

3. Стратегічний план на 2016–2018 pp. Офіс Прокурора МКС. 2015. Ст. 23. URL: https://www.icc-cpi.int/iccdocs/otp/en-otp_strategic_plan_2016-2018.pdf
4. Стратегічний план на 2016–2018 pp. Офіс Прокурора МКС. 2015. Ст. 45. URL: https://www.icc-cpi.int/iccdocs/otp/en-otp_strategic_plan_2016-2018.pdf
5. Стратегічний план на 2019–2021 pp. Офіс Прокурора МКС. 2019. URL: <https://www.icc-cpi.int/itemsDocuments/20190717-icc-strategic-plan-eng.pdf>
6. Prosecutor v Akayesu (judgment). ICTR-96-4-T. International Criminal Tribunal for Rwanda Arusha. Arusha, Tanzania. 2001. URL: http://www.worldcourts.com/icttr/eng/decisions/2001.06.01_Prosecutor_v_Akayesu.pdf
7. William A. Schabas. The International Criminal Court: A Commentary on the Rome Statute (Oxford Commentaries on International Law). 2nd Edition Oxford University Press. 2016. 1408 pages.
8. Draft Code of Crimes against the Peace and Security of Mankind with commentaries. International law commission. Yearbook of the International Law Commission. Part Two. Para 161996. URL: https://legal.un.org/ilc/texts/instruments/english/commentaries/7_4_1996.pdf
9. Raphael Cohen-Almagor. Confronting the Internet's Dark Side: Moral and Social Responsibility on the Free Highway. Woodrow Wilson Center Press and Cambridge University Press ISBN: 9781107105591. 2015. P. 303–304. URL: https://www.researchgate.net/publication/279175966_Confronting_the_Internet%27s_Dark_Side_Moral_and_Social_Responsibility_on_the_Free_Highway, UNODC. The use of the Internet for terrorist purposes. United Nations. 2012. 350 p. URL: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf
10. Bigos O. Jurisdiction over cross – border wrongs on the internet. International and comparative law quarterly. 2005. 592 p.

Ключові слова: юрисдикція Міжнародного кримінального суду, злочини проти людяності, Римський статут, злочини вчинені за допомогою мережі Інтернет.

Ключевые слова: юрисдикция Международного уголовного суда, преступления против человечности, Римский статут, преступления совершенные с помощью сети Интернет.

Key words: jurisdiction of the International Criminal Court, crimes against humanity, the Rome Statute, crimes committed through the Internet.

РУЛЬОВ ІЛЛЯ МИХАЙЛОВИЧ

*Національний університет «Одеська юридична академія»,
аспірант кафедри міжнародного та європейського права*

ПРІОРИТЕТ ІНТЕРЕСІВ ІТ-КОРПОРАЦІЙ НАД ІНТЕРЕСАМИ ДЕРЖАВИ ЯК ЗАГРОЗА КІБЕРБЕЗПЕЦІ ДЕРЖАВИ

У ХХІ столітті важко уявити наше життя без кіберпростору, навіть державний апарат та взаємодія громадян з державою здійснюються через комп'ютерні системи. Але між громадянином та державою досить часто є посередники якими виступають приватні компанії (корпорації).

Як зазначає І. П. Васильчук, з економічної й правової точки зору корпорація це юридична особа, яка функціонує на основі статуту та згідно з законодавством відповідної країни та належить групі незалежних один від одного фізичних та/або юридичних осіб. При цьому вона не відповідає за зобов'язаннями власників, власність же є відокремленою від управління, яке здійснюється колективними органами, обраними власниками, а також найманими менеджерами, призначеними власниками [1].

У світі сьогоденних тенденцій можна побачити конфліктування корпоративних інтересів з інтересами держави. Такі величезні корпорації як Google та інші мають більш велику владу над інформаційним простором ніж держава. У цьому контексті вважаємо, що треба досліджувати механізми врегулювання відносин держави та корпорацій. Важливим слід виділити те, що більшість корпорацій надають доступ користувачам у разі їх згоди з правилами платформи. Однак, які б не були правила користування платформою, ці правила не можуть йти у супереч з законодавством держав користувачів. В момент створення корпорацією правил платформи стає два питання: 1) яким чином правила платформи йдуть у різнобій з законодавством держави; 2) чи не ставить загрозу державі монополне право регулювання платформ корпораціями. Наприклад, згідно ст. 34 КУ коженній особі гарантується право на свободу думки та слова, на вільне вираження своїх поглядів і переконань, а в свою чергу, правилами платформи заборонено виражати свою думку про певні суспільне явища чи події. Ми розуміємо коли це право може бути обмежено законом в інтересах національної безпеки, територіальної цілісності або громадського порядку, але виникає питання, чи є у приватної компанії право вирішати, що обмежувати, а що ні. На нашу думку це може призвести у майбутньому до порушення конституційного права громадянина на вільне волевиявлення та доступ до інформації.

Уваги потребує також те, що основними інтересами корпорації виступають прибутки, а не безпека громадян. Тому виникає питання, чи не буде корпорація зацікавлена у односторонній подачі інформації користувачу задля забезпечення своїх інтересів. Той факт, що корпорація може відключити будь-якого політика у тому числі навіть президента країни без загрози санкцій з боку держави є нагодою переглянути відношення Інтернет платформ як до соціальних мереж, так і до регулятора інформаційного простору. У свою ж чергу, багато політиків та державних очільників мають зв'язок з громадськістю через платформи та соціальні мережі. Це дозволяє зменшити бюрократичний процес та швидко реагувати на політичні процеси у суспільстві, а також постійно підтримувати зв'язок з громадянами. Питання інформаційної безпеки гостро стає у зв'язку з тим, що обіг інформації у кіберпросторі регулюється ні чинними законами держави, а корпоративними інтересами, спрямованими не стільки на забезпечення прав людини, скільки на матеріальний здобуток. Можна побачити, немає ніяких гарантій, що корпорації у будь-який момент не заблокують доступ любому

державному службовцю доступ до платформи, що, в свою чергу, може призвести до абсолютно неконтрольованого процесу відгродження інформації від користувача, що, в свою чергу, також негативно вплине на кібербезпеку в країні, оскільки цей користувач може бути особою з повноваженнями любого рівня, а це може призвести до соціальної кризи, а навіть і політичної. Це є дуже прикладом того, що наш соціум, не зважаючи на широке використання платформ, ще не зник до соціальних мереж як до важливої частки інформаційного простору. Вважаємо, що треба створити систему стримування та протидії задля можливості держави дати відсіч ІТ-гігантам. Однак зазначимо, що повне блокування не є виходом, оскільки воно не відповідає реальним можливостям держав регулювати Інтернет простір.

Вважаємо доцільним згадати про безпеку монополізації ринку ІТ у світі та можливість при цьому кризи для держав. Згідно оцінки аналітичного агентства Morningstar: 90 відсотків ринку Інтернет пошуку належить Google. а 59 відсотків ринку соціальних мереж Facebook. Це створює ситуацію коли ІТ-гіганти скупують нові ІТ-компанії заважаючи тим самим створювати для себе нових конкурентів. ІТ-гіганти мають також угоди з виробниками мобільних телефонів, операторами зв'язку та Інтернет браузерів щодо встановлення Google як пошукової системи за замовчуванням [2]. Такі дії перешкоджають виникненню конкурентоспроможних ІТ-компаній та створення вітчизняних аналогів Інтернет платформ. У зв'язку з цим держави, які хочуть мати змогу стримувати ІТ-гігантів мають створювати свій ІТ-сегмент. В цьому разі доцільно підтримувати вітчизняні ІТ-розробки, створювати комфортні умови для ІТ-сектору для забезпечення конкурентоспроможних вітчизняних платформ.

Список використаної літератури:

1. Васильчук І. П. Сутність та ознаки корпорацій: теоретичний аспект. [Електронний ресурс]. – Режим доступу: <https://ecj.oa.edu.ua/articles/2013/n23/40.pdf>
2. Мін'юст США і 11 штатів звинуватили Google у монополії [Електронний ресурс]: [Інтернет-портал]. – Електронні дані. Режим доступу: <https://www.dw.com/uk/miniust-ssha-i-11-shtativ-zvynuvatyly-google-u-monopolii/a-55338041>

Ключові слова: інформаційна безпека, інформаційні технології, ІТ-корпорації, ІТ-монополії.

Ключевые слова: информационная безопасность, информационные технологии, ИТ-корпорации, ИТ-монополии.

Key words: information security, information technology, IT corporation, IT monopoly.