувають (або можуть набути у перспективі) суспільної небезпечності, випадають з поля зору кримінального права. Оскільки ж право завжди відстає від динаміки злочинності, на рівні переходу з загроз у реальні суспільно небезпечні діяння, останні лишаються некараними, адже відповідальність за потенційні, можливі діяння кримінальним правом не передбачається. Така ситуація свого часу мала місце стосовно кібернетичних злочинів, відображених спочатку у

ст. 198-1 КК України 1960 р., а пізніше у Розділі XVI Особливої частини КК України. Подібна ситуація мала місце і відносно шахрайства з використанням ІКТ, хоча, у певному обсязі вона зберігається і зараз: зміни до ч. 3 ст. 190 КК України торкнулися лише доповненням її особливо кваліфікованим складом "вчинення з використанням [лише, Н.С.] електронно-обчислювальної техніки"...

Зміни бачення державою нагальних проблем протидії злочинності нової доби, насамперед, залежать від політико-правових стратегій та рішень. Але такі стратегії неможливі без теоретичного підґрунтя наук теорії права та кримінального права у сфері забезпечення належного розвитку в державі інформаційного суспільства.

Література

1. "Developments in the field of information and télécommunications in the context of international security" / Report of the Secretary-General. - Fifti-Six Session. - United Nations. - 3 Juli 2001. - A/56/164
2. Закон України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" від 9 січня 2007 року № 537-V [Електронний ресурс] // Відомості Верховної Ради України. - Офіц. вид. - 2007. - № 12. - ст. 102. Режим доступу: <http://zakon1.rada.gov.ua/laws/show/537-16>
3. Результати громадського обговорення Стратегії розвитку інформаційного суспільства в Україні [Електронний ресурс] // Офіційний сайт Державного агентства з питань науки, інновацій та інформатизації України. - 03.08.2012. Режим доступу: <http://dknii.gov.ua>.

Науково-дослідний інститут інформатики і права
Національної академії правових наук України
Інститут політології і права
Національного педагогічного університету
імені М.П. Драгоманова

**ФІЛОСОФСЬКІ ТА СУСПІЛЬНО
ПРАВОВІ ПРОБЛЕМИ
СТАНОВЛЕННЯ І РОЗВИТКУ
ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА**

(Матеріали круглого столу)

Ужгород
ТОВ "ІВА"
2013

УДК 303.725.37
ББК 60.033.3
Ф 56

*Рекомендовано до друку Вченою радою
Науково-дослідного інституту інформатики
і права Національної академії правових наук України,
протокол № 6 від 21 червня 2013 року.*

Упорядники:

*Андрусишин Б. І., Майстренко І. А.,
Пилипчук В. Г., Фурашев В. М.*

Філософські та суспільно-правові проблеми становлення і ф 56 розвитку інформаційного суспільства: Матеріали круглого столу / 20 березня 2013 р., м. Київ / Упорядн.: Андрусишин Б. І., Майстренко І. А., Пилипчук В. Г., Фурашев В. М. - Ужгород : ТОВ "ІВА", 2013. - 194 с.

ISBN 978-617-501-071-6

До збірки увійшли матеріали, надані учасниками круглого столу "Філософські та суспільно-правові проблеми становлення і розвитку інформаційного суспільства", що відбувся 20 березня 2013 року в м. Києві.

Збірник охоплює низку актуальних проблем розбудови інформаційного суспільства, особливостей інформаційної діяльності та регулювання суспільних відносин в інформаційній сфері, протидії інформаційним викликам і загрозам, містить сформульовані завдання і рекомендації з питань формування та розвитку інформаційного суспільства в Україні.

Організатори круглого столу висловлюють вдячність за надану інформаційну підтримку у проведенні круглого столу газеті "Голос України", журналам "Інформація і право", "Правова інформатика". "Інформація та безпека", "Економіка і право", "Юридичному журналу", тижневику "Юридична практика" та "Юридичній газеті".

Матеріали круглого столу можуть бути корисними для фахівців заінтересованих державних органів та органів місцевого самоврядування, експертів і вчених інформаційної сфери, науково-педагогічного складу, аспірантів, докторантів, студентів вищих навчальних закладів, а також усіх, хто цікавиться суспільно-правовими та іншими проблемами становлення інформаційного суспільства.

- © Науково-дослідний інститут інформатики і права НАПрН України, 2013
- © Інститут політології і права НПУ ім. М.П. Драгоманова, 2013
- © Колектив авторів, 2013
- © ТОВ "ІВА", 2013

ISBN 978-617-501-071-6