НАПРЯМ 9. ПУБЛІЧНЕ УПРАВЛІННЯ ТА АДМІНІСТРУВАННЯ

Кудрявський І.В.
докторант,
Міжрегіональна Академія управління персоналом

DOI: https://doi.org/10.36059/978-966-397-365-4-37

АНАЛІЗ ЕФЕКТИВНОСТІ МЕХАНІЗМІВ ДЕРЖАВНОГО РЕГУЛЮВАННЯ У СФЕРІ ЗАХИСТУ БЕЗПЕКИ ІНФОРМАЦІЙНОГО ПРОСТОРУ

Загалом, варто відзначити що в українській науці та законодавстві питання захисту прав та охоронюваних законом інтересів від правопорушень та злочинів, пов'язаних із використанням сучасних інформаційних технологій не нове, а його опрацювання має свої практичні результати. П.5 ст. 42-4, п. 5, 9 ст. 116-2, п. 5 ст. 186-3, ст. 188-31, ст. 212-6 та ст. 212-9 Кодексу України про адміністративні правопорушення [1], п. 1, 6 ст. 111, п. 1, 2 ст. 156-1, п. 1 ст. 301, п. 1, 2, 3 ст. 301-2, п. 2 ст. 321-1, ст. 361, п. 1 ст. 361-1, п. 1 ст. 376-1 Кримінального кодексу України [2] свідчать про те, що українські законодавці намагаються своєчасно криміналізувати суспільно-небезпечні дії, в ході яких використовуються інформаційно-телекомунікаційні технології. Передусім перераховані статті стосуються злочинів проти основ національної безпеки України та інших тяжких злочинів, зокрема злочинів сексуального характеру, вчинених проти неповнолітніх. Можна сперечатися щодо оцінки своєчасності та повноти даних положень Кримінального кодексу України та Кодексу України про адміністративні правопорушення, але однозначно можна зробити висновок, що робота щодо удосконалення питань державного управління інформаційними правовідносинами та діями в інформаційному просторі проводиться. Наявність відповідних положень у згаданих кодексах залучає достатньо

ефективні механізми профілактики злочинів та адміністративних правопорушень і покарання винних у них шляхом надання відповідних повноважень судам, правоохоронним органам, активізації інших традиційних правозастосовних механізмів. Однак, у цьому випадку законодавство врегульовує відповідні суспільні відносини не за критерієм їхнього відношення до інформаційного простору, а за критерієм застосування інформаційно-телекомунікаційних технологій в ході здійснення традиційних правопорушень, давно відомих у правозастосовній практиці, що безумовно ускладнює ідентифікацію принципово нових суспільно-небезпечних дій, вчинення яких пов'язане з деструктивним інформаційним впливом. Крім того, Кримінальний кодекс України та Кодекс України про адміністративні правопорушення в принципі не мають своїм основним призначенням захист національної безпеки України від зовнішніх загроз, хоча відповідні розділи згаданих документів і передбачають відповідальність за низку відповідних дій. Що ж до позитивного аспекту кримінальної та адміністративної відповідальності за злочинні (протиправні) дії в інформаційному просторі – варто відзначити їх достатньо високу стримуючу ефективність у якості механізмів державного управління. Поряд з тим своєчасна і точна криміналізація нових форм та видів злочинів, які здійснюються із застосуванням інформаційного простору, повинна відбуватися постійно, безперервно та з урахуванням майбутніх можливих загроз. Так, наприклад, за заявою представниці ювенальних прокурорів Департаменту захисту дітей Офісу Генерального прокурора Юлії Усенко, лише за перші два місяці 2021 року відбулися 18 самогубств та спроб їх вчинення дітьми у віці від 10 до 16 років. Причиною цих випадків стала участь у різноманітних «групах смерті» та «смертельних онлайн іграх» на кшталт широко відомого «Синього кита», де так звані «куратори» видавали потерпілим завдання, що прямо загрожували їхньому здоров'ю та життю [3].

Враховуючи складнощі єдиного наукового визначення інформаційного простору серед українських науковців та відсутність такого визначення в основних Законах України, які регулюють правовідносини у сфері наповнення інформаційного

простору [4; 5; 6; 7], звернемося до розуміння інформаційного простору західними дослідниками воєнно-політичної та воєнно-стратегічної сфери, що закріплене у низці документів НАТО та наказах окремих керівників складових Сил Оборони України. У згаданих джерелах інформаційний простір розглядається як середовище, що складається з самої інформації, людей, організацій та систем, які отримують, обробляють та передають інформацію, а також когнітивного, віртуального і фізичного вимірів, у яких це відбувається [8]. Дане визначення, спрямоване на воєнно-прикладне застосування механізмів управління інформаційним простором у сучасних умовах і, на думку автора, достатньо добре підходить для окреслення сфери функціонування механізмів державного управління наповненням інформаційного простору.

Важливою є акцентуація не лише на віртуальному вимірі інформаційного простору, яким більшість споживачів інформації звикли обмежуватися на побутовому рівні, але й наголошення на ефектах у когнітивному та фізичному вимірах. Якщо дії у фізичному вимірі інформаційного простору можуть бути небезпечні значною латентністю до виявлення цифровими засобами, більш досконалими сьогодні аніж аналогові, на основі давно відомих фізичних принципів, то постановка питання про когнітивний вимір інформаційного простору відкриває цілий пласт загроз: починаючи від деструктивної зміни світогляду чисельних спільнот шляхом надання дезінформації, і закінчуючи деструктивним психологічним впливом підсвідомого характеру, який часто не фіксується особистістю але може становити критичну небезпеку, аж до того що штовхати людину на вчинення злочину чи самогубство поза свідомим прийняттям рішення про такі дії.

Налагодити саму по собі фіксацію описаних дій та процесів в інформаційному просторі шляхом застосування механізмів державного управління – дуже непросте завдання. Поряд з тим існує необхідність не просто фіксувати, але й належним чином реагувати, а в окремих випадках – працювати на випередження та не допускати деструктивних дій в інформаційному просторі, які можуть становити загрозу правам та охоронюваним законом

інтересам, включаючи загрозу національній безпеці, життю та здоров'ю людей. Таке завдання явно не під силу окремим особистостям чи невеликим спільнотам і повинно виконуватися відповідними державними уповноваженими органами з дотриманням затверджених механізмів державного управління, які виключатимуть зловживання чи неправильне трактування положень керівних документів, але при цьому зможуть забезпечити ефективну протидію інформаційним загрозам та належну безпеку інформаційного простору.

Література:

1. Кодекс України про адміністративні правопорушення : Закон України від 14.12.2023 р. № 2982-IX. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/80731-10#Text (дата звернення: 10.03.2024).

2. Кримінальний кодекс України : Закон України від 01.01.2024 р. № 3513-IX. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 10.03.2024).

3. Підліток з Рівного порізав собі руки за невиконання завдань у смертельній грі – ЗМІ. *Укрінформ*. 2021. URL: https://www.ukrinform.ua/rubric-other_news/3196240-pidlitok-z-rivnogo-porizav-sobi-ruki-i-nogi-za-nevikonanna-zavdan-u-smertelnij-gri.html

4. Конституція України : Закон України від 1 січня 2020 р. № 27-IX. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 10.03.2024).

5. Про інформацію : Закон України від 21.03.2023 р. № 3005. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2657-12/print (дата звернення: 10.03.2024).

6. Про медіа : Закон України від 11.02.2024 р. № 3269-IX. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text (дата звернення: 10.03.2024).

7. Про Стратегію інформаційної безпеки : Указ Президента України від 28 грудня 2021 року № 685/2021. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/685/2021/print (дата звернення: 10.03.2024).

8. NATO standard AJP-3.10.1(A) Allied Joint Doctrine for psychological operations. October 2007. URL: https://info.publicintelligence.net/NATO-PSYOPS.pdf (дата звернення: 10.03.2024).