

Карчевський Микола Віталійович,
перший проректор Луганського
державного університету внутрішніх
справ імені Е. О. Дідоренка, доктор
юридичних наук, професор

КЛЮЧОВІ ПОЛОЖЕННЯ ЩОДО ВДОСКОНАЛЕННЯ КРИМІНАЛЬНО-ПРАВОВОГО РЕГУЛЮВАННЯ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Найбільш помітні соціальні зміни пов'язані з інформатизацією. Розвиток і розширення сфери застосування інформаційних технологій (ІТ) обумовили, серед іншого, істотні трансформації кримінально-правового регулювання. Результатом удосконалення кримінального законодавства про посягання у сфері інформаційної безпеки має стати чітке визначення кола діянь, що треба відносити до кримінальних правопорушень. На нашу думку, специфічною вимогою до цих положень кримінального законодавства має бути технологічна нейтральність, що водночас здатна забезпечити стабільність законодавства в сучасних умовах постійних змін технологій. Спробуємо сформулювати ключові положення для розв'язання цієї проблеми.

1. Інформаційна безпека – система суспільних відносин щодо реалізації інформаційної потреби особи, суспільства, держави. Названа система має три складники: відносини у сфері використання ІТ, відносини у сфері забезпечення доступу до інформації, відносини у сфері формування інформаційного ресурсу.

2. Головна проблема кримінально-правового регулювання у сфері використання ІТ полягає у відсутності чітких критеріїв суспільної небезпеки на рівні законодавчих визначень. Через це у сфері дії кримінальної юстиції опиняються не тільки діяння, що здійснює суспільно небезпечними, але й ті, які такими не є. Ефективність протидії кіберзлочинності зменшується. Кількісна оцінка ефективності кримінально-правового регулювання може бути здійснена в спосіб аналізу динаміки облікованих кримінальних правопорушень у сфері використання ІТ (ст. 361–363-1 КК України) та засуджених за такі правопорушення осіб у контексті даних щодо проникнення Інтернету¹. Протягом

¹ Цей показник є одним з універсальних маркерів інформатизації, обчислюється у відсотках та являє собою частку населення країни, яка користується Інтернетом.

2013–2019 років спостерігалось зростання аудиторії Інтернету з 53 % до 71 % з одночасним майже чотириразовим(!) збільшенням зростання кількості облікованих правопорушень (з 595 до 2204), що цілком природно, оскільки чим більше людей використовує сучасні інформаційні технології, тим більше «комп'ютерних» злочинів може бути вчинено. Але водночас із зростанням кількості облікованих правопорушень, кількість обвинувальних вироків залишилася на рівні 2013 року (49 – 2013 рік, 50 – 2019). Можна твердити про рівень матеріально-технічного та кадрового забезпечення розслідування, брати до уваги необхідність спеціальних знань у судів та прокурорів тощо. Проте основна, фундаментальна причина ситуації, що склалась, саме у якості законодавства. На відміну від чинного кримінального законодавства, яке передбачає відповідальність за певні незаконні діяння з комп'ютерними даними, нове має передбачати відповідальність тільки тоді, коли такими діяннями заподіяно певну шкоду.

3. Проблеми кримінально-правового регулювання наступної групи відносин інформаційної безпеки – відносин у сфері забезпечення доступу до інформації – стосуються головно розбалансованості законодавства, існування численних конкурентних норм, надмірного рівня кількості кримінально-правових заборон у цій галузі. Необхідною є оптимізація означеної системи норм, заміна наявної розосередженої системи спеціальних кримінально-правових заборон такими, які б забезпечували регулювання більш широких сегментів інформаційної безпеки. Автор пропонує передбачити загальну норму про незаконне надання або отримання доступу до інформації з обмеженим доступом. До того ж критерієм відповідальності має бути не різновид інформації, а заподіяна шкода.

4. Основне питання кримінально-правового регулювання у сфері формування інформаційного ресурсу полягає в чіткому та послідовному визначенні межі можливостей ефективного впливу на суспільні відносини засобами кримінального права. Небезпеки інформаційних впливів і зловживань обговорюють досить активно в суспільно-політичному дискурсі, у науці. Багатомірність і масштабність шкоди від неконтрольованого інформаційного простору не викликає сумнівів. Водночас сумнівно, щоб розв'язання означених проблем через доповнення КК новими нормами було доцільним. Неодноразово пропонувалося встановлювати покарання за різноманітні форми маніпуляції суспільною свідомістю. Такі пропозиції є спірними через

прогнозовану неефективність і декларативність, їх невідповідність принципам кримінально-політичної адекватності, а також співрозмірності позитивних і негативних наслідків криміналізації. Окрім того, поширення глобальних інформаційних технологій загалом робить методи обмеження або заборони контенту все менш ефективними. Разючим прикладом тут може слугувати відомий «ефект Стрейзанд». Розв'язання проблеми перебуває поза межами кримінально-правового регулювання і, на нашу думку, передбачає передусім системну роботу в галузі освіти та формування конкурентних інформаційних продуктів.

5. Стосовно згаданої на початку технологічної нейтральності кримінального законодавства. Промовистим прикладом тут є чинна редакція ч.3 ст. 190 КК. Наскільки справедливо розглядати шахрайство, вчинюване шляхом незаконних операцій з використанням електронно-обчислювальної техніки, як тяжке кримінальне правопорушення (санкція ч. 3 ст. 190 передбачає покарання до восьми (!) років позбавлення волі)? На момент внесення цієї норми до КК України (20 років тому) застосування комп'ютерної техніки для здійснення шахрайства справді могло свідчити про підвищену суспільну небезпеку посягання. Поширеність засобів електронної комерції, систем дистанційного банківського обслуговування була незначною. Користувалися ними великі суб'єкти господарювання. Тому положення ч. 3 ст. 190 КК доволі чітко окреслювали коло діянь, які обґрунтовано було розглядати як особливо кваліфікований вид шахрайства, близький за ступенем суспільної небезпеки до шахрайства у великих розмірах. Проте стрімкі темпи проникнення інформаційних технологій у фінансову сферу зумовили якісну зміну цього виду шахрайства. Правоохоронні органи фіксують відчутну кількість таких злочинів, пов'язаних із спричиненням шкоди, що відповідає ознакам простого або кваліфікованого шахрайства (ч. 1, ч. 2 ст. 190 КК). Чи можна вважати обґрунтованою, а саме цього вимагає тлумачення норми, кримінально-правову оцінку таких дій за ч. 3 ст. 190 КК? Питання радше риторичне. У сучасних умовах немає підстав стверджувати, що використання електронно-обчислювальної техніки в процесі здійснення шахрайства настільки підвищує рівень суспільної небезпеки вчиненого діяння.

Наведений приклад наочно демонструє тезу про те, що в умовах стрімкого розширення сфери застосування нових технологій, положення КК «зав'язані» на певні технологічні аспекти, будуть швидко втрачати актуальність. Набуватимуть характеру таких, які не передають об'єктивного рівня розвитку

суспільних відносин. Саме тому внесення до КК таких понять, як «штучний інтелект», «нейроінтерфейс», «нанотехнології», «генна інженерія» тощо має розглядатися критично.

6. Загальновідомо, що сферою широкого застосування комп'ютерної техніки є банківська діяльність та платіжні системи, тому велика частка злочинів проти власності істотно змінилась. Доволі дискусійним як для науковців, так і для практиків стало питання юридичного змісту таких категорій, як «безготівкові гроші», «електронні гроші», «криптовалюта». Названі проблемні питання мають знаходити розв'язання в межах дискурсу про кримінально-правове регулювання відносин власності.

Отже, для продовження дискусії щодо змісту обумовлених інформатизацією змін у сфері кримінально-правового регулювання сформулюємо такі положення:

- розпочалося та триває формування нового предмета кримінально-правового регулювання – інформаційна безпека;

- проблемами цього процесу є недостатність визначеності законів про кримінальну відповідальність за «комп'ютерні» злочини, потреба оптимізації системи кримінально-правового регулювання у сфері доступу до інформації, відсутність консенсусу в питанні меж кримінально-правового регулювання у сфері формування інформаційного простору;

- важливою засадою вдосконалення кримінального законодавства у сфері інформаційної безпеки має стати технологічна нейтральність, адже її дотримання дасть змогу забезпечити стабільність нового законодавства та, відповідно, сталий розвиток практики його застосування.

Катеринчук Катерина Володимирівна,
професор кафедри приватного
та публічного права навчально-
наукового інституту права та сучасних
технологій навчання Київського
національного університету технологій
та дизайну доктор юридичних наук,
доцент

ДЕФІНІЦІЯ «ШКОДА ЗДОРОВ'Ю ОСОБИ» В ПРОЄКТІ КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ

Суспільно небезпечні наслідки, що описані законодавцем у диспозиціях статей кримінальних правопорушень проти здоров'я особи у тому, що в них передбачено наслідки у вигляді