Межі юрисдикції держави в протидії кіберзлочинності

Олена Орленко

Відділ кримінального права, кримінології та судоустрою, Інститут держави і права ім. В.М. Корецького, УКРАЇНА, м. Київ, вул.Трьохсвятительська, 4,
E-mail: olena.orlenko@gmail.com

The Article deals with one of the aspects of the problem of cybercrime, in particular with one of the problems of its counteraction, as well as detremination of the boundaries of intervention of a state in the counteraction of cybercrime.

Ключові слова – інформація, телекомунікації, кіберзлочин, кіберзлочинність, кіберправо.

Всі ми в побуті не раз зіштовхувались із тими чи іншими проявами кіберзлочинності. Хакер зламав електронну поштову скриньку, пограбовано банк, вкрадено інформацію з податкової щодо банківських рахунків мільйонів осіб. Як вберегти себе від подібних злочинів - це справа не одного індивіда, адже часом кіберзлочинність набирає таких погрозливих форм, що самотужки з нею не впоратись. Радше, це справа держави, і певно, навіть не однієї держави, а всього міжнародного співтовариства, адже кіберзлочинність є глобальним соціальним явищем.

Двадцяте та двадцять перше століття, що характеризується зростанням застосування телекомунікаційних технологій, істотно підірвало деякі з презумцій, на яких базувалась традиційна модель юрисдикції. Зокрема, стало легше для будь-кого вчинити злочин в одній країні, та швидко залишити її межі, таким чином підриваючи здатність держави застосувати санкції до правопорушника. Винайдення Інтернету зробило можливим для громадянина, наприклад, країни А вчинення злочину проти громадянина, що знаходиться в країні В, без фізичної присутності на території цієї країни В.

В праві Сполучених Штатів Америка поняття «юрисдикція» визначено як «здатність держави приймати закони, чинити правосуддя та здійснювати примусовий вплив» [1] Традиційно, всі три типи юрисдикції грунтуються на концепції території. Держава має здатність приписувати, що є законною або незаконною поведінкою в межах своєї території та здатність застосовувати примусовий вплив на суб'єктів, чиє правопорушення мало місце на її території. Ця концепція «юрисдикції» випливає з основного положення про те, що суверенне утворення має верховну владу в межах своєї території, що включає в себе владу здійснювати контроль над своєю територією та владу застосовувати там закони. [2]

Яке відношення має ця концепція юрисдикції до кіберзлочинності? Відомо, що з питання кіберзлочиності в рамках Ради Європи 23 листопада 2001 року було прийнято Конвенцію щодо запобігання кіберзлочинності, відому ще як «Будапештська конвенція», яка набрала чинності 1 липня 2004 року. Стаття 22 Конвенції врегульовує питання підсудності юрисдикції держави за

скоєння кіберзлочину, закріплюючи, що кожна держава вживає таких законодавчих та інших заходів з метою встановлення підсудності щодо будь-якого кіберзлочину, вчиненого: а) в межах її території; б) на судні, що несе прапор цієї держави; в) на борту літака під прапором цієї держави; г) вчинене одним з її громадян, якщо за це правопорушення передбачено покарання правом держави, де його було вчинено; або якщо правопорушення не підпадає під територіальну юрисдикцію жодної держави. [3]

Отже, як вбачається з пункту С статті 22 Конвенції, після території, громадянство правопорушника є другою суттєвою підставою юрисдикції щодо кіберзлочину. Законодавство Німеччини має схоже положення: держава має юрисдикцію щодо злочину, вчиненого за її межами громадянином Німеччини, якщо його діяння там криміналізовано. [4] В Нідерландах передбачено ряд спеціальних положень щодо підсудності громадянина цієї держави за скоєння кіберзлочину. Зокрема, підробка, включаючи комп'ютерну підробку, вчинена за кордоном державними службовцями Нідерландів або службовцями міжнародних організацій, що розташовані в Нідерландах, переслідується в Нідерландах, якщо злочин криміналізовано в державі, де його було вчинено. Також, підлягає переслідуванню за законодавством Нідерландів публікація конфіденційної інформації, що була отримана з доступом до комп'ютера громадянином Нідерландів. Нарешті, переслідується в Нідерландах й розповсюдження дитячої порнографії, якщо скоєне громадянином цієї держави. [5]

Існують також й інші підстави для визначення підсудності юрисдикції держави кіберзлочинця, це зокрема, місце знаходження комп'ютеру – знаряддя злочину.

Висновок

Отже, в даній статті ми визначили, що є підставами для визначення підсудності юрисдикції держави у випадку скоєння кіберзлочину.

Література

1. Restatement of Foreign Relations Law of the United States (1987), § 401.
2. Конституція України від 28 червня 1996 року, статті 1, 2, 5 та 8.
3. Convention on Cybercrime, 23. XI.2001, European Treaty Series, No. 185, p.13.
4. Strafgezetsbuch § 7 Nr (2) (1).
5. Wetboek van Strafrecht, art. 4 (11), 5 (1) (1), 5 (1) (3).