УДК / UDC 351.746.1:34:004
DOI: https://doi.org/10.37750/2616-6798.2026.2(57).364411

Іван Михайлович Доронін
Державна наукова установа "Інститут інформації, безпеки і права Національної академії правових наук України"
Київ, Україна
ORCID: https://orcid.org/0000-0002-5991-6713

СПРИЙНЯТТЯ ТЕХНОЛОГІЙ В ІНФОРМАЦІЙНУ ЕПОХУ У КОНТЕКСТІ ПРАВА ТА БЕЗПЕКИ

Анотація. *У статті розглядається питання розуміння технологій, у першу чергу, інформаційних, які мають окремі властивості потенційно здатні змінювати характер суспільних відносин, що впливає на регулятори таких відносин. Ці технології, що відомі під узагальнюючою назвою "емерджентних", здатні раптово і стрибкоподібно змінювати характер суспільних відносин. Водночас загалом інформаційні технології змінюють і характер загроз у сфері національної безпеки. Правова регламентація у сфері національної безпеки в Україні відбувається традиційним шляхом, що означає і певне відставання від розвитку технологій та пов'язаних змін у суспільних відносинах. За таких умов необхідно вжиття заходів щодо належної правової регламентації у контексті забезпечення безпеки, що має вважатися основною ціллю зазначеної регламентації. У статті визначено окремі проблемні моменти та звернуто увагу на зміни у характері загроз при використання заходів іноземного впливу та маніпуляцій. Наведено конкретні приклади та запропоновано шляхи реагування.*

Ключові слова: *технології, емерджентні технології, правове регулювання, національна безпека, інформаційна безпека, інформаційна політика, іноземний інформаційний вплив, дезінформація.*

Ivan M. Doronin
State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"
Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-5991-6713

PERCEPTION OF TECHNOLOGIES IN THE INFORMATION AGE IN THE CONTEXT OF LAW AND SECURITY

Summary. *This paper examines the conceptual understanding of technologies—primarily information technologies — possessing distinct characteristics that are potentially capable of altering the nature of social relations, thereby impacting the mechanisms of their regulation. These technologies, collectively known as "emergent technologies," are characterized by their ability to induce sudden and non-linear shifts in social dynamics. Concurrently, information technologies as a whole are transforming the landscape of national security threats. In Ukraine, legal regulation within the national security sector follows a traditional trajectory, resulting in a lag behind technological advancements and the corresponding shifts in social relations. Given these circumstances, it is imperative to implement measures for appropriate legal regulation (codification) within the context of security, which must be regarded as the primary objective of such regulation. This article identifies specific problematic issues and highlights the changing nature of threats associated with foreign*

influence operations and manipulation (FIMI). Concrete examples are provided, alongside proposed strategic responses.

Keywords: *technology, emergent technologies, legal regulation, national security, information security, information policy, foreign information influence, FIMI, disinformation.*

Постановка проблеми. Вплив тих чи інших технологій на розвиток суспільства має давню історію і досліджувався науковцями різних галузей під багатоманітними кутами зору. Зрозуміло, що деякі з комунікативних технологій, наприклад, письмо чи типографський друк змінювали хід людського розвитку на сторіччя вперед. Особливо це помітно в інформаційних технологіях, у першу чергу технологіях емерджентного характеру (або ж емерджентних технологіях) [1].

Загалом емерджентними технологіями визнаються такі технології, що виникають як поєднання (синергія) існуючих технологій, при цьому така синергія забезпечує нові властивості (можливості), що не були властиві окремим технологіям, як компонентам такої синергії. Зазначене поєднання зумовлює особливий характер трансформації. При цьому емерджентні технології розглядаються також і у соціальному аспекті. У контексті питань правового регулювання відповідних суспільних відносин під "емерджентною технологією" слід розуміти таку технологію, що є радикально новою, швидкозростаючою, узгодженою з існуючими технологіями, яка при цьому здійснює значний вплив на суспільне життя у різноманітних сферах, які неможливо передбачити наперед унаслідок вказаної вище синергії [2, с. 47]. Тобто синергія окремих технологій і стрибкоподібний характер її розвитку зумовлює наперед непередбачуваний наслідок.

У науковій літературі проблеми технологій розглядались у контексті інноваційних технологій [3], інформаційних технологій загалом [4-6] та окремих технологій у цій сфері [7-9], у тому числі тих технологій, які докорінно змінюють характер розвитку суспільства і можуть бути виокремлені або ж охарактеризовані як окремий клас технологій [10].

Слід зауважити, що певні технології за останні десять років мали значний вплив не тільки на суспільні відносини, а і на науковий пошук, зокрема час від часу підіймаючи питання про зміни у парадигмі правового регулювання та сприйняття права як суспільного регулятора. У цьому контексті особливу увагу викликають технології блокчейну [11], віртуальної чи доповненої реальності, а також певна сукупність технологій, що розглядаються у проблемному полі права інформаційних технологій (IT права) [12].

Вище наведені приклади окремих технологій можуть вважатись "емерджентними технологіями", при цьому їх виникнення, що є синергією існуючих, і подальший розвиток може розглядатись як стрибкоподібний, а суспільний відголос як ажіотажний (hype) і часом хаотичний.

Враховуючи визначений таким чином стан речей, можливо констатувати, що такі технології мають значний вплив на розвиток суспільства, їм притаманна низка властивостей, їх значення та розвиток непередбачувані, а суспільний ажіотаж доволі часто ускладнює їх сприйняття у традиційному праві та відповідно – правовій науці. До того ж особливий характер таких технологій дозволяє у деяких випадках і поставити питання про зміну парадигми правового регулювання або ж трансформації права чи введенні нового регулятора (форм регуляції).

На нашу думку проблематика технологічного впливу та загроз від технологій в інформаційній сфері потребуватиме напрацювання відповідних підходів з позицій правової науки. Намагання точкової регламентації окремих технологій або окремих

проявів застосування цих технологій, як правило, характеризується обмеженим ефектом, оскільки доволі складно розглянути багатоаспектне явище в межах обмеженого кола. Інші підходи, що розглядають проблему на рівні парадигми, або в ширшому аспекті, заслуговують на увагу, але на сьогодні іноді видаються надто футуристичними. Водночас безпекові проблеми технологій, що виникають, часто-густо зумовлюють хаотичне реагування регуляторів, що лише посилює синергію і зменшує передбачуваність регулювання.

Результати аналізу наукових досліджень. Безумовно, проблематика використання новітніх технологій в інформаційній сфері перебуває в полі зору науковців, чому свідченням численні публікації з цього приводу в літературі. При цьому увага науковців зосереджена як на дослідженні суті технологічного впливу так і конкретних технологій, що широко використовуються в інформаційній сфері. Слід також зазначити, що технологічний вплив і застосування технологій та їх впливу на суспільні відносини розглядається і у межах відповідних галузей права. У цьому аспекті варто виокремити цікаві і ґрунтовні дослідження низки науковців у галузі інформаційного права, зокрема, О. А. Баранова, К. І. Бєлякова, В. М. Брижка, О. В. Гладківської, Р. А. Калюжного, А. І. Марущака, В. М. Фурашева, К. В. Юдкової та інших. В аспекті новітніх галузей насамперед інноваційного права та права інформаційних технологій зазначені питання досліджувались С. В. Глібком, О. Е. Сімсон, А. В. Стріжковою та іншими. У цій статті розвинуто окремі положення, започатковані автором при визначенні проблемного поля для правової науки у межах розвитку емерджентних технологій та їх впливу на право і безпеку [2, 11].

Мета статті полягає у проведенні аналізу, дослідженні проблеми впливу технологій на право як регулятор та на стан безпеки, напрацюванні відповідних рекомендацій щодо подальших наукових досліджень, у першу чергу через призму проблематики інформаційної безпеки в умовах зміни характеру загроз сучасного світу (в першу чергу щодо іноземного впливу).

Виклад основного матеріалу. Питання технологій у контексті права розглядались тривалий час в основному з позицій науки цивільного права або ж кримінального права та окремих допоміжних дисциплін у відповідному контексті. У цивільному праві ця проблематика безумовно була пов’язана з правом інтелектуальної власності. Розгляд права інтелектуальної власності у межах цивільного права автором вжито лише в історичному контексті, а питання їх співвідношення є предметом окремої наукової дискусії, що перебуває за межами кола, визначеного метою цієї статті. У кримінальному праві особливості використання технологій розглядались в аспекті дослідження злочинів або ж їх розкриття у криміналістиці. Лише виникнення та розвиток технологій, які автором було свого часу віднесено до емерджентних, значно змінило кут розгляду цієї проблематики.

Емерджентні технології змінюють сам ландшафт суспільних відносин. Водночас такий вплив завжди неможливо передбачити як глобально так і у певних аспектах. Якщо брати до уваги суспільні відносини з приводу технологій з точки зору права, то галузевий розподіл права зумовлює і формування відповідного кута зору для розгляду. Тобто цивільне чи кримінальне право розглядають конкретні виклики та випадки у межах власних правових інститутів [6, 10, 14, 15]. Якщо ж вирізняти напрями права як напрями професійної спеціалізації, то на перше місце виходить сама технологія, що впливає на певні суспільні відносини, які потребуватимуть регулювання саме правом. У таких випадках певний сформований сегмент суспільних відносин викликає формування і певного сегменту права як регулятора. Так, розвиток телекомунікаційних технологій

зумовив появу медійного права або права комунікаційних технологій. У випадку права саме інформаційних технологій (ІТ-право та аналогічні терміни) мова йшла про певні практичні питання – інтелектуальна власність (точніше трансформація умов для застосування права), “прайвасі” та захист персональних даних, кіберзлочинність, регуляторна політика державних органів та особливості її врахування в економічній діяльності, електронна комерція у різних проявах та трансформація засобів масової інформації і розповсюдження інформації взагалі.

Якщо повернутись до емерджентних технологій, то неважко відзначити, що сам перелік практичних питань та викликів доволі непередбачуваний. Спершу треба визначити, що термінологічно варто повернутись до загального терміну “технології” дещо відійшовши від термінології “інформаційні технології” (ІТ) попри його усталеність. В інформаційну епоху майже всі технології є інформаційними, а щодо технологій традиційних інформаційна складова зумовлена поєднанням технологій між собою як прояв емерджентності. У цьому аспекті показовою є еволюція безпілотних літальних апаратів та безекіпажних морських суден, оскільки технологічну спроможність для їх існування забезпечили саме сучасні інформаційні технології управління та геолокації.

Розгляд зазначеної проблеми дозволяє сформулювати певне проблемне поле для дослідження, що полягає у визначенні суті емерджентності, реальних та потенційних загроз для безпеки відповідних суб’єктів, особливостей регулювання та регуляторів, застосування права та пошук відповідних нетрадиційних механізмів правового регулювання. На сьогодні неможливо чітко встановити перелік таких технологій, тому властивості емерджентності будуть розглядатись на конкретних прикладах у цій статті.

Оскільки під емерджентною технологією ми розуміємо технологію, що є радикально новою, швидкозростаючою, узгодженою з існуючими технологіями, яка при цьому здійснює значний вплив на суспільне життя у різноманітних сферах, які неможливо передбачити наперед [2, с. 44] варто розглянути окремі її властивості. Радикальність і новизна полягає в очевидному факті, що зазначене технологія є значно новою порівняно з існуючою. Швидкість її зростання є доволі складним фактором, проте у сучасних умовах вона вимірюється днями та місяцями. Зрозуміло, що такий зріст може прискорюватись і уповільнюватись, але загальна швидкість є невід’ємним фактором. Так симбіоз деяких технологій може прискорювати швидкість зростання основної технології прикладом чого є поєднання доповненої реальності зі штучним інтелектом. Вплив на суспільне життя може бути очевидним та неочевидним. Так у випадку технології штучного інтелекту очевидним є продукт chat-GPT, де технологія стала доступна у режимі чату. Але у випадку програмування із застосуванням специфічних продуктів тієї ж технології (LLM від Anthropic) вплив значний але не настільки очевидний на перший погляд.

У документах стратегічного планування з безпеки емерджентні технології часто розглядаються разом із “проривними (чи підривними) технологіями” (disruptive). Цей термін є умовним і не завжди означає шкідливу за умовами створення технологію. Більш того, їхня “підривна” сутність далеко не завжди вживається у негативному контексті. Загалом це технологія, яка змінює цінності на ринку, коли з’являється, оскільки ігнорує традиційні параметри конкуренції. Як правило, це відбувається, коли з’являється комерційний продукт, що побудований на базі певної інновації (винаходу), який знаходить споживача і його цінність для споживача перевищує традиційні продукти на ринку. Прикладом цього є наприклад цифрова фотографія, що витіснила плівкову для широкого споживача, поховавши цілу індустрію традиційної обробки

фотознімків. В історичному контексті згадують електролампи замість інших джерел освітлення (свічки, гасові лампи та інше), пароплави замість вітрильників. Але якщо раніше заміщення проводилось десятиріччями або роками, то зараз заміщення можливо значно швидше. Достатньо прослідкувати еволюцію засобів зв'язку або форматів з'єднання апаратури.

У даному разі, якщо розглядати правові проблеми технологій, то безпосередня регуляція не відбувається. Право, як регулятор, вступає у двох основних випадках. У першому випадку мова йде про неспроможність регуляції традиційним шляхом. У другому випадку у правовій формі відбувається регуляторна активність держави у випадку реальних та потенційних небезпек чи загроз. Зрозуміло, що характер таких загроз також є непередбачуваним. Тобто якщо, наприклад, Білл Гейтс ще у 1990ті роки передбачав смерть формату компакт-дисків із розширенням спроможності глобальних мереж для передачі даних, то проривною технологією була не сама по собі технологія алгоритмів обробки звуку, а закладена від самого початку можливість копіювання файлу, що закладена в архітектуру файлових та операційних систем. Саме вона разом з алгоритмами обробки та компресії дозволила вільне копіювання та розповсюдження. Поєднання ж цих технологій із супутніми повністю змінило ринок музичних творів.

Якщо ж оцінювати технології в аспекті загроз, то необхідно звернути увагу на низку факторів.

По-перше, практично будь-яка технологія може використовуватись зі злочинною метою і такі намагання відбуваються відразу. Емерджентна технологія або ж синтез таких технологій з технологіями проривними, відразу створює кримінальні загрози підвищеної небезпеки причому в діаметрально протилежних сферах. Прикладом є технологія 3D друку. Окремі намагання використати її для виробництва вогнепальної зброї не мали широкого розповсюдження внаслідок низької якості через брак матеріалів. Тому вироблені продукти неможливо використовувати у військових цілях. Водночас вона дала змогу виготовляти "ghost gun" [16] тобто окремі частини зброї, що у комплексі, будучи зібраними, дозволяють виробити пристрій, здатний зробити декілька пострілів. Ці зразки також не підлягають криміналістичній ідентифікації внаслідок технічного знищення каналів стволу при пострілах. Звичайно, що з точки зору закону вони є класичним зразком незареєстрованої зброї, яку неможливо відслідкувати та ідентифікувати. Ця ж сама технологія практично дала нове дихання фальсифікації предметів антикваріату та шахрайству з ними, причому в промислових масштабах.

Враховуючи сучасний стан речей, варто звернути увагу насамперед на технологічних загрозах в інформаційній сфері, і насамперед у контексті національної безпеки.

Взагалі визначення суті, переліку та характеру таких загроз в Україні здійснюється відповідно до спеціального законодавства у сфері національної безпеки. Так, Закон України "Про основи національної безпеки України", що діяв протягом 2003-2018 років, визначав наступний підхід. Визначались конкретні види загроз в інформаційній сфері, до яких законодавцем було віднесено:

- прояви обмеження свободи слова та доступу громадян до інформації;
- поширення засобами масової інформації культу насильства, жорстокості, порнографії;
- комп'ютерна злочинність та комп'ютерний тероризм;
- розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Якщо проаналізувати зміст дефініції таких загроз, викладеної у ст. 7 зазначеного Закону, то можливо стверджувати, що самі загрози визначені чітко і прагматично. При цьому варто також загадати, що початкова редакція Закону України "Про основи національної безпеки України" визначала і низку загроз у науково-технологічній сфері. Зокрема мова йшла про "наростаюче науково-технологічне відставання України від розвинутих країн"; "неефективність державної інноваційної політики, механізмів стимулювання інноваційної діяльності", "низьку конкурентоспроможність продукції", "нерозвиненість внутрішнього ринку високотехнологічної продукції та відсутність його ефективного захисту від іноземної технічної і технологічної експансії"; "зниження внутрішнього попиту на підготовку науково-технічних кадрів для наукових, конструкторських, технологічних установ та високотехнологічних підприємств, незадовільний рівень оплати науково-технічної праці, падіння її престижу, недосконаліть механізмів захисту прав інтелектуальної власності", а також відплив учених, фахівців, кваліфікованої робочої сили за межі України. Ця сукупність загроз мала безпосередній вплив і на стан розвитку сучасних технологій як в реальному часі так і у найближчій перспективі.

Водночас стратегічне планування державної політики у відповідних сферах мало відбуватись і з урахуванням основних напрямів, визначених у тому ж Законі. Так, в інформаційній сфері такі напрями було визначено, щоправда деякі з них носили занадто аморфний характер. Прикладом чому є такий напрям як "активне залучення засобів масової інформації до боротьби з корупцією, зловживаннями службовим становищем, іншими явищами, які загрожують національній безпеці України". На виконання відповідних визначених напрямів мало відбуватись і стратегічне планування у відповідній сфері. Водночас з самого початку таке планування відбувалось шляхом схвалення Стратегії національної безпеки України, що за сенсом державного планування мало втілювати основні напрями державної політики нового обраного Президента України.

За час дії зазначеного законодавчого акту було ухвалено декілька Стратегій (точніше редакцій). Зокрема, варто порівняти Стратегію національної безпеки в редакції Указу Президента України від 12 лютого 2007 року № 105/2007 (Президент В. Ющенко) та від 8 червня 2012 року № 389/2012 (В. Янукович). В обох випадках заходи в інформаційній сфері були ідентичними, хоча і викладались по-різному (у другому випадку в окремому п. 4.3.8). До них належали заходи із стимулювання впровадження новітніх інформаційних технологій і виробництва конкурентоспроможного національного інформаційного продукту (у тому числі і сучасних систем захисту інформаційних ресурсів), забезпечення безпеки найбільш важливих інформаційно-телекомунікаційних систем у критичних сферах, розробка та впровадження національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із відповідними стандартами держав - членів ЄС, у тому числі згідно з вимогами Конвенції про кіберзлочинність, а також створення національної системи кібербезпеки. Кожний блок заходів зумовлював вироблення і реалізацію відповідної державної політики згідно із компетенцією державних органів. Не вдаючись до занурення у питання державного управління та публічного адміністрування можливо лише зазначити, що практика зумовила необхідність значного оновлення у подальшому спеціального законодавства насамперед стосовно кібербезпеки.

Стратегія національної безпеки, затверджена Указом Президента України від 26 травня 2015 року № 287/2015, виокремила у відповідні блоки загрози і напрями державної політики в інформаційній сфері та сфері кібербезпеки, при цьому в першому випадку було констатовано доволі різке зменшення загроз, які автори Стратегії вважали актуальними. Мова йшла лише про ведення інформаційної війни проти України та відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства (п 3.6 Стратегії), а у сфері кібербезпеки та безпеки інформаційних ресурсів - уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак та фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом (п. 3.7 Стратегії). Звертає на себе увагу і фактичне вилучення загроз у науково-технічній сфері з числа актуальних. У даному випадку такий підхід видається занадто спрощеним оскільки інформаційні безпека була зведена лише до інформаційної війни. Водночас у подальшому саме питанням інформаційної безпеки було присвячено Доктрину інформаційної безпеки.

Зазначена Доктрина була затверджена Указом Президента України від 25 лютого 2017 року № 47/2017. Цей документ є більш вузько спрямованим за сферою застосування. Водночас характеристика загроз, визначена у Доктрині, практично більш докладно розкриває загальні загрози у цій сфері, визначені у Стратегії національної безпеки. Так, до числа безпосередніх загроз двічі віднесено спеціальні інформаційні операції (СІО) противника в Україні та в інших країнах на шкоду інтересам України, інформаційна експансія, інформаційне домінування держави-агресора. Разом із тим, інші аспекти, насамперед глобального характеру і технологічний вплив у цій сфері залишились поза увагою. Зрозуміло, що констатована "недостатня розвиненість національної інформаційної інфраструктури" може бути сприйнята і як недосконаліть суверенітету в сфері інформаційних технологій, але загрози були констатовані лише у загальних рисах.

Термінове оновлення законодавства у сфері національної безпеки, що відбулось уже наступного року шляхом ухвалення нового спеціального базового законодавчого акту – Закону України "Про національну безпеку України" змінило підходи у стратегічному плануванні оскільки загрози і напрями державної політики щодо нейтралізації та протидії загрозам мають визначатись у відповідних документах стратегічного планування. У чинній Стратегії національної безпеки України, затвердженій Указом Президента України від 14 вересня 2020 року № 392/2020, загрози в інформаційній сфері визначено як вивідні від інформаційної війни (ІПО, деструктивна пропаганда тощо), при цьому констатовані і загрози технологічного характеру. Водночас визначено як і конкретні напрями протидії, так і необхідність розробки Національної системи стійкості, що має передбачати оцінку ризиків, своєчасну ідентифікацію загроз і визначення вразливостей.

Національна система стійкості впроваджена Указом Президента України від 27 вересня 2021 року № 479/2021. Її Концепція передбачає низку базових елементів, зокрема захищеність та безперебійне функціонування інформаційних та комунікаційних послуг, суспільну стійкість, зокрема, до інформаційних впливів та деякі інші. У загальному вигляді відповідні блоки мають забезпечувати нормальне функціонування держави як суспільної організації та її органів у будь-яких умовах.

Таким чином питання реагування не негативний вплив окремих технологій розглядаються у межах відповідних існуючих концептів в управлінні – концепті "національної безпеки" і "національної стійкості". Слід зазначити, що потенціальний негативний вплив технологій на суспільні відносини, суспільство і державу, як

соціальну організацію, як правило є неможливим для прогнозування. Попри на певну дискусію стосовно існування чи заперечення існування технологічної нейтральності [17-21] варто зазначити, що реальна чи вдавана нейтральність технології не виключає її емерджентний розвиток.

Якщо ж розглядати застосування та розвиток емерджентних технологій з точки зору обсягів регуляторного впливу держави, то звичайно у випадках глобальних інформаційно-комунікативних мереж він є обмеженим. Підхід щодо застосування національного (або наднаціонального на прикладі ЄС) законодавства до корпорацій, що є власниками відповідних технологій або відповідають зі її застосування, далеко не повною мірою досягає мети такого впливу.

Зазначений тезис варто розглянути в аспекті відповідної загрози і напрямів державного регуляторного впливу. Так мінімізація негативного впливу розглядається в основному з позицій забезпечення безпеки, а, як відомо, у межах концепту "національної безпеки" здійснюється регуляторний вплив у досить великому обсязі сфер соціального життя. Оскільки передбачається заборона на заподіяння шкоди та ефективне і швидке відшкодування, то з точки зору теорії права мова йде про юридичну відповідальність. З іншого боку мова йде про виокремлення відповідних повноважень для державних органів та встановлення меж їх застосування.

Певна невдача із застосуванням заходів протидії дезінформації в країнах ЄС останнім часом має декілька причин, і технології – одна з них. Зміна підходів зумовила і необхідність іншого розуміння природи явища "дезінформації". Так це явище не може розглядатись фрагментарно оскільки є лише методом, що обирає виконавець в межах певної стратегії, зумовленою реалізацією відповідних настанов глобального характеру. Тому практично завжди дезінформація у сучасному світі є проявом політики іноземного впливу (Foreign Information Manipulation and Interference (FIMI), "іноземне інформаційне маніпулювання та втручання"). Сам термін доволі складним і передбачає у загальному вигляді певну модель поведінки (яка в основному не порушує вимоги законодавства), що загрожує або ж може негативно вплинути на цінності процедури та політичні процеси. Зазначена діяльність носить маніпулятивний характер, здійснюється навмисно та скоординовано [22]. При цьому така діяльність має ціль, шо відповідає цілям державної політики або стратегічним цілям суб'єкта, який її проводить, але може здійснюватися доволі складним шляхом, наприклад при реалізації концепції рефлексивного управління [23]. За таких обставин країни-члени ЄС перейшли від традиційних заходів обмеження інформації та контр-пропаганди до формування ефективної інформаційної політики в умовах поширення дезінформації, як складової політики протидії FIMI. Тривалий час базовим документом у цій сфері був та є Кодекс діяльності при дезінформації *(Code of Conduct on Disinformation)*, що встановлює напрями державної політики в умовах поширення дезінформації та іншого зловживання і перекручування інформації в інформаційно-комунікаційних мережах.

Цей Кодекс є складовою Керівництва зі зміцнення ЄС, що також включає *Плани заходів з комунікації та зміцнення демократії в ЄС, боротьби з дезінформаційним впливом в онлайн-комунікаціях, а також інших планів та керівництва ЄС в інформаційній сфері.* Ці документи ухвалені на виконання завдання реагування на розповсюдження дезінформації, "мізінформації" (розповсюдження хибної інформації без наміру ввести в оману), операцій інформаційного впливу, а також зовнішнього (іноземного) втручання в інформаційній сфері.

Кодексом визначено окремі напрями зусиль, що мають спрямовуватися на: "позбавлення фінансування" (демонетізація, дефінансування) розповсюджувачів хибної

інформації; встановлення обмежень в рекламній сфері; кооперація та сприяння "добросовісним" учасникам; встановлення нагляду щодо ведення політичних та виборчих кампаній, зокрема, щодо фінансування розповсюдження та виробництва інформації, яка використовується у ході таких кампаній; "прозорість" (повна деанонімізація) виробників та розповсюджувачів інформації, яка використовується у ході політичних та виборчих кампаній, вжиття чітких заходів щодо встановлення справжніх джерел надходження інформації; регламентація обмежень та технічних заходів закриття програмних продуктів, що використовуються в політичних цілях; координація технічних заходів регулювання в інформаційній сфері.

Слід зазначити, що вище наведені заходи стосувались фактично лише одного методу або способу FIMI. При цьому саме явище впливу мало зумовити і зміну підходів у плануванні державної політики у цій сфері. У загальному вигляді FIMI є продовженням зовнішньої політики держава (іншого глобального суб'єкта) для досягнення відповідних стратегічних цілей. Зокрема, в 4 звіті щодо FIMI Європейської служби зовнішніх справ (4th EEAS Report on Foreign Information Manipulation and Interference Threats, березень 2026 року) констатовано новітні тенденції щодо проявів FIMI і акцентовано увагу на одночасне застосування політичних акцій, розвідувально-підривної активності, військових заходів (у т. ч. демонстративного характеру), розповсюдження хаосу і т. ін. Слід зауважити, що традиційними способами впливу щодо інформації при проведенні операцій та окремих заходів у межах політики FIMI є "спотворення інформації" (distorting information). "Спотворення" треба розуміти як поняття широке. При цьому той же Звіт характеризує значний вплив на заходи у межах FIMI сучасних технологій, при цьому зі значною варіативністю саме останнього року. існуючі моделі дозволяють кратно збільшити генерацію інформації та швидкість каналів розповсюдження, що дозволяє досягти цілей перевантаження каналів особливо коли проводяться акції "збурення" або "хаосу". Окрім цього, значною проблемою є "грумінг" систем штучного інтелекту (великих мовних моделей, LLM), що полягає у спотворенні процесу навчання моделей шляхом навмисного розповсюдження великої кількості інформації у вигляді, розрахованому лише на навчання LLM [25, 26]. При цьому мова йде не тільки про класичну політичну пропаганду, але про складні випадки розповсюдження хибних знань, теорій змов, упереджених висновків, і т. ін. При цьому сам вплив технології штучного інтелекту у вигляді LLM (як чат-боти так і AI-агенти чи системи генерації) непередбачений внаслідок недоліків технологій.

Таким чином, розглянуте вище дозволяє сформулювати низку **висновків.**

1. Розвиток сучасних технологій зайвий раз підтверджує загальний висновок, що їх використання змінює сам характер суспільних відносин. Така зміна відбувається раптово, стрибкоподібно і передбачати як сам розвиток так і особливості зміни відносин неможливо. Регулювання відносин відстає від цих змін і зазвичай є додатковим фактором впливу, що змінює як сам характер відносин так і їхні властивості.

2. Емерджентні технології останнього часу яскраво підкреслюють зазначене і дають відповідні приклади, що додатково ілюструють непередбачуваність впливу таких технологій. Певні особливості технологій можуть використовуватись у деструктивних цілях як навмисно так і іншим шляхом. Інші особливості технологій здатні мати негативний вплив внаслідок самої суті технології.

3. Загрози у сфері національної безпеки модифікуються як внаслідок використання емерджентних технологій з руйнівною чи підривною метою так і внаслідок непередбачуваності їхнього розвитку. Реагування у відповідних сферах відбувається із значним запізненням.

4. Правове забезпечення у сфері національної безпеки включає проблематику інформаційної безпеки водночас питання національної безпеки у науково-технологічній сфері та сфері інформаційних технологій останнім часом залишались здебільшого поза увагою законодавця.

ПОДЯКИ: Немає.

КОНФЛІКТ ІНТЕРЕСІВ: Немає.

Використана література

1. Rotolo Daniele, Hicks Diana, Martin Ben R. What Is Emerging Technology? Working Paper of Science Policy Research Unit. University of Sussex. Feb., 2015. 46 p. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2743186

2. Доронін І.М. Розвиток емерджентних (новітніх) технологій та регулювання у цій сфері як реалізація функцій держави. *Інформація і право.* 2017. № 4. С. 41-48.

3. Правове забезпечення інноваційного процесу в умовах адаптації законодавства України до законодавства Європейського Союзу: монографія / [С. В. Глібко, О. В. Розгон, Ю.В. Георгієвський та ін.]; за ред. С. В. Глібка, О. В. Розгон. – Харків: НДІ прав. забезп. інновац. розвитку НАПрН України, 2022. 290 с.

4. Баранов О. Система принципів інформаційного права. *Правова інформатика.* 2006. № 2. С. 5-15.

5. Юдкова К.В. Особливості визначення поняття «інформаційні технології». *Інформація і право.* 2015. № 1. С. 63-67.

6. Стефанчук Р. О. Інформаційні технології та право: quo vadis? *Право України*. 2018. № 1. С. 30-50.

7. Бєляков К.І. Інформаційна діяльність: зміст та підходи до класифікації. *Інформація і право.* 2012. № 1. С. 63-69.

8. Баранов О.А. «Інтернет речей» як правовий термін. *Юридична Україна.* 2016. № 5-6. С. 96-103.

9. Стріжкова А.В. Правове регулювання в ЄС похідних від GRID інноваційних технологій. *Право та інновації.* 2017. № 1. С. 34-40.

10. Мандрика Л.М., Даниленко О.В. Проривні цифрові технології як засадничі фактори трансформації цивільного права України. Вісник Національної академії правових наук України. 2025. № 1. С. 164-190. DOI: 10.31359/1993-0909-2025-32-1 -164.

11. Доронін І.М. Блокчейн, суспільство і держава: проблеми правотворчості. ІТ-право: проблеми та перспективи розвитку в Україні: зб. матер. ІІ Міжнар. наук.-практ. конф.(м. Львів, 17 листоп. 2017 р.). Львів: НУ «Львівська політехніка. 2017. С. 73-78.

12. Сімсон О. ІТ-право V. Інформаційного права: на зламі епох ІТ-право: проблеми та перспективи розвитку в Україні: зб. матер. ІІ Міжнар. наук.-практ. конф.(м. Львів, 17 листоп. 2017 р.). Львів: НУ «Львівська політехніка. 2017. С. 180-187.

13. Wiener Jonathan. The regulation of technology, and the technology of regulation. *Technology in Society.* Vol. 26, Issues 2–3, April–August 2004, P. 483-500. URL: https://doi.org/10.1016/j.techsoc.2004.01.033.

14. Карчевський М.В. Основні проблеми кримінально-правового регулювання у сфері інформатизації // *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка*. 2017. Вип. 3. С. 67-78.

15. Радутний О.Е. Право та окремі аспекти світу атомів і бітів (робототехніка, штучний інтелект, цифрова людина) // *Питання боротьби зі злочинністю.* 2021. Вип. 41. С. 13-28.

16. Dass, R. 3D-Printed Firearms: Global Proliferation Trends and Analyses. *Studies in Conflict & Terrorism*, 1–35. https://doi.org/10.1080/1057610X.2025.2477849

17. Баранов О.А. Інтернет речей (IoT): мета застосування та правові проблеми // *Інформація і право.* 2018. № 2 (25). С. 31-44.

18. Акулов Ю.В. Принципи державного управління у сфері цифрових інновацій та AI-розробок *Академічні візії.* 2024. Вип. 36. С. 1-7. https://doi.org/10.5281/zenodo.14186657

19. Стиранка М.Б. Онтологія становлення цифрового права як галузі права // *Правові новели.* 2024. № 23. С. 542-546. https://doi.org/10.32782/ln.2024.23.73

20. Зінич Л.В. Принцип технологічної нейтральності як регуляторний імператив у сфері захисту прав інтелектуальної власності *Pravo.UA.* 2025. № 4. С. 41-46. https://doi.org/10.71404/LAW.UA.2025.4.7

21. Shadikhodjaev S. Technological Neutrality and Regulation of Digital Trade: How Far Can We Go? *The European Journal of International Law.* 2021. Vol. 32 no. 4. P. 1221–1248.

22. Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI). European External Action Service. 17.03.2026. URL: https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

23. Lopes, J.R.D.C.C. The Russian Reflective Control: Theory and Military Applications. *Communications*. 2025, *12*(1), P. 11-23. doi: 10.11648/j.com.20251201.12

24. Prosser E., Edwards M. Helpful or Harmful? Exploring the Efficacy of Large Language Models for Online Grooming Prevention. *Computer Science/Cryptography and Security. 14/03/2024.* arXiv:2403.09795

25. Danet, Didier, LLM Grooming: A New Cognitive Threat to Generative AI (September 09, 2025). Available at SSRN: https://ssrn.com/abstract=5461315; http://dx.doi.org/10.2139/ssrn.5461315

Іван Михайлович Доронін
доктор юридичних наук, доцент
керівник наукового центру Державної наукової установи "Інститут інформації, безпеки і права Національної академії правових наук України"
04053, Україна, м. Київ, пров. Несторівський, 4
email: inive7777@gmail.com

Ivan M. Doronin
Doctor of Juridical Sciences, Associate Professor
Head of the Scientific Research Center of the State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine"
4 Nestorivskyi Lane, Kyiv, 04053, Ukraine
email: inive7777@gmail.com

Рекомендоване цитування: Доронін І.М. Сприйняття технологій в інформаційну епоху у контексті права та безпеки. *Інформація і право.* № 2(57)/2026. 2026. С. 130-140. https://doi.org/10.37750/2616-6798.2026.2(57).364411

Suggested Citation: Doronin I. (2026) Perception of Technologies in the Information Age in the Context of Law and Security. *Information and Law*. 2(57)/2026. 130-140. https://doi.org/10.37750/2616-6798.2026.2(57).364411

Дата надходження статті до редакції: 13.05.2026 р.
Дата прийняття статті до друку після рецензування: 20.05.2026 р.
Дата публікації (оприлюднення): 26.05.2026 р.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~