АКТУАЛЬНІ ПИТАННЯ ЮРИСПРУДЕНЦІЇ

УДК 343:973

ВАСИЛЬКОВСКИЙ І.І.

ДЕРЖАВНЕ РЕГУЛЮВАННЯ І САМОРЕГУЛЮВАННЯ ЯК МОДЕЛЬ БОРОРОТЬБИ З КІБЕРЗЛОЧИНАМИ

У статті розглядаються питання державного регулювання і саморегулювання як моделі бороротьби з кіберзлочинами, які можуть співіснувати в різних формах, в залежності від області співробітництва

Ключові слова: *державне регулювання, саморегулювання, кіберзлочини, співробітництво.*

В статье рассматриваются вопросы государственного регулирования и саморегулирования как модели бороротьбы с киберпреступностью, которые могут сосуществовать в различных формах, в зависимости от области сотрудничества

Ключевые слова: *государственное регулирование, саморегулирование, киберпреступления, сотрудничество.*

The article deals with issues of state regulation and self-regulation as a model for the fight against cybercrime that can coexist in different forms, depending on the area of cooperation.

Key words: *state regulation, self-regulation, cybercrime, cooperation.*

З розвитком інформаційних технологій питання боротьби зі злочинністю в глобальних інформаційних мережах виходить далеко за рамки таких проблем, як розробка норм кримінального та кримінального процесуального права, що дозволяють проводити ефективне розслідування і переслідування електронних посягань. Проникнення інформаційних мереж буквально в усі сфери життя і зростаюча залежність від глобального інформаційного середовища держави, бізнесу і суспільства обумовлюють необхідність вироблення нового підходу до забезпечення кібербезпеки.

Метою даної статті є визначення підходу, який повинен враховувати, крім транскордонної природи кіберпростору, той факт, що в інформаційному обміні бере участь незліченну кількість приватних осіб та комерційних компаній. Глобальні інформаційні мережі включають все більша і більша кількість взаємозалежних суб'єктів: сьогодні безпеку користувачів і критичних інформаційних інфраструктур залежить від компаній, які володіють мережами або є постачальниками певних послуг (банківських, фінансових, послуг зв'язку та інших).

Розвиток інформаційних мереж і послуг в останні два десятиліття у багатьох країнах було, і до сих пір залишається заслугою приватного бізнесу і його інвестицій. Однак в результаті цього еволюція глобальних інформаційних технологій на кілька кроків випереджає розвиток принципів і моделей їх регулювання. У багатьох країнах саме приватний сектор володіє і управляє комунікаційної інфраструктурою, будучи «двигуном» зростання використання інформаційних технологій, в той час як на рівні держави чітке розуміння того, як повинні регулюватися багато аспектів кіберпростору (і повинні взагалі) або відсутня, або перебуває в зародковому стані.

Одним з цих аспектів регулювання кіберпростору є питання: хто несе відповідальність за кібербезпека і як розподілити відповідальність щодо захисту громадських інтересів при тому, що посягання на ці інтереси відбуваються в мережах, якими володіє приватний бізнес. Однією з останніх тенденцій, в зв'язку з цим, є усвідомлення, як на рівні держави, так і на рівні бізнесу, необхідність розробки підходів до спільної діяльності в галузі боротьби зі злочинністю та кібербезпеки.

© ВАСИЛЬКОВСКИЙ І.І. – аспірант кафедри кримінального права, процесу та криміналістики (ПВНЗ «Європейський університет»)

Необхідність залучення бізнесу до участі в боротьбі з кіберзлочинністю і в забезпеченні безпеки в кіберпросторі обумовлена децентралізованою структурою інформаційних мереж і їх транскордонних. Оскільки злочинці можуть легко обійти традиційні механізми регулювання, наприклад, оперуючи з території держав, де відсутні правові норми в області боротьби з електронними посяганнями, централізоване правотворчість і правозастосування, яке історично є ядром будь-якої концепції боротьби зі злочинністю в рамках держави, не може впоратися з проблемою злочинності в інформаційних мережах [1].

Інтернет в цілому, як децентралізована структура, змінив традиційні моделі правового регулювання з їх ієрархією, коли держава перебуває на вершині «піраміди» управління і володіє необхідними інструментами контролю. Ці традиційні моделі не застосовні до інформаційних мереж, оскільки в децентралізованої структурі застосування старих механізмів контролю та примусу не завжди можливо. Необхідність вироблення нових способів регулювання особливо позначається на системі боротьби зі злочинністю, оскільки правозастосування в сфері кримінального та кримінально-процесуального права в цілому є однією з найвищих форм державного примусу, що вимагає наявності механізмів соціального контролю.

З розвитком глобальних інформаційних мереж система протидії злочинності в кіберпросторі стає все складніше, оскільки проблема зачіпає ті сфери, які до повсюдного поширення інформаційних технологій ставилися до різних областей регулювання: наприклад, банківська сфера і телекомунікаційні технології. В результаті регулюючі органи можуть бути наділені повноваженнями, які дублюють один одного. У сфері боротьби з кіберзлочинністю і її попередження це часто створює ситуацію, коли неясно, який державний орган відповідальний за регулювання в певній галузі і що власне підлягає регулюванню взагалі [2].

Саме ця невизначеність вкупі з неможливістю застосування багатьох традиційних ієрархічних механізмів контролю створює нові моделі співпраці – як вважають деякі дослідження [3], боротьба з кіберзлочинністю на національному та міжнародному рівні трансформується в нову систему, яку правильніше називати «мережевий моделлю». Ця система сфокусована не на тому, які суб'єкти (державні органи або приватні компанії) відповідальні за боротьбу з кіберзлочинністю, а на процесах і діяльності, необхідних для запобігання, розслідування, переслідування електронних посягань (наприклад, створення «гарячих ліній» для повідомлення про нелегальне контенті або дії, необхідні для боротьби з ботнетами), і каналах обміну інформацією між учасниками системи. У різних державах учасники мережевої моделі можуть бути різними – наприклад, на національному рівні боротьбою зі спамом можуть займатися правоохоронні органи, спеціальні адміністративні органи, органи по захисту прав споживачів, державні інститути з охорони персональних даних тощо. Однак відповідно до «мережевий моделлю» важливий не суб'єкт цієї діяльності, а процес сам по собі: модель відображає різноманіття акторів в системі боротьби з кіберзлочинністю і безліч підходів, але при цьому акцент ставиться на необхідність виконання певних функцій (нормотворчої, контрольної, превентивної, функції примусу і т.п.) в цій області, які б суб'єкти не були відповідальні за їх виконання.

Включення приватного бізнесу в цю систему – необхідність, зумовлена багатьма факторами. Крім загальної проблеми децентралізації та труднощів застосування традиційних ієрархічних моделей регулювання, сама природа кіберзлочинності з її глобальністю, транскордонного та швидкістю передачі інформації в комунікаційних мережах створює труднощі для застосування механізмів державного контролю. Держава в силу обмеженості застосування традиційних механізмів примусу не може бути єдиним учасником, зацікавленим в боротьбі з кіберзлочинністю, і єдиним суб'єктом, відповідальним за безпеку в глобальних інформаційних мережах. Висока латентність кіберзлочинів і недолік механізмів і ресурсів з боку держави створюють ситуацію, коли правоохоронні органи можуть без підтримки з боку приватного бізнесу розкривати і розслідувати тільки «мізерну частину» [4] від загальної кількості злочинних посягань, скоєних в мережі Інтернет [5]. Співпраця з бізнесом розширює можливості вироблення нових і адаптації вже існуючих механізмів протидії злочинності в кіберпросторі, створюючи в кінцевому підсумку гнучкий механізм контролю, що дозволяє реагувати на нові способи вчинення посягань і нові загрози [6].

Держава і бізнес в сфері боротьби з кіберзлочинністю доповнюють один одного в різних областях компетенції. Держава володіє необхідними механізмами для правотворчості і правозастосування (за допомогою механізмів примусу). Приватний бізнес, в силу того, що саме завдяки його участі відбувається розвиток і зростання інформаційних технологій, володіє великими знаннями в цій області, і здатний швидше розпізнавати нові проблеми і гнучкіше реагувати на них. Неможливо вимагати від держави, щоб воно своїми силами за короткий час акумулював

необхідні пізнання і знайшло необхідні ресурси для розкриття і кримінального переслідування будь-яких зазіхань в кіберпросторі. Тільки співпраця з приватним сектором дозволить поліпшити зусилля держави в боротьбі з кіберзлочинністю, саме тому багато країн виробляють моделі співпраці з бізнесом, що дозволяють обом сторонам доповнити «сильні» сторони один одного [7].

Стверджується, що спільне регулювання і саморегулювання в області боротьби з кіберзлочинністю подає більше надій на успіх, ніж традиційні правозастосовні заходи [8]. Різні суб'єкти бізнес-спільноти, які оперують в різних сферах послуг, розглядаються державою як критичний елемент боротьби з посяганнями в кіберпросторі. Крім Інтернет-провайдерів, в систему боротьби з кіберзлочинністю включаються компанії в галузі електронної комерції, мобільного комерції, електронних платежів, розробники додатків, постачальники обладнання [9].

Спільне регулювання і саморегулювання, будучи допоміжними джерелами і формами правового регулювання, мають на увазі різний рівень державної інтервенції. Оскільки спільне регулювання включає можливості прямого втручання держави в процес, особливо в області застосування механізмів примусу в разі порушень, ця форма регулювання розглядається в якості різновиду ієрархічної моделі з «низхідним» регулюванням, де ініціатором і гарантом виконання є держава і його механізми примусу [10]. Спільне регулювання розглядається як допоміжні заходи, які доповнюють існуючі правові норми, встановлені законом, але не є альтернативою регулюванню як механізму примусу і контролю.

Саморегулювання відрізняється (по крайней мере, в теорії) тим, що воно ініціюється приватним бізнесом і включає в себе заходи, які розробляються і встановлюються без прямої участі держави. Держава також не має прямого відношення до виконання цих заходів: приватний бізнес контролює сам себе і здатний в цьому випадку застосувати відповідні механізми примусу щодо суб'єктів, які порушують встановлені норми поведінки. Цю модель називають «висхідною», що означає, що ініціатива виходить не від держави по низхідній ієрархічної лінії, а від бізнесу, «знизу», з точки зору традиційних моделей регулювання [10].

У різних державах ці дві моделі можуть співіснувати в різних формах, в залежності від області співробітництва. Спільне регулювання як більш інтенсивний варіант державної інтервенції існує, коли елементи співпраці в тій чи іншій мірі регулюються законодавством, або коли держава частково відповідальна за механізми контролю і примусу в разі порушення партнерами добровільно взятих на себе зобов'язань [11]. Ступінь втручання може бути різною: від угод між державою та приватними компаніями, які передбачають відповідальність за їх порушення, до таких форм, як регулювання законом принципів співпраці між державою і приватними партнерами. У деяких випадках співробітництво може бути обумовлено певними прогалинами в законодавстві. Наприклад, в Нідерландах ініціатива спільного регулювання процесу блокування і видалення нелегального контенту виходила від бізнес-спільноти.

Однак ця добровільна міра з їхнього боку була обумовлена тим, що в країні були законодавчо введені зобов'язання Інтернет-провайдерів з видалення нелегального контенту з заходами відповідальності в разі за їх невиконання, при цьому відсутнє регулювання процедур повідомлення провайдерів і видалення контенту [12]. Бізнесу нічого не залишалося, як виступити з ініціативою вирішення проблеми, не чекаючи інтервенції держави.

Інтервенція держави при спільному регулюванні, і навіть при саморегулювання, може приймати різні форми. Держава може сприяти без прямого втручання створенню різних асоціацій, організацій і форумів. Підтримка може бути надана при розробці угод між бізнесом і правоохоронними органами, при створенні «гарячих ліній» та інших платформ для повідомлення про нелегальне контенті, а також при розробці програм підвищення обізнаності суспільства про кіберзлочинність.

На відміну від спільного регулювання, де державна інтервенція презюмується як необхідний компонент, саморегулювання здійснюється виключно бізнес-спільнотою, і зазвичай представлено у вигляді неієрархічних організацій, таких, як асоціації та об'єднання в рамках певної індустрії. Участь цих організацій в боротьбі з кіберзлочинністю може приймати різні форми, від співпраці для розслідування конкретного злочину до довгострокових програм, таких, як кодекси поведінки або «гарячі лінії», що реєструють повідомлення про правопорушення.

У багатьох країнах держава так чи інакше задіяні в ініціативах саморегулювання, хоча найчастіше без прямої участі [13] – воно може бути ініціатором тих чи інших програм або надавати їм підтримку, хоча самі програми здійснюються приватним бізнесом.

У деяких країнах – наприклад, в Німеччині, – досить складно розмежувати саморегулювання, спільне регулювання і державний контроль. Так, одна з німецьких програм саморегулю-

вання була ініційована державою: в законодавстві встановлено, що захист інтересів неповнолітніх в медіа-індустрії (в тому числі в питаннях, що стосуються шкідливого контенту) повинна здійснюватися саморегулюючими асоціаціями на підставі підписаного учасниками ринку угоди. Ці асоціації є казус, званий «регульованим саморегулюванням» – форма самоконтролю для бізнесу була ініційована державою і встановлена законом (пряма інтервенція), хоча самі асоціації діють як саморегульовані організації, самостійно розробляючи правила поведінки і дотримуючись їх [14]. Таким чином, обидві форми участі бізнесу в регулюванні найчастіше мають на увазі якусь залученість держави, нехай навіть на рівні надання підтримки без прямого втручання. Підтримка ініціатив бізнесу з саморегулювання і створення для нього сприятливих умов – один з необхідних компонентів створення довгострокових програм співробітництва держави і бізнесу.

Список використаних джерел:

1. BROUSSEAU, E. (2002), Internet Regulation: Does Self-Regulation Require an Institutional Framework, DRUID Summer Conference on «Industrial Dynamics of the New and Old Economy – who is embracing whom?» Copenhagen/Elsinore 6-8 June 2002, P. 1

2. GERCKE, M., TROPINA, T., LOZANOVA, Y. and SUND, C. (2011), The Role of ICT Regulation in Addressing Offences in Cyberspace. In: "Trends in Telecommunication Reform 2010/11. Enabling Tomorrow's Digital World". ITU, 2011.

3. THE WORLD BANK GROUP, (n/d), Global ICT Department. Cybersecurity: A New Model for Protecting the Network, <http://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/CyberSecurity.pdf>; BRUCE, R., at al, (2005), TNO Report. International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues <http://www.ists.dartmouth.edu/library/158.pdf>

4. VOGEL, J. 2007. Towards a Global Convention against Cybercrime. World Conference on Penal Law, Guadalajara, Mexico. <http://www.penal.org/IMG/Guadalajara-Vogel.pdf> , P. 5

5. LOVET, G. 2009. Fighting Cybercrime: Technical, Juridical and ethical Challenges. Virus Bulletin Conference. September, 2009. <http://www.fortiguard.com/sites/default/files/VB2009_Fighting_Cybercrime_-_Technical,Juridical_and_Ethical_Challenges.pdf >, P. 69

6. FAFINSKI, S., DUTTON, W. and MARGETTS, H. (2010), Mapping and Measuring Cybercrime, OII Forum Discussion Paper No 18, <http://www.law.leeds.ac.uk/assets/files/staff/FD18.pdf >, P. 19

7. MARSDEN C., at al. 2006. Options for an Effectiveness of Internet Self- and Co-Regulation. Phase 1 Report: Mapping Existing Co- and Self-Regulatory Institutions on the Internet. RAND Europe <http://ec.europa.eu/dgs/information_society/evaluation/data/pdf/studies/s2006_05/phase1. pdf>; SAHEL, J., (2006), A new policy-making paradigm for the Information Society, TPRC conference, 2006, <http://web.si.umich.edu/tprc/papers/2006/635/NewParadigmInfoSociety.pdf>.

8. SIEBER, U. 2008. Mastering Complexity in the Global Cyberspace: The Harmonization of Computer-Related Criminal Law. In: DELMAS-MARTY, M. / PIETH, M. / SIEBER, U. (ed(s).): Les chemins de l'Harmonisation Pénale/Harmonising Criminal Law, Collection de L'UMR de Droit Comparé de Paris, Bd. 15. Paris, Société de législation comparée, 2008, p. 127 – 202.

9. OECD, (2011), The Role of Internet Intermediaries in Advancing Public Policy Objectives. OECD Publishing, P. 196

10. SENDEN, L., (2005), Soft Law, Self-Regulation and Co-Regulation in European Law: Where Do They Meet?, in "Electronic Journal of Comparative Law", vol, 9.1 (January 2005), P. 12

11. BARTLE I. and VASS P., (2007), Self-Regulation and the Regulatory State: A Survey of Policy and Practice, in „Public Administration", Volume 85, Issue 4, December 2007.

12. KOOP, B. J., (2010), Cybercrime Legislation in the Netherlands, in "Electronic Journal of Comparative Law", vol. 14.3 (December 2010), <http://www.ejcl.org>

13. BARTLE I. and VASS P., (2007), Self-Regulation and the Regulatory State: A Survey of Policy and Practice, in „Public Administration", Volume 85, Issue 4, December 2007.

14. BRUNST, P., and SIEBER, U. Cybercrime Legislation in Germany, in: BASEDOW/ KISCHEL/ SIEBER (eds.), German National Reports to the XVIII. International Congress of Comparative Law, pp. 711 – 800. Mohr-Siebeck, Tübingen 2010; MARSDEN C., at al. 2006. Options for an Effectiveness of Internet Self- and Co Regulation. Phase 1 Report: Mapping Existing Co- and Self-Regulatory Institutions on the Internet. RAND Europe, <http://ec.europa.eu/dgs/information_society/evaluation/data/pdf/studies/s2006_05/phase1.pdf>