з наданням публічних послуг. *Национальный юридический журнал: теория и практика*. Июль, 2017 С. 176-179.
2. Кримінальний процесуальний кодекс України. *Відомості Верховної Ради України (ВВР)*. 2013. № 9-13. Ст. 88. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text.
3. Вирок Вищого антикорупційного суду від 21.09.2021 у справі № 303/1425/18. Єдиний державний реєстр судових рішень. URL https://reyestr.court.gov.ua/Review/99804279.
4. Малюга Р.В. Доказування в кримінальному процесі: проблеми визначення структурних елементів. *Наукові записки Львівського університету бізнесу та права*. 2013. Вип. 11. С. 280–283.
5. Прокурорський нагляд в Україні: підручник для студентів юрид. спеціальностей вищих навч. закладів / І.Є. Марочкін, П.М. Каркач, Ю.М. Грошевой та ін.; за ред. проф. І.Є. Марочкіна, П.М. Каркача. Х.: ТОВ «Одіссей», 2008. 240 с.

ОКРЕМІ ПИТАННЯ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ІННОВАЦІЙНОГО РОЗВИТКУ СУСПІЛЬСТВА

Радзієвська О. Г.
кандидат юридичних наук, старший дослідник,
провідний науковий співробітник
Державної наукової
установи «Інститут інформації, безпеки і права
Національної академії правових наук України»
м. Київ, Україна

Цифровізація суспільних відносин внаслідок активного впровадження нових інформаційних та комунікаційних технологій у життя сучасної людини, збільшення кількості та частоти інформаційних обмінів неминуче призводить до підвищення рівня інформаційної небезпеки у суспільстві. Система забезпечення інформаційної безпеки у державі вимушена постійно модернізуватися, трансформувати власні підходи і механізми протидії інформаційним небезпекам, пристосовуючись під нові виклики глобального інформаційного простору. Правова система держави мусить оперативно реагувати на зміни у суспільстві, які пов’язані із інноваціями та впровадженням нових технологій,

забезпечуючи ефективне правове регулювання суспільних відносин в усіх без виключення сферах.

Будь-яка діяльність сучасного суспільства нерозривно пов'язана з інформацією та інформаційними технологіями, відповідно складова інформаційної безпеки сьогодні є досить значимою у будь-якій сфері. Тоді як загрози в інформаційному просторі стають дедалі масштабними і носять наскрізний характер. Нині, для прикладу, не можна говорити лише про економічну безпеку не торкаючись низки проблем інформаційної безпеки. Зокрема, у питаннях, які пов'язаних з використання нових технологій в економічної діяльності, у здійсненні фінансових транзакцій, а також у сфері обігу та захисту даних. Так само, як не можна вести мову про військову чи національну безпеку оминаючи інформаційні загрози як на державному, так і на міжнародному рівнях.

Особливо гостро сьогодні постають питання правового забезпечення захисту приватності особи та її персональних даних. Наприклад, інноваційні підходи сучасного маркетингу передбачають використання великих даних (BIG DATA) для створення цифрового профілю об'єкта. Автоматично сформовані дані про користувача, його вподобання, інтереси, зібрані методом аналізу його діяльності в мережі, разом з поширеною ним же інформацією про себе, у тому числі фото, відео, становлять живий інтерес для бізнесу, політики, соціальних та комерційних проектів. Ця інформація стає надзвичайно цінним ресурсом знань для будь-якої компанії, у тому числі й для створення персоналізованої (таргетованої) реклами. Постають суттєві питання щодо правомірності автоматичного збирання та використання даних про особу в мережі.

Основною правовою підставою для обробки персональних даних у контексті продажу й просування в Інтернеті є згода суб'єкта персональних даних відповідно до Закону України «Про захист персональних даних» [1]. Відповідно до цього ж Закону для отримання згоди суб'єкта персональних даних на обробку його персональних даних необхідно попередньо повідомити йому про порядок обробки таких даних, зокрема, надати інформацію про володільця персональних даних, склад і зміст зібраних персональних даних, права, мету збору, а також про осіб, яким буде передано персональні дані. При зміні мети обробки персональних даних необхідним є повторне отримання згоди суб'єкта персональних даних на обробку його персональних даних. Однак на практиці надана інформація про порядок обробки персональний даних, зібраних допомогою файлів cookies, є недостатньою, а повторний запит на згоду суб'єкта персональних даних як правило взагалі не здійснюється. Крім того на даний час інформація, зібрана про особу з використанням автоматичних можливостей мережі, офіційно не визнана персональними даними. Тоді як в Європейському Союзі інформація, зібрана з допомогою файлів cookies, вважається персональними даними відповідно до

Загального регламенту щодо захисту даних 2016/679 (GDPR) [2] та Директиви про обробку персональних даних та захист конфіденційності в секторі електронних комунікацій 2002/58/EC (ePrivacy Directive) [3]. Такі роз'яснення були надані за рішенням Суду справедливості Європейського Союзу у справі Vidal-Hall v Google Inc. та у роз'ясненнях European Data Protection Board [4].

Також відкритими залишаються питання правомірності використання персоналізованої (таргетованої) реклами в мережі в аспекті порушення права особи на приватність.

З іншого боку великі дані (BIG DATA) є незамінним інструментом у політичній сфері, яка нині активно використовує сучасні інформаційні технології. Політичні перегони сьогодні перетворюються на інформаційні війни, а політична реклама від головної мети інформування виборця переходить до маніпулювання з інформацією та його свідомістю. Тобто проведення спеціальних інформаційних операцій для отримання політичних переваг сьогодні є реальною загрозою. Підвищення об'єму недостовірної, або викривленої інформації в інформаційному просторі, збільшує кількість негативних та маніпулятивних впливів на свідомість громадян, що порушує його право на захист від маніпулювання свідомістю та від недостовірної інформації, а також ставить під загрозу повноцінну реалізацію права вибору. Правомірність використання даних, зібраних про користувача в мережі, для політичної реклами є сумнівною.

Крім того, використання великих даних для проведення спеціальних інформаційних операцій робить їх більш ефективними та може призвести до завдання суттєвої шкоди суспільству та державі. Виклики, які постають перед сучасним світом при застосування спеціальних інформаційних операцій настільки значимі, що жодна країна світу сьогодні не здатна самостійно забезпечити інформаційну безпеку, а від так, і гарантувати своїм громадянам сталий і гармонійний розвиток задля реалізації індивідуальних, суспільних та національних інтересів. Тому потрібно говори про вироблення єдиних механізмів захисту та гармонізації відповідних правових норм на міжнародному рівні.

Це далеко не повний перелік актуальних завдань, які постають перед правовою наукою та правом загалом через впровадження нових інноваційних технологій та цифровізації суспільства. Виникнення нових інформаційних загроз та специфіка інформаційної сфери потребують оперативного реагування та нових правових механізмів. Система протидії інформаційним загрозам на всіх етапах функціонування, починаючи від виявлення реальних чи потенційно можливих інформаційних небезпек та їх фіксації до заходів протидії, повинна бути забезпечена нормативно-правовими документами, діяти в рамках національного законодавства та міжнародного права. Технічні та програмно-технологічні заходи протидії інформаційним загрозам не

можуть зазіхати на інформаційні права громадян, гарантовані національним та міжнародним правом, так само, як не можуть обмежувати інформаційні свободи особи.

Література:

1. Про захист персональних даних: Закон України від 1 червня 2010 р. // База даних Законодавство України / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG
3. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) *Official Journal L 201, 31/07/2002 P. 0037 – 0047*. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058
4. Vidal-Hall v Google Inc. [2015] EWCA Civ 311. URL: https://www.judiciary.uk/wp-content/uploads/2015/03/google-v-vidal-hall-judgment.pdf

ЩОДО ПОНЯТТЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ВЧИНЕНИХ ВІЙСЬКОВОСЛУЖБОВЦЯМИ

Риженко І. М.

кандидат технічних наук, доцент, доцент кафедри цивільно-правових дисциплін Міжнародного економіко-гуманітарного університету імені академіка Степана Дем'янчука

м. Рівне, Україна

Сьогодні вчинення кримінального правопорушення серед військовослужбовців – це суспільно-небезпечне явище, яке зберігає свою тенденцію до зростання і становить особливу небезпеку у сфері інформаційних технологій і ресурсів, використання глобальних комп'ютерних, телекомунікаційних мереж в терористичних, екстремістських та пропагандистських цілях, що згодом наносить велику шкоду державі та її громадянам.