AMERICANBARASSOCIATION
Rule of Law Initiative

ПЛАТФОРМА ПРАВ ЛЮДИНИ

РЕКОМЕНДАЦІЇ

щодо покращення ситуації зі свободою вираження поглядів онлайн в контексті інтересів національної безпеки

ВСТУП

В червні 2020 року Американська асоціація юристів Ініціатива з верховенства права (ABA ROLI) в Україні видала *«Базовий документ з питань національної та кібербезпеки, інтернет-свободи та міжнародного права»*. Цей інформаційно-аналітичний продукт компактно підсумовує основні загрози інформаційному простору України з боку Російської Федерації, каталогізує сучасні підходи до допустимої та ефективної реакції держав на інформаційні та кіберзагрози.

Відміною рисою дослідження ABA ROLI є те, що в ньому бажаний стан законодавчого регулювання інтернет свобод та практика його реалізації розглядається крізь призму сучасних загроз національній безпеці України. Це робить дане дослідження не стільки теоретичним зрізом правової реальності, скільки корисним аналітичним посібником для формування пропорційної та виваженої політики України щодо кібербезпеки та забезпечення інтернет-свобод.

Базовий документ ABA ROLI складається з трьох основних субстантивних розділів, що присвячені наступним темам:

I. Огляду регіональної та національної панорами кібербезпеки у Європі та Євразії. Найбільший фокус тут зроблено на інформаційних загрозах, що походять від Російської Федерації. В цій частині сформульовані цілі РФ у її операціях інформаційного впливу, які полягають у: а) намаганні досягти конкретних тактичних результатів як то зняття санкцій чи псування відносин між ЄС та США, ЄС та Україною тощо та б), так і у спричинені ерозії довіри до влади, фактів, правди та науки. В цій ж частині запропоновано огляд підходів до вирішення проблеми інформаційної безпеки у країнах ЄС (створення спеціалізованих інституцій, законодавства щодо видалення ненависницьких повідомлень та фейкових новин в інтернеті, запуск неурядових ініціатив). Наостанок, представлено дослідження української реакції на кібер- та інформаційні загрози зі сторони Росії. Серед її недосконалостей відзначено: деяку непослідовність політики, непередбачуваність обмежувальних заходів, неналежне інституційне оформлення та сумнівну юридичну аргументацію відповіді України.
II. Міжнародному та українському національному правовому регулюванню свободи слова та, відповідно, свободи вираження поглядів в інтернеті. Розглянути як акти, що безпосередньо пов'язані зі зазначеними свободами, так і ті, що слугують тлом для їх застосування: міжнародні договори та закони України що визначають загальний пейзаж прав людини, акти, що стосуються відповідальності держав, норми міжнародного гуманітарного права, що встановлюють загальну рамку кібероперацій в рамках збройних конфліктів тощо. Запропонований до огляду також набір контрзаходів, що держави можуть застосовувати у випадку посягання на їх кібербезпеку з боку інших держав.
III. Компаративному огляду практики держав у їх реакціях на кіберзагрози та недружні кібероперації (поширення дезінформації). Окрім європейських держав, вивчено досвід деяких інших країн: Австралія, Індія, Пакистан, Сінгапур, США. Аналітику тут запропоновано у двох зручних для навігації форматах: табличному та описовому. Розглянуто законодавчі, інституційні та регуляторні механізми реагування на інформаційні загрози. Зокрема, Базовий документ у цій частині пропонує детальний опис використання журналістських стандартів, які підстави для вжиття штрафних заходів проти поширювачів дезінформації; громадський тиск через називання та осоромлення;

створення списків ресурсів, що поширюють неправдиву інформацію; фінансові та банківські обмеження, а також штрафи за порушення санкційного законодавства; урядові заходи з недопущення поширення ненависті; криміналізація навмисного надання неправдивої інформації чи навмисного інформаційного впливу на політичний ландшафт як форм іноземного втручання; законодавче регулювання заборони брехні та маніпуляцій в інтернеті тощо.

На основі коротко представленого тут матеріалу з Базового документу ABA ROLI експерти організації підготували рекомендації для українських органів влади. При виборі органів-адресатів цих рекомендацій, найпершими орієнтирами були:

- причетність до формування безпекової політики;
- причетність до формування політики у сфері культури;
- причетність до формування політики у сфері інформаційної безпеки;
- здійснення правоохоронної діяльності, у тому числі щодо правопорушень у сфері інтернет та спрямованих проти безпеки держави;
- наявність повноважень приймати регуляторні рішення щодо свободи вираження думки, свободи слова та інформації;
- здійснення узагальнення судової практики по питанням, що стосуються свободи слова та інформації.

Ґрунтуючись на зазначених вище характеристиках органів, були визначені наступні ключові адресати рекомендацій:

- Президент України
- Рада національної безпеки і оборони України
- Верховна Рада України
- Уповноважений Верховної Ради України з прав людини
- Служба безпеки України
- Міністерство оборони України
- Міністерство внутрішніх справ України
- Міністерство юстиції України
- Міністерство цифрової трансформації України
- Міністерство культури та інформаційної політики України
- Офіс Генерального прокурора України
- Верховний суд
- Державна служба спеціального зв’язку та захисту інформації України (ДССЗЗІ)

Далі наводяться рекомендації згруповані по кожному з цих органів.

*Американська асоціація юристів та партнерські організації готові надавати свою допомогу державним органам з метою покращення законодавчої бази в Україні, яка регулює та впливає на Інтернет Свободи в країні.

Київ, березень 2021 року

ПРЕЗИДЕНТ УКРАЇНИ (ОФІС ПРЕЗИДЕНТА УКРАЇНИ)

Відповідно до частини 1 статті 13 Закону України «Про національну безпеку України» керівництво у сферах національної безпеки і оборони відповідно до Конституції України здійснює Президент України, який: 1) забезпечує державну незалежність та національну безпеку; 2) є Верховним Головнокомандувачем Збройних Сил України, як Верховний Головнокомандувач видає накази і директиви з питань оборони; 3) очолює Раду національної безпеки і оборони України, вводить у встановленому порядку в дію її рішення; 4) видає укази і розпорядження з питань національної безпеки і оборони, які є обов'язковими до виконання на території України, зокрема указами Президента України затверджуються Стратегія національної безпеки України, Стратегія воєнної безпеки України, інші стратегії, доктрини, концепції, якими визначаються актуальні загрози національній безпеці, основні напрями і завдання державної політики у сферах національної безпеки і оборони, розвитку сектору безпеки і оборони; 5) реалізує право законодавчої ініціативи у Верховній Раді України щодо законодавчого врегулювання питань національної безпеки і оборони; 6) здійснює загальне керівництво розвідувальними органами України та здійснює інші повноваження, визначені Конституцією України.

Виходячи з повноважень у оборонній сфері та у сфері міжнародних відносин, Президент відіграє важливу роль у формуванні та реалізації політики інформаційної безпеки держави.

Рекомендується:

1. Забезпечити комплексний підхід у тісній співпраці з приватним сектором та громадянським суспільством до визначення основних засад формування державної політики у сфері інформаційної безпеки та кібербезпеки, створити реальні умови для забезпечення кіберзахисту інформаційної інфраструктури України. Зокрема, однією з першочергових задач у зазначених сферах є побудова ефективної структури та ієрархії відповідальних органів державної влади та посадових осіб, уникнення дублювання та чітке розмежування повноважень і завдань.
2. Ініціювати оновлення Доктрини інформаційної безпеки України від 25 лютого 2017 року та Стратегією кібербезпеки України від 15 березня 2016 року із врахуванням нової Стратегії національної безпеки України.
3. Разом з РНБО здійснювати постійний моніторинг виконання Стратегій у сфері національної безпеки та її інформаційних та кібер складових та забезпечити їх ефективну реалізацію.
4. Із врахуванням і на виконання Стратегій підтримувати існуючі проєкти законів та ініціювати власні у інформаційній та/або медійній сфері, яка має у 2021-му році містити інструменти та механізми відповіді на загрози та виклики національній безпеці, пов'язані зі збройною агресією і яка триває в Україні з 2014-го року. Адже, однією з основних складових зазначеної агресії є інформаційна, яка проявляється в різноманітних маніпуляціях та зловживаннях, в т.ч. за допомогою мережі Інтернет та засобів масової інформації. Зокрема, у Верховній Раді України зареєстровано Проєкт Закону «Про медіа», який містить розділ щодо обмежень у медійній сфері, пов'язаних зі збройною агресією і який в цілому отримав підтримку міжнародних організацій та багатьох посольств за умови його доопрацювання між першим та другим читанням. Будь-які механізми відповіді на загрози та виклики національній безпеці, пов'язані зі збройною агресією обов'язково мають містити запобіжники задля унеможливлення зловживання ними та відповідати міжнародним стандартам щодо можливих обмежень прав та свобод людини.
5. Із врахуванням і на виконання Стратегій ініціювати аналіз відповідними міністерствами та відомствами чинного законодавства щодо забезпечення кібербезпеки та ініціювати необхідні зміни, розробку нових проєктів законів або здійснити заходи для прискорення прийняття поточних проєктів НПА. Насамперед тих, які спрямовано на чітке визначення завдань, розмежування сфер відповідальності та врегулювання спільної діяльності суб'єктів у сфері інформаційної та кібербезпеки, а також власників (розпорядників) об'єктів критичної інформаційної інфраструктури. Також, потребують нормативно-правового визначення алгоритми інформаційного обміну між такими суб'єктами,

послідовність дій і розподіл їх функцій під час запобігання кібератакам та кіберінцидентам, їх виявлення та припинення, а також під час усунення їх наслідків. Так, прийнятий у 2017-му році Закон України «Про основні засади забезпечення кібербезпеки України» містить глосарій у зазначеній сфері, але в частині механізмів має загальний, рамковий характер, який без відповідних додаткових норм матиме і далі декларативний характер. Зокрема, на Кабінет Міністрів України згідно статті 5 зазначеного Закону покладено обов'язок сформувати вимоги та забезпечити функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури. Станом на кінець 2020-го року між установами тривало обговорення відповідного проєкту постанови КМУ, а НАЗК 02 жовтня 2020 р. надало висновок про наявність корупційних ризиків у ньому. Через чотири роки після прийняття зазначеного Закону України все ще потребує деталізації питання обсягу повноважень суб'єктів у сфері національної системи кібербезпеки, а також порядок їх взаємодії. Навіть нові нормативно-правові не додають ясності в цій частині. Так, для прикладу, Закон України «Про розвідку» в статтях 8 та 9 визначив, що сфера кібербезпеки в контексті розвідувальної діяльності є фокусі, як служби зовнішньої розвідки так і у розвідувального органу Міністерства оборони України.

6. Переглянути рішення про застосування санкцій у формі обмеження доступу користувачів до інформаційних ресурсів та привести їх у відповідність до Конституції та міжнародних зобов'язань України, зокрема:
    - Ініціювати зміни до законодавства, щоб гарантувати дотримання законності, обґрунтованості та пропорційності санкцій щодо інформаційних ресурсів та забезпечення незалежного судового контролю від зловживань;
    - Забезпечити ефективний діалог з експертами та правозахисниками щодо гарантування дотримання прав людини в ініціативах, спрямованих на протидію російській агресії;
    - Зобов'язати РНБО регулярно (щороку) здійснювати оцінку ефективності застосування санкцій з обов'язковим оприлюдненням результатів такого аналізу.

РАДА НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

Як зазначає стаття 1 Закону України «Про Раду національної безпеки і оборони України», РНБО відповідно до Конституції України є координаційним органом з питань національної безпеки і оборони при Президентові України. Стаття 3 того ж закону визначає функції Ради, що розділяються на три групи: 1) внесення пропозицій Президентові України щодо реалізації засад внутрішньої і зовнішньої політики у сфері національної безпеки і оборони; 2) координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони у мирний час; 3) координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони в умовах воєнного або надзвичайного стану та при виникненні кризових ситуацій, що загрожують національній безпеці України.

Таким чином, РНБО є органом, відповідальним за формування, координацію та контроль за реалізацією політики в сфері національної безпеки, включно з інформаційною безпекою. Відповідно, діяльність Ради повинна бути серед іншого націлена на програмування пропорційної відповіді України на інформаційні загрози національній безпеці держави.

Рекомендується:

1. Підтримати та включитися в адвокацію реформи санкційної архітектури України, що зараз пропонується кількома групами народних депутатів України. Ця реформа повинна перетворити РНБО в координаційно-аналітичний орган з запровадження санкцій, моніторингу їх дотримання та порушень санкційного режиму. Відсутність на сучасному етапі ефективної системи моніторингу підважує уже запроваджені та можливі майбутні санкції.
2. У разі серйозних зазіхань на кібербезпеку України, які порушують принципи міжнародного права, зазіхають на фундаментальні норми міжнародного права прав людини, міжнародного безпекового права чи міжнародного гуманітарного права, забезпечити накладення на відповідні суб'єкти санкцій.
3. Моніторити дотримання запровадженого санкційного режиму через створене в рамках РНБО бюро щодо санкцій. Таке Бюро має стати постійно діючим допоміжним органом РНБО, до складу якого мають входити уповноважені з санкційної політики від міністерств та відомств. Бюро має стати тією, відсутньою на сьогодні рукою РНБО, що забезпечуватиме якісний аналітичний супровід, обґрунтування рішень та проактивну позицію щодо запровадження зміни та зняття санкцій РНБО.
4. Підтримати, після проведення реформи санкційної архітектури, внесення змін до Кримінального кодексу України та Кодексу про адміністративні правопорушення щодо встановлення відповідальності за порушення санкційного законодавства та санкційних заборон та обмежень. Налагодити комунікацію з правоохоронними органами щодо притягнення до відповідальності фізичних та юридичних осіб, винних у порушенні санкційних режимів.
5. Утримуватися від запровадження санкцій за посягання на інформаційну безпеку України проти українських фізичних та юридичних осіб. Санкції мають залишатися зарезервованими переважно для реагування на загрози, що походять від суб'єктів які не знаходяться під українською юрисдикцією. Для реагування на дії українських суб'єктів мають використовуватися інші правові інструменти, передбачені законами України (щодо боротьби з тероризмом, фінансування тероризму, ліцензування ЗМІ тощо). В разі коли санкції таки запроваджуються проти українських суб'єктів (що наразі є допустимим за діючим законом України "Про санкції"), має даватися належне обґрунтування: а) наявності елементів терористичної діяльності таких суб'єктів або б) підконтрольності таких суб'єктів іноземним юридичним чи фізичним особам чи іноземним державам з урахуванням розуміння терміну "контроль" у статті 1 Закону України "Про захист економічної конкуренції".

ВЕРХОВНА РАДА УКРАЇНИ

Верховна Рада України відповідно до статті 85 Конституції України здійснює парламентський контроль та приймає закони України, які визначають і регулюють діяльність органів сектору безпеки і оборони та їхні повноваження, а також затверджує відповідні бюджетні асигнування та приймає рішення щодо звіту про їх використання. Відповідно до статті 89 Конституції України Верховна Рада України створює комітети Верховної Ради України, до повноважень яких належить, зокрема, забезпечення контролю за діяльністю органів сектору безпеки і оборони.

У частині 1 статті 15 Закону України "Про основні засади забезпечення кібербезпеки України" передбачено, що контроль за дотриманням законодавства при здійсненні заходів із забезпечення кібербезпеки здійснюється Верховною Радою України в порядку, визначеному Конституцією України. Відповідно до частини 3 статті 15 того ж Закону - комітет Верховної Ради України, до предмета відання якого належать питання національної безпеки і оборони, та Комітет Верховної Ради України, до предмета відання якого належать питання інформатизації та зв'язку, на своїх засіданнях розглядають звіти основних суб'єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, про результати незалежного аудиту їхньої діяльності щодо ефективності системи забезпечення кібербезпеки держави.

Основні суб'єкти національної кібербезпеки, визначені частиною другою статті 8 цього Закону, подають один раз на рік звіти про стан виконання ними заходів з питань забезпечення кібербезпеки держави, віднесених до їх компетенції, які мають містити, зокрема, інформацію про результати проведення незалежного аудиту їхньої діяльності. За результатами розгляду звітів основних суб'єктів національної кібербезпеки Комітет Верховної Ради України, до предмета відання якого належать питання інформатизації та зв'язку, може порушити питання про розгляд цих питань Верховною Радою України.

Таким чином Верховна Рада Україна, за допомоги її комітетів (Комітету з питань національної безпеки, оборони та розвідки, Комітету з питань гуманітарної та інформаційної політики, Комітету з питань цифрової трансформації, Комітету з питань свободи слова), формує законодавчу рамку політики щодо інформаційної безпеки, а також здійснює парламентський контроль за її забезпеченням.

Рекомендується:

1. Здійснювати регулярний аналіз та оцінку виконання законів у сфері інформаційної та кібербезпеки, свободи вираження поглядів і поширення інформації. У випадку виявлення вад, які не дають в повній мірі реалізувати норми законів, досягти визначених ними цілей вживати заходів для їх усунення, в т.ч. звертати увагу відповідних суб'єктів на важливість розробки та прийняття необхідних підзаконних нормативно-правових актів. Зазначена діяльність є надзвичайно актуальною, оскільки навіть швидкий, за твердженнями авторів, аналіз виконання Закону України "Про основні засади забезпечення кібербезпеки України" у 2020 році виявив системні проблеми, як в формулюваннях самого закону, так і в частині відсутності великої кількості підзаконних НПА, які є важливими для реалізації багатьох положень закону. Зокрема, останнє стосується чіткого розподілу завдань між суб'єктами у сфері безпеки та оборони в частині кібербезпеки, проведення незалежного аудиту діяльності основних суб'єктів національної кібербезпеки та повноти звітів, які надаються зазначеними суб'єктами профільному комітету Верховної Ради України.
2. Більш активно залучати до законотворчості з питань інформаційної і кібербезпеки, свободи вираження поглядів і поширення інформації та під час здійснення парламентського контролю у зазначених сферах експертів з міжнародних та національних неурядових організацій, а також експертів міжурядових організацій.
3. Прискорити гармонізацію національного законодавства із законодавством Європейського Союзу, стандартами Ради Європи у сфері інформаційної та кібербезпеки, свободи вираження поглядів. Зокрема, імплементувати в національне законодавство норми Конвенції Ради Європи про кіберзлочинність, Директиви ЄС щодо мережевої та інформаційної безпеки (NIS Directive), Директива ЄС про аудіовізуальні медіа послуги, дотримуватись при реформуванні

спецслужб та правоохоронних органів Рекомендацій Ради Європи № 1402 (1999) та Рекомендацій Венеціанської комісії Ради Європи та рекомендації ООН щодо розділення функцій спеціальних служб по захисту національної безпеки та правоохоронних органів.

УПОВНОВАЖЕНИЙ ВЕРХОВНОЇ РАДИ УКРАЇНИ З ПРАВ ЛЮДИНИ

Закон України «Про Уповноваженого Верховної Ради України з прав людини» передбачає, що метою парламентського контролю, який здійснює Уповноважений, є, зокрема: 1) захист прав і свобод людини і громадянина, проголошених Конституцією України, законами України та міжнародними договорами України; 2) додержання та повага до прав і свобод людини і громадянина суб'єктами, зазначеними у статті 2 цього Закону; 3) запобігання порушенням прав і свобод людини і громадянина або сприяння їх поновленню; 4) сприяння приведенню законодавства України про права і свободи людини і громадянина у відповідність з Конституцією України, міжнародними стандартами у цій галузі; 5) поліпшення і подальший розвиток міжнародного співробітництва в галузі захисту прав і свобод людини і громадянина; 6) запобігання будь-яким формам дискримінації щодо реалізації людиною своїх прав і свобод; 7) сприяння правовій поінформованості населення та захист конфіденційної інформації про особу.

Враховуючи широкий спектр прав людини, на захист яких спрямована діяльність Уповноваженого, його обов'язком, безперечно, є й моніторинг та захист інформаційних прав та свобод.

Рекомендується:

1. Продовжувати здійснювати моніторинг дотримання прав та свобод людини в Україні, в тому числі свободи вираження поглядів та права на приватність.
2. Зокрема, звертати увагу на законопроєкти, якими пропонується введення обмежень на свободу вираження поглядів, в тому числі з метою захисту національної безпеки України, її територіальної цілісності, громадської безпеки, для запобігання заворушенням чи злочинам тощо. Надавати таким законопроєктам правову оцінку на предмет дотримання вимог національного законодавства та міжнародного права, а саме щодо «якості закону», існування легітимної мети та необхідності таких обмежень в демократичному суспільстві. За результатами цієї роботи готувати відповідні висновки та рекомендації.
3. Посилити контроль за законністю обробки персональних даних, запровадити механізм швидкого реагування на факти порушення законодавства у сфері персональних даних (в тому числі у разі їх несанкціонованого витоку). Такий контроль повинен включати комплекс невідкладних заходів, спрямованих на швидке вилучення зазначених відомостей із загальнодоступних джерел та іншого припинення порушення прав, відшкодування завданої шкоди.
4. Здійснювати постійний контроль за впровадженням та функціонуванням системи цифрової ідентифікації (створенням документів, що підтверджують певний правовий статус, зокрема, посвідчень водіїв, студентських квитків, ID-карток тощо в цифровій формі), серед іншого за дотриманням прав людини при її створенні та експлуатації.

СЛУЖБА БЕЗПЕКИ УКРАЇНИ

Відповідно до статті 1 Закону України «Про Службу безпеки України» Служба безпеки України – державний орган спеціального призначення з правоохоронними функціями, який забезпечує державну безпеку України. Стаття 2 того ж Закону передбачає, що на Службу безпеки України покладається у межах визначеної законодавством компетенції захист державного суверенітету, конституційного ладу, територіальної цілісності, економічного, науково-технічного і оборонного потенціалу України, законних інтересів держави та прав громадян від розвідувально-підривної діяльності іноземних спеціальних служб, посягань з боку окремих організацій, груп та осіб, а також забезпечення охорони державної таємниці. До завдань Служби безпеки України також входить попередження, виявлення, припинення та розкриття кримінальних правопорушень проти миру і безпеки людства, тероризму, корупції та організованої злочинної діяльності у сфері управління і економіки та інших протиправних дій, які безпосередньо створюють загрозу життєво важливим інтересам України.

У статтях 12, 19 Закону України «Про національну безпеку України» визначено Службу безпеки України, як один з державних органів, який входить до складу сектору безпеки та оборони на який покладено: 1) протидію розвідувально-підривній діяльності проти України; 2) боротьбу з тероризмом; 3) контррозвідувальний захист державного суверенітету, конституційного ладу і територіальної цілісності, оборонного і науково-технічного потенціалу, кібербезпеки, економічної та інформаційної безпеки держави, об'єктів критичної інфраструктури; 4) охорону державної таємниці.

Рекомендується:

1. Підвищити ефективність реалізації цілей та задач, визначених для СБУ Доктриною інформаційної безпеки України від 25 лютого 2017 року та Стратегією кібербезпеки України від 15 березня 2016 року.
2. Забезпечити дотримання міжнародних стандартів (наприклад, запропонованих в Рекомендації Ради Європи № 1402 (1999), рекомендації Венеціанської Комісії Ради Європи та ООН щодо розділення функцій спеціальних служб по захисту національної безпеки та правоохоронних органів) під час реформи Служби та здійснювати її на засадах поваги до прав людини, законності, легітимності та обґрунтованості обсягу та порядку здійснення повноважень Службою безпеки України. Зокрема, проєкт закону № 3196-д «Про внесення змін до Закону України «Про Службу безпеки України» має передбачити позбавлення СБУ правоохоронних функцій, визначити чіткі запобіжники проти зловживання повноваженнями СБУ у сфері прав людини та передбачити детальні процедури і механізми, покликані створити ефективну систему незалежного контролю над СБУ. В частині онлайн він має більш чітко визначити підстави та порядок судового та позасудового блокування сайтів, передбачити достатні запобіжники від зловживань при перехопленні електронних комунікацій, звузити доступ до державних баз даних та можливості отримувати будь-яку персональну інформацію про особу за своїм запитом. Крім того, потребують значного вдосконалення процедури втручання СБУ у виборчий процес та ініціювання анулювання ліцензій для телерадіоорганізацій або, має бути прийняте рішення про відмову від таких можливостей взагалі.
3. Здійснювати постійний моніторинг вітчизняних та іноземних засобів масової інформації, мережі Інтернет з метою виявлення загроз національній безпеці України в інформаційній сфері та оперативну розробку та вжиття заходів протидії виявленим загрозам. Особливу увагу приділяти дезінформації від держави-агресора або інших суб'єктів, якщо така кампанія з дезінформації може бути охарактеризована як спеціальна інформаційна операція, спрямована на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуацій, втручання у виборчий процес тощо.
4. Підвищити ефективність виявлення та притягнення до відповідальності осіб, що створені та/або використовуються державою-агресором або іншими суб'єктами з метою заподіяння

шкоди національним інтересам України в інформаційній сфері та унеможливлення їхньої підривної діяльності.

5. Підвищити ефективність попередження, виявлення, припинення та розкриття злочинів, які вчиняються у кіберпросторі і загрожують національній безпеці України, здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на боротьбу з кібертероризмом та кібершпигунством.
6. Щорічно надавати детальний та змістовний звіт до профільного комітету Верховної Ради України про стан виконання заходів з питань забезпечення кібербезпеки.

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ

Відповідно статей 12, 15 Закону України «Про національну безпеку України» Міністерство оборони України входить до складу сектору безпеки і оборони і є головним органом у системі центральних органів виконавчої влади, що забезпечує формування та реалізує державну політику з питань національної безпеки у воєнній сфері, сферах оборони і військового будівництва у мирний час та особливий період. У п.1 Положення про Міністерство оборони України передбачено, що Міноборони є центральним органом виконавчої влади та військового управління, у підпорядкуванні якого перебувають Збройні Сили та Держспецтрансслужба, а згідно норм п.п. 4,5 – Міноборони визначає шляхи становлення та розвитку спроможностей системи стратегічних комунікацій у Міноборони та Збройних Силах як складової загальнодержавної системи стратегічних комунікацій, бере участь у проведенні аналізу воєнно-політичної обстановки, прогнозуванні, виявленні та визначенні рівня воєнної загрози національній безпеці України, відповідно до компетенції вживає заходів до забезпечення інформаційної безпеки, кібербезпеки та кіберзахисту, а також підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони), а також забезпечує в межах повноважень, передбачених законом, реалізацію державної політики у сфері охорони державної таємниці, захисту інформації з обмеженим доступом, інформаційної безпеки та кібербезпеки, а також технічний захист інформації, контроль за її збереженням в апараті Міноборони, на підприємствах, в установах і організаціях, які належать до сфери його управління.

Враховуючи центральне місце Міністерства у формуванні та реалізації безпекової та оборонної політики України, а також покладання на міністерство завдань щодо стратегічних комунікацій, протидії агресії в кіберпросторі тощо, принципово важливим є лідерство Міністерства у досягненні інформаційної безпеки України.

Рекомендується:

1. Підвищити ефективність реалізації цілей та задач, визначених для Міноборони Доктриною інформаційної безпеки України від 25 лютого 2017 року та Стратегією кібербезпеки України від 15 березня 2016 року.
2. Створити і розвивати структури, що відповідають за інформаційно-психологічну безпеку, насамперед у Збройних Силах України, з урахуванням практики держав – членів НАТО.
3. Брати участь у виробленні і оперативній адаптації державної політики у сфері кібербезпеки/кіберпростору з відповідними стандартами ЄС та НАТО.
4. Здійснювати постійний моніторинг дезінформаційних кампаній держави-агресора або інших суб’єктів, якщо їх кампанії з дезінформації направлені на заподіяння шкоди ЗСУ, послаблення обороноздатності країни та унеможливлення оперативної реалізації ефективних заходів протидії.
5. Організувати і підтримувати в ефективному стані систему військово-цивільних зв’язків/комунікацій у місцях постійної дислокації та розгортання підрозділів Збройних Сил України, інших військових формувань.
6. Організувати і забезпечувати:
    - зв'язки з українськими та іноземними засобами масової інформації щодо висвітлення ситуації в районі проведення ООС в Донецькій та Луганській областях;
    - належний рівень інформаційного супроводу виконання завдань з оборони України;
    - оперативне донесення достовірної інформації до військовослужбовців Збройних Сил України, інших військових формувань;
    - здійснення військової співпраці з НАТО, пов’язаної з безпекою кіберпростору та сумісним захистом від кіберзагроз;
    - здійснення заходів з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони).
7. Забезпечити цивільний контроль над військовими формуваннями, що діють у сфері кібербезпеки.
8. У взаємодії з Державною службою спеціального зв'язку та захисту інформації України і Службою безпеки України забезпечити кіберзахист власної інформаційної інфраструктури.

9. Щорічно надавати детальний та змістовний звіт до профільного комітету Верховної Ради України про стан виконання заходів з питань забезпечення кібербезпеки.

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Відповідно до частини 2 статті 12 Закону України «Про національну безпеку України» Міністерство внутрішніх справ України (МВС України) входить до складу сектору безпеки і оборони. У пункті першому частини 1 статті 18 того ж закону передбачено, що МВС є центральним органом виконавчої влади, що забезпечує формування та реалізує державну політику щодо забезпечення охорони прав і свобод людини, інтересів суспільства і держави, протидії злочинності, підтримання громадської безпеки і правопорядку, а також надання поліцейських послуг. Відповідно до пункту другого частини 2 статті 8 Закону України «Про основні засади забезпечення кібербезпеки України» Національна поліція України забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від кримінально протиправних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі.

Законодавчі повноваження МВС знайшли своє подальше роз'яснення в Положенні про Міністерство внутрішніх справ України МВС України, де вони інтерпретуються через визначення, що МВС: узагальнює практику застосування законодавства з питань, що належать до його компетенції, розробляє пропозиції щодо його вдосконалення та в установленому порядку вносить їх на розгляд Кабінету Міністрів України; розробляє проекти законів та інших нормативно-правових актів з питань, що належать до його компетенції; організовує та забезпечує експлуатацію, розвиток, координацію та функціонування системи зв'язку МВС, управління і моніторинг єдиної цифрової відомчої телекомунікаційної мережі МВС та закріпленого радіочастотного ресурсу України; забезпечує в межах повноважень, передбачених законом, захист інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

Найбільш спеціалізованим підрозділом МВС, функціонал якого значною мірою лежить в площині інформаційної безпеки, є створена 13 жовтня 2015 року Кіберполіція. Кіберполіція є структурним підрозділом Національної поліції. Метою створення Кіберполіції в Україні було реформування та розвиток підрозділів МВС України, що забезпечило підготовку та функціонування висококваліфікованих фахівців в експертних, оперативних та слідчих підрозділах поліції, задіяних у протидії кіберзлочинності, та здатних застосовувати на високому професійному рівні новітні технології в оперативно-службовій діяльності.

Рекомендується:

1. Підвищити ефективність реалізації цілей та задач, визначених для МВС України Доктриною інформаційної безпеки України від 25 лютого 2017 року та Стратегією кібербезпеки України від 15 березня 2016 року.
2. Забезпечити притягнення до адміністративної відповідальності за поширювання неправдивих чуток в мережі Інтернет на підставі статті 173-1 КУпАП у відповідність із законодавством у сфері адміністративних правопорушень так і нормами, які гарантують свободу вираження поглядів та поширення інформації. Зокрема, зміст та форма протоколів про адміністративні правопорушення та матеріалів, які надсилаються до суду повинні точно відповідати вимогам КУпАП, а зміст та опис фабули має містити всі ознаки складу правопорушення, як в частині поширення і неправдивості чуток, так і обґрунтування того, чому вони можуть викликати паніку серед населення або порушення громадського порядку. Від зазначеного складу правопорушення поліцейські мають відрізняти різноманітні прояви свободи вираження поглядів (в т.ч. гумор, сарказм, іронію) та поширення неправдивої інформації, яка не може мати наслідків, передбачених статтею 173-1 КУпАП, як обов'язкових ознак складу правопорушення.
3. Покращити рівень розслідування злочинів, вчинених проти журналістів онлайн видань через їх професійну діяльність. Зокрема, за статтями 171 КК України («Перешкоджання законній професійній діяльності журналістів»), 345-1 («Погроза або насильство щодо журналіста»), 347-1 («Умисне знищення або пошкодження майна журналіста»), 348-1 («Посягання на життя журналіста»). Проблема відсутності належного покарання за погрози, напади,

вбивства журналістів, знищення та пошкодження майна редакцій, в т.ч. онлайн видань в Україні є системною та тривалою.

4. Забезпечити сталий/інституційний розвиток кіберполіції з метою підвищення ефективності її діяльності, виявлення та притягнення до відповідальності за вчинення злочинів у кіберпросторі.
5. Щорічно надавати детальний та змістовний звіт до профільного комітету Верховної Ради України про стан виконання заходів з питань забезпечення кібербезпеки.

МІНІСТЕРСТВО ЮСТИЦІЇ УКРАЇНИ

Положення про Міністерство юстиції України, затверджене постановою Кабінету Міністрів України від 02.07.2014 року № 228 з наступними змінами та доповненнями, передбачає, що до основних завдань Міністерства, зокрема, відносяться наступні: 1) забезпечення формування та реалізація державної правової політики; 2) контроль за дотриманням прав людини і громадянина; 3) забезпечення формування та реалізація державної політики у сфері правової освіти, правової обізнаності, інформування населення, доступу громадян до джерел правової інформації; 4) здійснення міжнародно-правового співробітництва, забезпечення дотримання і виконання зобов'язань, узятих за міжнародними договорами України з правових питань.

Враховуючи функціональне спорядження Міністерства та його залученість до формування та реалізації державної політики у згаданих вище сферах, воно є активним гравцем у сфері інформаційної безпеки держави.

Рекомендується:

1. Під час реформування санкційного законодавства та запровадження санкцій, які обмежують свободу вираження в інтернеті, наполягати на врахуванні європейських та конституційних стандартів в галузі свободи вираження. Взяти до уваги, що обмеження доступу до веб-ресурсів на підставі такої санкції, як «інші санкції, що відповідають принципам їх застосування, встановленим цим Законом», не відповідає стандартам прав людини, адже порушується вимога щодо якості закону, зокрема, стосовно його передбачуваності. З огляду на це варто уникати застосування цієї підстави для обмеження доступу до соціальних мереж та веб-сайтів.
2. Водночас, зважаючи на посилення ролі інтернету в суспільному житті та ризики, пов'язані із особливостями цієї технології, яка дозволяє швидко поширювати, довго зберігати інформацію, охоплюючи при цьому широку аудиторію, запропонувати зміни або підтримати пропозиції про внесення змін до законодавства, спрямовані на визначення чітких та передбачуваних підстав та порядку обмеження доступу до поширюваної в інтернеті інформації, яка завдає, або може завдати шкоди українській національній безпеці та, зокрема, кібербезпеці. Під час розробки відповідних законопроєктів врахувати міжнародні стандарти в галузі свободи вираження, забезпечивши баланс між інтересами, які захищаються та правом на свободу слова. Наполягати на застосуванні зазначених підходів в тому числі під час підготовки та розгляду пропозицій про внесення відповідних змін до Закону України «Про санкції».
3. Розробити пропозиції до законодавства України з метою врегулювання правового статусу онлайн засобів масової інформації, встановивши вимоги до їх прозорості (в тому числі фінансової) та визначивши інші особливості їх діяльності.
4. Ініціювати розробку концепції боротьби з дезінформацією, в якій дати визначення різним типам шкідливої інформації, що поширюється в національному інформаційному просторі України, запропонувати різні засоби правового впливу на кожен з них залежно від ступеня суспільної небезпеки та запропонувати комплекс організаційних, технічних, освітніх, та інших заходів, спрямованих на запобігання її поширенню та/або нейтралізацію негативних наслідків від її розповсюдження.
5. Для реалізації наведених у попередньому пункті рекомендацій провести широкі консультації з усіма зацікавленими особами, в тому числі операторами телекомунікацій, хостинг-провайдерами, реєстраторами доменних імен, медійними організаціями, відповідними профільними асоціаціями, громадськими організаціями та широкою громадськістю, залучивши їх до розробки відповідних змін до законодавства.
6. Здійснюючи експертне забезпечення правосуддя та виконуючи обов'язки, покладені на Мінюст Законом України «Про виконання рішень та застосування практики Європейського суду з прав людини», оперативно доводити до відома Верховного Суду, інших судів України та інших зацікавлених осіб найважливіші рішення, які стосуються блокування веб-сайтів в інтернеті (зокрема, у справах «Vladimir Kharitonov v. Russia», application no. 10795/14; «Bulgakov v. Russia», application no. 20159/15; «Engels v. Russia», application no. 61919/16;

«OOO Flavus and Others v. Russia», application nos. 12468/15 and 2 others), здійснюючи їх офіційний переклад.

МІНІСТЕРСТВО ЦИФРОВОЇ ТРАНСФОРМАЦІЇ УКРАЇНИ

Положення про Міністерство цифрової трансформації України, затверджене постановою Кабінету Міністрів України від 18.09.2019 року № 856 з наступними змінами і доповненнями, до основних завдань Міністерства відносить формування та реалізацію державної політики, зокрема у сферах: цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій та технологій, електронного урядування та електронної демократії, розвитку інформаційного суспільства; розвитку цифрових навичок та цифрових прав громадян; відкритих даних, розвитку національних електронних інформаційних ресурсів та інтероперабельності, розвитку інфраструктури широкосмугового доступу до Інтернету та телекомунікацій, електронної комерції та бізнесу; надання електронних та адміністративних послуг; електронних довірчих послуг та електронної ідентифікації та інвестицій в ІТ-індустрію; у сфері розвитку ІТ-індустрії.

Враховуючи те, що реалізація цифрової трансформації у наведених у попередньому параграфі сферах має здійснюватися з урахуванням вимог та потреб національної безпеки (включаючи національну безпеку у кіберсфері), Міністерство є одним з ключових гравців у галузі інформаційної безпеки.

Рекомендується:

1. Реалізуючи свої повноваження, пов'язані із виконанням Національної програми інформатизації, в тому числі в частині захисту інформаційного суверенітету держави, неухильно дотримуватись вимог законодавства України та міжнародних договорів в галузі прав людини, і зокрема, права на свободу вираження поглядів та права на приватність.
2. Періодично, не рідше одного разу на рік, оприлюднювати інформацію (звіти) про результати моніторингу даних про вчинення та/або спроби вчинення несанкціонованих дій щодо державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, а також про їх наслідки, та про вжиті заходи щодо їх припинення та усунення негативних наслідків і проводити їх публічні обговорення за участі громадськості. За результатами обговорень готувати пропозиції щодо посилення інформаційної безпеки України.
3. Періодично, не рідше одного разу на рік, оприлюднювати інформацію (звіти) про результати здійснення нагляду у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення щодо постачальників послуг, пов'язаних з обігом віртуальних активів та проводити їх публічні обговорення за участі громадськості. За результатами обговорень готувати пропозиції щодо посилення інформаційної безпеки України.
4. Впроваджуючи цифрові послуги та використовуючи систему цифрової ідентифікації неухильно дотримуватись прав людини. З цією метою розробити відповідний проект закону, який врегулює коло прав та обов'язків осіб, які приймають участь у створенні, впровадженні та функціонуванні системи цифрової ідентифікації, а також передбачить підстави та процедуру захисту прав громадян від можливих правопорушень. Під час підготовки законопроєкту провести консультації з широким колом зацікавлених представників громадськості, в тому числі з правозахисними організаціями.
5. Впроваджуючи надання пріоритетних публічних послуг в електронній формі та/або здійснюючи модернізацію державного управління за допомогою інформаційно-комунікаційних технологій неухильно дотримуватись вимог, визначених законами України та міжнародними стандартами у сфері захисту персональних даних осіб. Зокрема, не допускати обробки персональних даних з іншою метою, ніж та, для якої вони законно збирались. Не об'єднувати значні обсяги персональної інформації про особу в одну базу та/або не об'єднувати кілька існуючих баз персональних даних в одну. Унеможливити доступ осіб, які надають адміністративні та інші онлайн послуги, до інформації, яка не є необхідною для надання відповідного виду адміністративних послуг.
6. Посилити контроль за обробкою, в тому числі зберіганням персональних даних, а також за доступом до іншої інформації з обмеженим доступом під час надання адміністративних послуг, запобігаючи незаконному витоку персональних даних. Особливу увагу приділити обробці чутливої інформації, зокрема, відомостей, які стосуються стану здоров'я осіб.

7. Виступаючи із ініціативами впровадження системи фільтрації інформації з метою обмеження доступу неповнолітніх дітей до незаконного контенту, який поширюється в інтернеті і може завдати їм шкоди, враховувати міжнародні стандарти в галузі свободи слова, зокрема, ті, що викладені в Рекомендації CM/Rec(2018)2 Комітету Міністрів державам-членам [Ради Європи] про ролі та обов'язки Інтернет-посередників *(ухвалені Комітетом Міністрів 7 березня 2018 року на 1309-му засіданні Заступників Міністрів)*, які передбачають, що:

   - органи державної влади не повинні прямо чи опосередковано нав'язувати посередникам загальний обов'язок контролю за контентом, до якого вони усього лиш надають доступ або ж передають, або зберігають її використовуючи автоматизовані чи інші подібні засоби. При зверненні із будь-яким запитом до Інтернет-посередників або заохоченні, самостійно або з іншими державами чи міжнародними організаціями, Інтернет-посередників до підходів спільного регулювання, державні органи повинні уникати будь-яких дій, які можуть призвести до загального моніторингу контенту. Усі співрегуляторні підходи мають відповідати принципам верховенства права та гарантій прозорості (див. п. 1.3.5 Додатку до Рекомендації CM/Rec (2018)2 Керівні принципи для держав стосовно дій, що мають бути вжиті щодо Інтернет-посередників, з належним врахуванням їх ролей і обов'язків);
   - держави повинні забезпечити закріплення, у законодавстві та на практиці, що посередники не несуть відповідальності за сторонній контент, до якого вони просто надають доступ або ж передають, або зберігають. Органи державної влади можуть вважати, що посередники є спів-відповідальними за контент, який вони зберігають, якщо вони не діятимуть оперативно, аби обмежити доступ до контенту чи послуг, як тільки-но вони усвідомлюють їх незаконний характер, у тому числі через процедури на основі сповіщення. Органи державної влади повинні забезпечувати, щоб процедури, орієнтовані на сповіщення, не розроблялись таким чином, щоб стимулювати вилучення законного контенту, наприклад, через неприйнятно короткі терміни. Сповіщення повинні містити інформацію, достатню для посередників для вжиття відповідних заходів. Сповіщення, подані державами, повинні базуватися на власній оцінці незаконності контенту, про який сповіщено, відповідно до міжнародних стандартів. Обмеження контенту повинні передбачати сповіщення виробника/видавця контенту про таке обмеження якомога швидше, якщо це не перешкоджатиме поточній правоохоронній діяльності. Інформація також повинна бути доступною для користувачів, які шукають доступ до контенту, відповідно до застосовних законів про захист даних (див. п. 1.3.7 Додатку до Рекомендації CM/Rec (2018)2 Керівні принципи для держав стосовно дій, що мають бути вжиті щодо Інтернет-посередників, з належним врахуванням їх ролей і обов'язків).

МІНІСТЕРСТВО КУЛЬТУРИ ТА ІНФОРМАЦІЙНОЇ ПОЛІТИКИ УКРАЇНИ

В Положенні про Міністерство культури України, затвердженому Постановою Кабінету міністрів України від 16 жовтня 2019 року № 885, наступним чином визначенні окремі завдання Міністерства: 1) забезпечення формування та реалізації: державної політики у сферах культури та державної мовної політики; державної політики у сферах інформаційного суверенітету, інформаційної безпеки України; державної політики у сферах популяризації України в світі, стратегічних комунікацій; 2) забезпечення формування та реалізації державної політики у сферах кінематографії, відновлення та збереження національної пам'яті, міжнаціональних відносин, релігії та захисту прав національних меншин...; 3) забезпечення формування та реалізації державної політики у сфері телебачення і радіомовлення, інформаційній та видавничій сфері; 5) участь у формуванні та реалізації державної політики з питань тимчасово окупованих територій України у Донецькій та Луганській областях, Автономній Республіці Крим і м. Севастополі та населення, що на них проживає, з метою їх реінтеграції в єдиний культурний та інформаційний простір України.

Так як окремі загрози інформаційній національній безпеці виникають вздовж лінії діяльності у сфері культури та реалізації культурних проектів, а також у зв'язку із відповідальністю відомства за координацію інформаційної політики держави, то Міністерство має мати чітке уявлення про власні можливості щодо протидії інформаційним загрозам із одночасним дотриманням вимог пропорційності та захищеності прав людини.

Рекомендується:

1. Продовжити адвокацію прийняття законопроєкту «Про медіа», який регулюватиме сучасні засоби поширення інформації та надаватиме Міністерству важелі впливу на випадок створення останніми загроз національній безпеці України.
2. Уникати рекомендації килимових заборон інформаційного контенту в рамках свого повноваження по «формуванню толерантності в українському суспільстві». Натомість акцент має робитися на точкових обмеженнях, що мають реагувати на безпосереднє порушення інформаційної безпеку держави через розпалювання міжетнічної ворожнечі, проявів дискримінації чи нетерпимості. Уникати килимових заборон й при оцінці видавничої продукції та кінематографічної продукції задля їх розповсюдження на території України.
3. Повернутися до реалізації ідеї, зафіксованої ще у 2017 році у Доктрині інформаційної безпеки, щодо створення центру стратегічних комунікацій як допоміжного органу Міністерства культури та інформаційної політики. Такий Центр має координувати зусилля міністерств та інших органів державної влади щодо протидії поширенню дезінформації в українському інформаційному просторі. Він також має налагодити співпрацю з існуючими "горизонтальними" ініціативами щодо протидії дезінформації, що наразі існують в окремих органах державної влади та в форматі громадських ініціатив. Можливим прикладом по конструюванню такого органу може стати Аналітичний центр ЄС щодо протидії дезінформації.

ОФІС ГЕНЕРАЛЬНОГО ПРОКУРОРА

Відповідно до частини 1 статті 8 Закону України «Про прокуратуру» Офіс Генерального прокурора організовує та координує діяльність усіх органів прокуратури, забезпечує належне функціонування Єдиного реєстру досудових розслідувань та його ведення органами досудового розслідування, визначає єдиний порядок формування звітності про стан кримінальної протиправності і роботу прокурора з метою забезпечення ефективного виконання функцій прокуратури, а також здійснює управління об'єктами державної власності, що належать до сфери управління Офісу Генерального прокурора.

Покладені на прокуратуру функції визначають її як важливого гравця у сфері процесуального керівництва розслідуваннями, що пов'язані з скоєнням посягання на інформаційну безпеку держави, та тими, що скоюються за допомогою мережі Інтернет.

Рекомендується:

1. Покращити процесуальне керівництво розслідуваннями і рівень розкриття злочинів, вчинених проти журналістів онлайн видань через їх професійну діяльність. Зокрема, за статтями 171 КК України («Перешкоджання законній професійній діяльності журналістів»), 345-1 («Погроза або насильство щодо журналіста»), 347-1 («Умисне знищення або пошкодження майна журналіста»), 348-1 («Посягання на життя журналіста»).
2. Покращити процесуальне керівництво розслідуваннями, рівень та якість розкриття злочинів, вчинених за допомогою мережі Інтернет у сфері національної безпеки, запобігання тероризму та пропаганди війни. Зокрема, за статтями 109 КК України («Дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади»), 110 («Посягання на територіальну цілісність і недоторканність України»), 111 («Державна зрада»), 114-1 («Перешкоджання законній діяльності Збройних Сил України та інших військових формувань»), 258-2 («Публічні заклики до вчинення терористичного акту»), 436 («Пропаганда війни»), а також за статтею 161 КК України («Порушення рівноправності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за іншими ознаками») та 295 («Заклики до вчинення дій, що загрожують громадському порядку».

ВЕРХОВНИЙ СУД

Закон України «Про судоустрій і статус суддів» встановлює, що Верховний Суд є найвищим судом у системі судоустрою України, який забезпечує сталість та єдність судової практики у порядку та спосіб, визначених процесуальним законодавством. Верховний Суд, зокрема, здійснює аналіз судової статистики, узагальнення судової практики; забезпечує однакове застосування норм права судами різних спеціалізацій у порядку та спосіб, визначені процесуальним законом; забезпечує апеляційні та місцеві суди методичною інформацією з питань правозастосування; здійснює інші повноваження, визначені законом.

Враховуючи вищесказане, Верховний Суд є ключовим гравцем у формуванні одноманітного, заснованого на повазі до прав людини та європейських стандартах, підходу до вирішення спорів, що виникають внаслідок реалізації державою політики у сфері інформаційної безпеки.

Рекомендується:

1. Узагальнити судову практику у кримінальних провадженнях, пов'язаних із притягненням осіб до кримінальної відповідальності за поширення в мережі інтернет забороненої інформації, зокрема, за наступними статтями Кримінального кодексу України: 109 (дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади); 110 (посягання на територіальну цілісність і недоторканність України); 111 (державна зрада); 114-1 (перешкоджання законній діяльності Збройних Сил України та інших військових формувань); 161 (порушення рівноправності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за іншими ознаками); 258-2 (публічні заклики до вчинення терористичного акту); 258-3 (створення терористичної групи чи терористичної організації), 295 (заклики до вчинення дій, що загрожують громадському порядку); 300 (ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію), 301 (ввезення, виготовлення, збут і розповсюдження порнографічних предметів), (436 (пропаганда війни) тощо. Під час узагальнення звернути увагу на:

    - правомірність прийняття судами повідомлень, оприлюднених на сайті «Миротворець», як належних, допустимих та достовірних доказів, що підтверджують вину підсудних (засуджених), а також на обґрунтованість судових рішень, що спираються на подібні повідомлення;
    - правомірність віднесення соціальних мереж, зокрема, «Вконтакте» та «Одноклассники», а також Інтернету як такого, **до засобів масової інформації** та застосування у зв'язку з цим до засуджених за статтями 109, 258-2, 436-1 КК України такої кваліфікуючої ознаки, як «дії, вчинені з використанням засобів масової інформації»;
    - обґрунтованість притягнення до кримінальної відповідальності за ч. 1 статті 253-3 КК України осіб, які надавали інформаційну підтримку діяльності терористичної організації, зокрема, пропагували та розповсюджували ідеологію тероризму, або іншими словами здійснювали «інше сприяння створенню або діяльності терористичної групи та терористичної організації»;
    - обґрунтованість судових рішень в частині оцінки змісту повідомлень, поширення яких стало підставою для притягнення до кримінальної відповідальності. Зокрема, звернути увагу на те, чи здійснюють суди самостійний аналіз змісту поширених обвинуваченими повідомлень, чи надають вони їм відповідну **правову** оцінку, а також оцінку належності, допустимості та обґрунтованості відповідних експертних висновків;
    - оцінку судами впливу протиправного контенту, поширеного в мережі інтернет, на аудиторію (з урахуванням її чисельності), а також обґрунтування ними негативних наслідків від такого поширення;

- можливість ухвалення рішень про видалення незаконного контенту з мережі Інтернет або обмеження доступу до нього.

2. Узагальнити судову практику застосування судами такого заходу забезпечення кримінального провадження, як арешт майна. Під час узагальнення звернути увагу на:
   - законність ухвалення судами рішень про накладення арешту на майнові права інтелектуальної власності, які начебто виникають у користувачів мережі інтернет при використанні веб-ресурсів шляхом зобов'язання інтернет провайдерів, що здійснюють діяльність на території України, які відповідно до частини 2 ст. 42 ЗУ «Про телекомунікації» включені до реєстру операторів, провайдерів телекомунікацій й перелік яких міститься на офіційному веб-сайті Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, закрити доступ до веб-ресурсів зазначених в ухвалі;
   - відповідність зазначеного заходу законній меті;
   - дотримання принципу пропорційності при ухваленні судових рішень щодо накладення арешту;
   - відповідності та достатності мотивів, наведених в таких судових рішеннях в обґрунтування необхідності застосування наведеного заходу.
3. Узагальнити судову практику у адміністративних справах про поширювання неправдивих чуток (стаття 173-1 КУпАП). Під час узагальнення звернути увагу на:

   - обов'язковість застосування під час розгляду зазначеної категорії справ міжнародних стандартів в галузі свободи слова, в тому числі, визначених статтею 10 Європейської Конвенції про захист прав людини і основоположних свобод та практикою Європейського суду з прав людини;
   - необхідність встановлення точного змісту інформації, у зв'язку із поширенням якої складено протокол про адміністративне правопорушення, викладаючи її зміст в рішенні суду;
   - належність та достатність наведених судом міркувань щодо встановлення наявності складу адміністративного правопорушення (зокрема, умислу на спричинення паніки та/або порушення громадського порядку);
   - неприпустимість застосування покарання за критику діяльності тих чи інших владних інституцій або посадових осіб, а також на необхідність застосування європейських стандартів звільнення від відповідальності у випадках поширення інформації, отриманої від третіх осіб із посиланням на її джерело.

4. Узагальнити судову практику у справах про захист честі, гідності, ділової репутації, спростування недостовірної інформації та відшкодування шкоди, пов'язаної із поширенням спірної інформації в мережі Інтернет. Під час узагальнення звернути увагу на:
   - правильність застосування судами правових підстав для застосування такого способу правового захисту, як видалення спірної інформації, визнаної судом недостовірною, а також на різні підходи судів до застосування зазначеного способу правового захисту;
   - відповідність зазначеного способу правового захисту міжнародним стандартам в галузі свободи слова (зокрема в світлі рішення ЄСПЛ у справі «Węgrzynowski and Smolczewski проти Польщі» (заява № 33846/07, рішення від 16 липня 2013 року);
   - обґрунтованість одночасного застосування судами таких способів правового захисту як спростування та видалення спірної інформації, визнаної недостовірною, та дотримання судами принципу пропорційності при ухваленні зазначених рішень;
   - необхідність дотримання авторських прав і неприпустимість порушення цілісності твору під час виконання рішення суду про спростування недостовірної інформації (наприклад, у разі зобов'язання оприлюднити спростування між заголовком і текстом спірної публікації);
   - неприпустимість порушення права на приватність та захист персональних даних при ухваленні рішень, якими на відповідача покладається обов'язок оприлюднити спростування у вигляді повного тексту рішення суду, що містить персональні дані

позивача, відповідача та інших учасників судового розгляду (наприклад, паспортні дані, реєстраційний номер облікової картки платника податків, домашню адресу тощо);

- необхідність досягнення балансу між правом на свободу слова, з одного боку, та презумпцією невинуватості, з іншого, та ухвалення рішень з урахуванням відповідної практики Європейського суду з прав людини із зазначених питань.

5. Узагальнити судову практику у справах про захист права на приватне життя (включаючи персональні дані), в тому числі справах, пов'язаних із вилученням (видаленням) з мережі інтернет (певних веб-ресурсів, статей тощо) персональних даних, інформації про приватне, сімейне та особисте життя та/чи обмеженням доступу до такої інформації. Під час узагальнення звернути увагу на:

    - правильність застосування судами правових норм, що регулюють право на використання імені особи та дотримання міжнародних стандартів балансування права на приватне життя та свободи слова;
    - ефективні способи захисту права на захист персональних даних та інформації про приватне, сімейне та особисте життя та особливості застосування цих способів;
    - міжнародних стандартів балансування права на приватне життя та права на захист приватного, сімейного та особистого життя.

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ (ДССЗЗІ)

Відповідно до частини 2 статті 12 Закону України "Про національну безпеку України" ДССЗЗІ входить до складу сектору безпеки та оборони. Стаття 22 того ж Закону визначає, що ДССЗЗІ є державним органом, призначеним для забезпечення функціонування і розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, формування та реалізації державної політики у сферах кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, а також інших завдань відповідно до закону.

Відповідно до частини 2 статті 8 Закону України "Про основні засади забезпечення кібербезпеки України" ДССЗЗІ є одним з основних суб'єктів національної системи кібербезпеки України, на яку покладено завдання щодо забезпечення формування та реалізації державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, кіберзахисту об'єктів критичної інформаційної інфраструктури, державного контролю у цих сферах. Також ДССЗЗІ координує діяльність інших суб'єктів забезпечення кібербезпеки щодо кіберзахисту, забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту, здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків, інформує про кіберзагрози та відповідні методи захисту від них, забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації), координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість, забезпечує функціонування Державного центру кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA.

Протягом 2020-го року було прийнято багато важливих підзаконних нормативно-правових актів у сфері кіберзахисту. Зокрема, щодо створення національної телекомунікаційної мережі, порядку ведення реєстру об'єктів критичної інфраструктури. Проте, не менше знаходяться на етапі погоджень або розробки.

Рекомендується:

1. Вжити заходів для прискорення роботи над розробкою, доопрацюванням та/або просуванням проєктів законів у сфері кібербезпеки. Зокрема:
    - щодо збереження резервних копій інформації та відомостей державних електронних інформаційних ресурсів;
    - забезпечення можливості страхування ризиків у сфері кібербезпеки та компенсації збитків, завданих кібератаками;
    - визначення відповідальності для державних публічних осіб та осіб, які мають забезпечити захист об'єктів критичної інфраструктури;
    - наполягати, щоб зміни до законодавства України про санкції передбачали можливості або обмеження використання на об'єктах критичної інфраструктури програмного забезпечення та технічних засобів телекомунікацій, розроблених/виготовлених за участі організацій держави-агресора;
    - щодо критичної інфраструктури та її захисту;
    - проєкту закону "Про безпеку інформації та комунікаційно-інформаційних систем".
2. Вжити заходів для прискорення роботи над розробкою, доопрацюванням та/або просуванням підзаконних нормативно-правових актів у сфері кіберзахисту. Зокрема, проєкту Постанови Кабінету Міністрів України «Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури», проєкту Постанови Кабінету Міністрів України «Про затвердження Протоколу спільних дій суб'єктів забезпечення кібербезпеки, власників (розпорядників) об'єктів критичної інформаційної інфраструктури під час

виявлення, попередження, припинення кібератак та кіберінцидентів, а також при усуненні їх наслідків» та ін.

3. Щорічно надавати детальний та змістовний звіт до профільного комітету Верховної Ради України про стан виконання заходів з питань забезпечення кібербезпеки.

Рекомендації підготовано в рамках реалізації програми «Сприяння Інтернет свободі в Україні» організації American Bar Association Rule of Law Initiative.
Контакти:
yaropolk.brynykh@abaroli.org
+38-063-241-20-87