Сергій Буяджа
Президент благодійного фонду «Ангели Доброти», Україна

ПОЗИТИВНИЙ ДОСВІД ПРАВОВОГО РЕГУЛЮВАННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В КРАЇНАХ ЄС

Serhii Buiadzha
President of the Charity Foundation "Angels of Kindness", Ukraine

POSITIVE EXPERIENCE OF LEGAL REGULATION OF THE FIGHT AGAINST CYBERCRIME IN EU COUNTRIES

The article outlines peculiarities of legal regulation of the fight against cybercrime in the EU countries. The positive experience of the European Union in Ukraine may be borrowed by the following ways: the evolution of domestic legislation in accordance with European standards; expansion of the activities of European international organizations to combat cybercrime on the Ukrainian territory; specification of the concept of "cybercrime" in domestic legislation through the norms of European legislation. The legal regulation of the fight against cybercrime in France was analyzed and the following ways of borrowing positive experience in Ukraine were identified: the requirement for authoring websites was set; establishment of cooperation between law enforcement agencies and Internet service providers in order to respond promptly to emerging threats; establishment of a bilateral dialogue with citizens; establishing a course for free cooperation with other states.
Keywords: legal regulation, fight against cybercrime, cyber security, legislation, EU, copyright.

Одним з пріоритетних напрямків вдосконалення вітчизняної правової системи є впровадження міжнародних концепцій, принципів і ідей. В умовах євроінтеграційних процесів важлива заміна застарілих способів і методів у регулюванні суспільних відносин і виконання конкретних вимог, поставлених перед Україною. Актуальність дослідження закордонного досвіду функціонування системи правового регулювання боротьби з кіберзлочинністю обумовлена загостренням ситуації зі збільшенням обсягів злочинної діяльності в кібермережах і відсутністю у нашій державі розвиненості в даній сфері. Масштаби мережі Інтернет свідчать про те, що окремі елементи кіберзлочинності не можуть обмежуватися територією цієї держави, тому в будь-якому випадку національне законодавство повинно відповідати загальноприйнятим стандартам у цій сфері для можливості здійснювати міжнародне співробітництво. Более того, процесс становления системы правового регулирования боротьби з кіберзлочинністю неможливо без урахування досягнень і помилок, які допущені іноземними державами при формуванні даного інституту.

Окремі проблеми правового регулювання боротьби з кіберзлочинністю в країнах ЄС розглядалися такими дослідниками, як Г. А. Калюжний, В. В. Коваленко, Я. Ю. Кондратьєв, Б. А. Кормич, В. В. Марков, А. І. Марущак, Г. В. Новицький, А. Л. Осипенко, Т. Л. Сироєдов, Р. Ю. Сень та ін. Проте, питання особливостей правового регулювання боротьби з кіберзлочинністю в країнах ЄС вимагає більш комплексного підходу, і обумовлює актуальність обраної теми дослідження.

Правове регулювання боротьби з кіберзлочинністю в Європейському Союзі характеризується наступними ознаками: 1) наявність як національного, так і міжнародного законодавства про боротьбу з кіберзлочинністю; 2) діяльність щодо протидії кіберзлочинності здійснюється одночасно національними та міжнародними організаціями, які сформовані з найкращих фахівців країн-учасниць; 3) важлива роль відводиться теоретичним питанням: експертна оцінка кіберзлочинів, розробка передових методів профілактики і розслідування тощо; 4) здійснення активного інформаційного обміну.

Отже, серед шляхів запозичення позитивного досвіду Європейського Союзу в Україні є наступні:

1) еволюція вітчизняного законодавства відповідно до європейських стандартів.

Варто відзначити, про активну діяльність України щодо розробки нормативно-правового регулювання з питань боротьби з кіберзлочинністю. Головний нормативно-правовий акт у цій сфері, Конвенція про кіберзлочинність, ратифікований нашою державою, відбувається оперативне реагування на вказівки Ради Європи по еволюції вітчизняного законодавства у всіх сферах. Тому єдиним вірним напрямком з реалізації даного вектора запозичення досвіду є подальше втілення в вітчизняне законодавство європейських стандартів та імплементація європейських програм розвитку даного інституту у вітчизняні стратегії. Іншими словами, євроінтеграція України можлива тільки за умови відповідності норм вітчизняного законодавства до європейських стандартів. Втілення цього напрямку можливе в першу чергу шляхом ратифікації або запозичення досвіду. У будь-якому випадку, вимоги ЄС повинні виконуватися вітчизняним законодавцем, тому звернення до європейського законодавства є безперечною необхідністю.

2) поширення діяльності європейських міжнародних організацій з боротьби з кіберзлочинністю на українську територію.

Пріоритетним напрямком реалізації даного вектора є продовження співпраці з Європейським Союзом і подальше входження в цю організацію. Однак, такий шлях ретроспективний і не в повній мірі залежить від України. Тому, на даному етапі більш важливо укладення двосторонніх або багатосторонніх угод про співпрацю з такими організаціями, як Комп'ютерна група швидкого реагування (CERT – Computer Emergency Response Team), Європейський центр з боротьби з кіберзлочинністю (European Cybercrime Centre) і Європейське агентство з питань мережевої та інформаційної безпеки (European Network and Information Security Agency – ENISA), обміном інформацією і правовою допомогою, даними оперативно-розшукового характеру, прийняттям співробітників правоохоронних органів іноземних держав в Україні і т.д. Оскільки негайне входження в європейське співтовариство поки неможливе, доцільним є поступове підвищення участі та ролі нашої держави в міжнародних процесах з боротьби з кіберзлочинністю.

3) конкретизувати поняття «кіберзлочинність» у вітчизняному законодавстві за допомогою норм європейського законодавства. Беручи Закон України «Про боротьбу з кіберзлочинністю», який покликаний систематизувати всі ключові поняття досліджуваного інституту, слід здійснити роз'яснення того, які саме групи злочинів віднесено до категорії кіберзлочинів. Тому пропонується регламентувати норму в наступному вигляді – «Стаття 1. Основні поняття. ... традиційні форми кіберзлочинності, – які здійснюються у світовому чи регіональному масштабі кіберзлочинцями, суспільно небезпечні діяння, пов'язані з шахрайством і підробкою в електронних комунікаційних мережах та інформаційних системах; публікація протизаконного контенту в електронних медіа – здійснювані в кіберпросторі суспільно небезпечні діяння, пов'язані з розповсюдженням дитячої порнографії, матеріалів із закликами до расової ненависті і т.п.; специфічні злочини в електронних мережах – здійснювані у світовому чи регіональному масштабі кіберзлочинцями або їх угрупованнями, в тому числі за підтримки державних органів окремих держав, суспільно небезпечні діяння, пов'язані з атаками на інформаційні системи, хакерство та ін.

Отже, в контексті курсу України до євроінтеграції, дослідження особливостей правового регулювання боротьби з кіберзлочинністю в Європейському Союзі показало необхідність постійної співпраці нашої держави з іншими країнами. Фундаментальне значення в протидії кіберзлочинності в європейських державах має єдність і взаємодія, що відображається в залученні кращих фахівців кожної з країн-учасниць в глобальні процеси. Тому, з метою участі, сприяння та обміну досвідом і знаннями для України доцільно якомога швидше залучення до таких процесів.

Крім дослідження досвіду всієї європейської спільноти, доцільно проаналізувати практики провідних держав Союзу. Почнемо з аналізу правового регулювання боротьби з кіберзлочинністю у Франції, оскільки ця держава одна з перших в Європі, що вжила заходів до посилення ролі держави в регулюванні кіберпростору. Так, сьогодні в даній державі виділено такі форми кіберзлочинності: 1) суспільно небезпечні діяння, пов'язані з незаконним тиражуванням комп'ютерного програмного забезпечення, незаконним втручанням в автоматизовані системи обробки даних, вторгненням на сайти, створенням і розповсюдженням шкідливих програм тощо; 2) поширення сайтів, пов'язаних з дитячою порнографією, збутом наркотиків, расистської, ксенофобської або антисемітської спрямованості, терористичної спрямованості, про замахи

на приватне життя, з інструкціями по експлуатації вибухових речовин, реклами в шахрайських цілях і т.д.[1]. Даний досвід є актуальним для втілення в Україні, з огляду на недосконалість розуміння і формулювання сутності поняття «кіберзлочинність». Крім того, важливо чіткий розподіл проступків за ступенем впливу на суспільні процеси в державі і негативними наслідками. Якщо регулювання першої форми кіберзлочинності за Французькою класифікацією здійснюється в Україні на достатньому рівні Розділом XVI Кримінального кодексу України[2], то досвід регулювання другої форми кіберзлочинів доцільне для детального аналізу.

Вже сьогодні у Франції діють спеціальні закони, що забороняють публікацію матеріалів, що містять нацистську символіку, яка підтримує ідеї нацизму[3]. Дане питання є актуальним для Франції в силу багатонаціональності даної держави, проте останнім часом в силу інформаційної війни, спрямованої проти України, актуалізувалося і в наших умовах. Схожий нормативно-правовий акт був прийнятий і в Україні, однак на 15 років пізніше. Так, 09.04.2015 року датовано прийняття Закону України «Про засудження комуністичного і націонал-соціалістичного (нацистського) тоталітарних режимів в Україні і заборона пропаганди їх символіки» № 317-VIII[4]. Однак, відзначимо, що в нашій державі норми цього Закону не містять прямих вказівок на віднесення такої негативної діяльності до кіберзлочинів, обмежуючись формулюванням «поширення інформації», чого недостатньо для формування розуміння пропаганди такої символіки в мережі Інтернет як кіберзлочини.

Також привертає увагу французький Закон про обов'язкову реєстрацію власників сайтів країни і про кримінальну відповідальність провайдерів за надання хостингу ідентифікованим користувачам. Ще одним цікавим моментом даного нормативно-правового акту є встановлення вимоги до провайдерів про надання відомостей про авторів сайтів будь-яким третім особам, за порушення якої передбачена кримінальна відповідальність. Також даний вид відповідальності передбачений за надання неповних або недостовірних відомостей авторами французьких сайтів і за надання провайдерами місця на сервері ідентифікованим користувачам. Причому, по всіх сайтах, авторство яких не встановлено, відповідальність несе провайдер, а можливою мірою покарання є позбавлення волі терміном на півроку[5]. Будь-яка державна діяльність по встановленню контролю за громадянами апріорі є негативною, тому такий напрямок розвитку вітчизняного законодавства щодо боротьби з кіберзлочинністю не вважаємо першочерговим. Однак, з огляду на останні тенденції розвитку вітчизняного законодавства, питання встановлення відповідальності за порушення правил авторизації в кібермережах рано чи пізно виявляться на порядку денному вітчизняного законодавця. При таких умовах доцільним буде аналіз досвіду більш розвинених держав і законодавство Франції є одним з першочергових для вивчення в даному контексті.

У сфері активної боротьби з кіберзлочинністю 14 лютого 2008 року було прийнято французьку Стратегію по боротьбі з кіберзлочинністю, метою якої є співпраця між приватним бізнесом (постачальниками інформаційно-телекомунікаційних послуг) і правоохоронними органами з обміну інформацією і питаннях об'єднання зусиль в боротьбі з кіберзлочинністю. Цікавими моментами Стратегії є курс на встановлення співробітництва провайдерів і поліції і жандармерії, і створення національної комісії з професійної етики зі зв'язків з громадськістю[6]. Особливо доцільним вбачається останній напрям. Будь-яке обмеження прав і свобод громадян вимагає

[1] Бутузов, В.М. (2008). Міжнародний досвід: ініціатива правоохоронних органів Франції з протидії комп'ютерній злочинності. *Боротьба з організованою злочинністю і корупцією (теорія і практика), вип. 19,* 241.

[2] *Кримінальний кодекс України 2001* (Верховна Рада України). *Відомості Верховної Ради України, 25-26,* 131.

[3] Курицкий, А.Ю. (2000). *Интернет-экономика: закономерности формирования и функционирования.* Санкт-Петербург: издательство С.-Петербургского университета, 88.

[4] *Закон про засудження комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів в Україні та заборону пропаганди їхньої символіки 2015* (Верховна Рада України). *Відомості Верховної Ради, 26,* 219.

[5] Савчук, Н.В. (2012). Світовий досвід державного регулювання ринку інтернет–послуг. *Формування ринкових відносин в Україні, 4,* 26.

[6] Бутузов, В.М. (2008). Міжнародний досвід: ініціатива правоохоронних органів Франції з протидії комп'ютерній злочинності. *Боротьба з організованою злочинністю і корупцією (теорія і практика), вип. 19,* 242.

належного роз'яснення і двостороннього конструктивного діалогу з громадянами. Для цього у Франції крім намірів створити спеціальну комісію здійснюються й інші дії. Відмітимо відкриття сайту Хартії Інтернету (Charte de'Internet), на якому визначені принципи добровільних обов'язків користувачів і постачальників Інтернет-послуг. Ще одним подібним напрямом є створення Інтернет-ресурсу Mineurs.org, на якому викладена інформація про проекти в сфері безпечного користування кібермережами. Користувачі можуть отримувати консультації про протистояння кіберзагрозам і потенційно загрозливого змісту мережі[1]. Такий досвід є безумовно позитивним, адже знайомлячись з правилами користування Інтернетом, суб'єкти суспільних відносин в даній сфері фактично надають згоду на дотримання цих правил. Крім того, важливі роз'яснення, надані з боку держави щодо обмеження прав громадян. Однією з проблем України у всіх сферах є фактична відсутність суспільного діалогу з державною владою. Всі ключові рішення приймаються без урахування громадської думки та належного подальшого роз'яснення прийнятих норм. Тому в даному контексті звернення до досвіду Франції було б доцільним.

Щодо напрямків співпраці з іншими державами, особливо відзначимо положення Закону про внутрішню безпеку 2003 року, який дозволяє проводити обшуки в інформаційній мережі, якщо інформаційні системи розташовуються на території держави. Тобто, шляхом укладення угод у Франції передбачена можливість надання дозволу проводити віддалений обшук інформаційних ресурсів, без отримання попереднього дозволу країни, де розміщений сервер[2]. У даній роботі до перспектив розвитку правового регулювання боротьби з кіберзлочинністю нами було віднесено потенційну необхідність скасування державних кордонів в питаннях боротьби з кіберзлочинністю. Для втілення цього напряму в Україні доцільно вивчення досвіду Франції, оскільки можливість такої «вільної» співпраці чинним законодавством України не передбачено.

Отже, особливостями правового регулювання боротьби з кіберзлочинністю у Франції є: 1) істотна роль держави в регулюванні суспільних відносин в Інтернеті; 2) контроль за користувачами шляхом встановлення вимоги до авторизації авторів веб-сайтів; 3) налагодження співпраці правоохоронних органів та Інтернет-провайдерів з метою оперативного реагування на виникнення загроз; 4) наявність двостороннього діалогу з громадянами та належне роз'яснення їх прав і обов'язків як користувачів Інтернету, надання інструкцій; 5) встановлення курсу на вільне співробітництво з іншими державами шляхом надання доступу до власних кібермереж в разі вчинення на території Франції кіберзлочинів.

Практично кожна з обраних характеристик була б доцільною для втілення в сучасних українських реаліях. Тому, аналіз правового регулювання боротьби з кіберзлочинністю в Франції дозволяє виділити наступні шляхи запозичення позитивного досвіду в Україні:

1) встановлення вимоги авторизації авторів веб-сайтів.

Використовуючи досвід Франції, по-перше, доцільним було б ухвалення Закону України «Про обов'язкову реєстрацію власників сайтів». В такому нормативно-правовому акті слід передбачити наступні положення:

– створити єдиний загальнодержавний реєстр власників сайтів;

– встановити обов'язок провайдерів реєструвати відомості про авторів сайтів;

– надати такій інформації статус публічної;

– передбачити обов'язок надання Інтернет-провайдерами інформації про авторів сайтів під час вступу таких запитів. По-друге, варто доповнити Розділ XVI Кримінального кодексу України наступними статтями:

– «Порушення в сфері надання Інтернет-провайдерами хостингу не ідентифікованих користувачів. 1. Надання Інтернет-провайдерами хостингу не ідентифікованих користувачів, – карається штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до 6 місяців. 2. Дії, передбачені частиною першою цієї статті, вчинені повторно або за попередньою змовою, або якщо вони заподіяли істотну шкоду, – караються позбавленням волі на строк до одного року»;

[1] Савчук, Н.В. (2012). Світовий досвід державного регулювання ринку інтернет–послуг. *Формування ринкових відносин в Україні, 4,* 26.

[2] Бутузов, В.М. (2008). Міжнародний досвід: ініціатива правоохоронних органів Франції з протидії комп'ютерній злочинності. *Боротьба з організованою злочинністю і корупцією (теорія і практика), вип. 19,* 242.

– «Порушення в сфері ненадання Інтернет-провайдерами відомостей про авторів сайтів у відповідь на запит. 1. Ненадання Інтернет-провайдерами відомостей про авторів сайтів у відповідь на запит, що надійшов – карається штрафом до п'ятисот неоподатковуваних мінімумів доходів ... 3. Дії, передбачені частиною першою цієї статті, вчинені повторно або за попередньою змовою, або якщо вони заподіяли значну шкоду, – караються штрафом до тисячі неоподатковуваних мінімумів доходів або позбавленням волі на строк до одного року »;

– «Надання неповних або недостовірних відомостей авторами сайтів, або надання провайдерами місця на сервері ідентифікованим користувачам. 1. Надання неповних або недостовірних відомостей авторами французьких сайтів, або надання провайдерами місця на сервері ідентифікованим користувачам, – карається штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до 6 місяців. 2. Дії, передбачені частиною першою цієї статті, вчинені повторно або за попередньою змовою, або якщо вони заподіяли істотну шкоду, – караються позбавленням волі на строк до одного року».

2) налагодження співпраці правоохоронних органів та Інтернет-провайдерів з метою оперативного реагування на виникнення загроз.

Для реалізації цього напрямку варто, по-перше, в запропонованому Законі України «Про обов'язкову реєстрацію власників сайтів» передбачити норму, яка зобов'язувала б Інтернет-провайдерів максимально оперативно надавати правоохоронним органам відповіді на запити про авторів сайтів і підозрюваних у вчиненні кіберзлочинів. По-друге, в розділі XVI Кримінального кодексу України[1] запропоновану статтю «Порушення в сфері ненадання Інтернет-провайдерами відомостей про авторів сайтів у відповідь на запит» доцільно доповнити частиною 2: «2. Ненадання Інтернет-провайдерами відомостей у відповідь на запит правоохоронних органів, – карається позбавленням волі на строк до шести місяців».

3) налагодження двостороннього діалогу з громадянами.

Використовуючи досвід Франції запропоновано створити спеціальні Інтернет-ресурси, обов'язковими умовами яких будуть:

– роз'яснення користувачам Інтернету їх прав і обов'язків;

– тлумачення норм законодавства та причин обмеження прав і свобод громадян;

– надання консультацій за отриманими запитами;

– своєчасно інформувати громадян про проекти, які розробляються.

4) встановлення курсу на вільне співробітництво з іншими державами.

У випадку здійснення на території України кіберзлочинів, наслідки яких були негативними для інших держав, запропоновано надавати без запиту доступу до власних кібермереж державам, з якими Україна підписала двосторонні договори про співробітництво в сфері боротьби з кіберзлочинністю. Для цього, по-перше, потрібно укласти відповідні угоди або внести зміни в уже укладені. По-друге, доповнити статтю 8 Закону України «Про основи національної безпеки України» від 19.06.2003 № 964-IV[2] наступним чином «Основними напрямами державної політики з питань національної безпеки України є: у зовнішньополітичній сфері – проведення активної міжнародної політики України з метою ... поглиблення співробітництва із закордонними державами в сфері боротьби з кіберзлочинністю ...; в сфері державної безпеки ... участь України в міжнародному співробітництві у сфері боротьби з кіберзлочинністю».

Таким чином, Франція – вдалий приклад для запозичення позитивного досвіду в Україні. По-перше, ця держава в порівнянні з іншими країнами Європейського Союзу характеризується жорсткими підходами до встановлення контролю в кіберпросторі. Тому, в контексті нещодавніх змін до вітчизняного законодавства, доцільно звернення до досвіду країн, в яких подібні обмеження прав і свобод громадян були успішно реалізовані. По-друге, Франція є зразком з укладання двосторонніх відносин на рівнях «держава – держава», «держава-громадянин», «держава – приватний сектор економіки». З огляду на загальну незадоволеність громадян України реформами, що відбуваються в нашій державі і недостатність гласності в діях суб'єктів державної влади, досвід Франції є безумовно корисним для втілення в наших реаліях.

[1] *Кримінальний кодекс України 2001* (Верховна Рада України). *Відомості Верховної Ради України, 25-26,* 131.
[2] *Закон про основи національної безпеки України 2003* (Верховна Рада України). *Відомості Верховної Ради України, 39*, 351.

References:

1. Butuzov, V.M. (2008). Mizhnarodnyi dosvid: initsiatyva pravookhoronnykh orhaniv Frantsii z protydii kompiuternii zlochynnosti [The International experience: the initiative of French law enforcement agencies on counteraction of computer criminality]. *Borotba z orhanizovanoiu zlochynnistiu i koruptsiieiu (teoriia i praktyka)* [Combating organized criminality and corruption (theory and practice)], *vyp. 19,* 240-246. [in Ukrainian].
2. *Zakon pro zasudzhennia komunistychnoho ta natsional-sotsialistychnoho (natsystskoho) totalitarnykh rezhymiv v Ukraini ta zaboronu propahandy yikhnoi symvoliky 2015* [The Act on condemnation of communist and national-socialist (natsist) totalitarian regime in Ukraine and proscription of propaganda of their symbolism 2015] (The Verkhovna Rada of Ukraine). *Vidomosti Verkhovnoi Rady* [Official Bulletin of the Verkhovna Rada of Ukraine], 26, 219. [in Ukrainian].
3. Zakon pro osnovy natsionalnoi bezpeky Ukrainy 2003 [The Act on fundementals of national security of Ukraine 2003] (The Verkhovna Rada of Ukraine). *Vidomosti Verkhovnoi Rady Ukrainy* [Official Bulletin of the Verkhovna Rada of Ukraine]*, 39, 351.* [in Ukrainian].
4. Konventsiia pro kiberzlochynnist 2001. [The Convention on cyber criminality 2001]. Ofitsiinyi visnyk Ukrainy,[The official bulletin of Ukraine] *65, stor. 107, stattia 2535.* [in Ukrainian].
5. Kryminalnyi kodeks Ukrainy 2001 [The Criminal Code of Ukraine 2001] (Verkhovna Rada of Ukraine). *Vidomosti Verkhovnoi Rady Ukrainy* [The News of the Verkhovna Rada of Ukraine]*, 25-26,* 131. [in Ukrainian].
6. Kurickij, A.Ju. (2000). *Internet-jekonomika: zakonomernosti formirovanija i funkcionirovanija* [Internet-economy: the regularities of the formation and functioning]. *S*aint Petersburg: izdatel'stvo S.-Peterburgskogo universiteta. [in Russian].
7. Savchuk, N.V. (2012). Svitovyi dosvid derzhavnoho rehuliuvannia rynku internet–posluh [The World experience of state regulation of the market of Internet-services]. *Formuvannia rynkovykh vidnosyn v Ukraini* [The formation of market relations in Ukraine]*, no. 4,* 24-28. [in Ukrainian].