розслідування окремих категорій кримінальних правопорушень» № 720-IX від 17 червня 2020 року. Режим доступу: https://zakon.rada.gov.ua/laws/show/720-20#Text (дата звернення 02.12.2020)

4. Закон України Про внесення змін до деяких законодавчих актів України щодо спрощення досудового розслідування окремих категорій кримінальних правопорушень від 22 листопада 2018 року № 2617-VIII. Режим доступу: https://zakon.rada.gov.ua/laws/show/2617-19#Text. (дата звернення 02.12.2020)

ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ПАНДЕМІЇ COVID-19

Ковалевич Б. В.
магістр
Міжнародного економіко-гуманітарного університету
імені академіка Степана Дем'янчука
м. Рівне, Україна

В умовах формування інформаційної цивілізації інформація стає вирішальним чинником розвитку сучасного суспільства. У зв'язку з цим спостерігається тенденція не тільки до розширення правового регулювання інформаційних відносин, а й до створення договорів, які регулюють інформаційні відносини на міжнародному рівні, особливо у сфері інформаційної безпеки.

Ще більшої актуальності питання регулювання інформаційної сфери набуло в умовах пандемії коронавірусу, коли задля протидії поширенню захворювання держави почали відслідковувати пересування своїх громадян, а компанії та підприємства – переводити своїх працівників на віддалений режим роботи і використовувати у своїй діяльності новітні технології.

Яскравим прикладом першого аспекту є досвід Китаю, який використовує безпілотники, камери розпізнавання облич тощо для контролю за місцезнаходженням своїх громадян [1]. Низка інших держав отримує дані з телефонних мереж, аби слідкувати за пересуванням громадян і визначати коло потенційно інфікованих осіб. Зокрема, у Південній Кореї уряд використовував дані транзакцій за допомогою кредитних карток, геолокацію телефону й відеоспостереження, щоб мати детальну інформацію про пацієнтів із коронавірусом, не ідентифікуючи їх на ім'я. У результаті була складена карта, на якій люди могли побачити чи перебували вони поруч із носієм коронавірусу. Проте це призвело до

того, що дані про деяких пацієнтів були оприлюднені без їхньої згоди, тому органи державної влади вирішили обмежити політику обміну даними [2]. Водночас Словаччина ухвалила закон, який дозволяє уряду контролювати пересування людей, заражених коронавірусом. Поправка покликана надати службі охорони здоров'я Словаччини доступ до даних про місцезнаходження з мобільних телефонів осіб, які перебувають на карантині [2]. І хоча таке спостереження за пересуванням громадян є ефективним для боротьби з коронавірусом, питання про захищеність зібраних даних, у тому числі конфіденційних, їхнє подальше використання, а також дотримання основоположних прав і свобод людини залишається відкритим.

Можливим вирішенням цієї проблеми є відновлення всіх порушених прав після закінчення карантинних обмежень. При цьому наразі нові заходи мають застосовуватися державами у межах чинного законодавства, наприклад, про захист персональних даних; дійсно допомагати у боротьбі з коронавірусом, а також обмежуватися терміном, необхідним для боротьби з хворобою [2].

Другий аспект стосується більш широкого кола правових норм, пов'язаних з регулюванням інформаційних відносин загалом. Варто зазначити, що законодавство, присвячене цьому питанню, виникає поступово разом з появою та розвитком відповідних суспільних або технічних явищ. Специфіку правового регулювання в інформаційній сфері почали детально розглядати лише у 70-ті роки XX століття, коли відбулися революційні зміни як у кількісних, так і в якісних характеристиках інформаційних відносин, обумовлені технічним і соціальним прогресом людства [3].

Загалом дослідники права інформаційної безпеки визначають два правові компоненти: певний комплекс поглядів, принципів і установок щодо питань інформаційної безпеки, який виступає в якості системоутворюючого чинника та комплекс правових норм, в яких втілені вищезгадані погляди, і за допомогою яких регулюються суспільні відносини в сфері інформаційної безпеки. Фактично така схема є теоретичним обґрунтуванням терміну «правова база політики інформаційної безпеки». Адже система поглядів, принципів і установок тих політичних сил, що знаходяться при владі, втілюється у політичні рішення, які закріплюються у відповідних нормативно-правових актах [4, с. 38]. Формування подібної правової бази відбувається штучно через прийняття відповідних актів і залежить від волі законодавчого органу, тобто від політики держави в цій сфері.

Сьогодні в силу особливої актуальності об'єктом детального дослідження національних і зарубіжних фахівців дедалі частіше стають проблеми захисту інформації в автоматизованих системах не тільки в

окремих державах, а й на глобальному рівні. Національна практика у цій сфері переважно зосереджується на способі правової охорони інформації, тоді як міжнародна – тяжіє до комплексного способу її захисту на рівні міжгалузевих комплексних інститутів права [5, с. 15].

Ще одна проблема виникає у зв'язку з тим, що нові технології реалізуються на практиці швидше, ніж вносяться зміни до відповідних правових норм. Це призводить до того, що частина діяльності підприємств не охоплюється чинним законодавством. При цьому варто враховувати, що з огляду на створення комп'ютерної інформації за участі великої кількості людей в різних країнах і її творчий характер регулювання цієї сфери вимагає синергії правових норм як на національному (законодавства окремих держав), так і на міждержавному (положення міжнародного публічного права, у тому числі щодо регулювання міжнародних приватно-правових відносин) рівні.

Отже, забезпечення інформаційної безпеки сьогодні стає все більш значущою складовою суспільних відносин за умов формування інформаційної цивілізації. Проте складність та багатосторонній характер інформаційних відносин, особливо з огляду на поточну ситуацію у світі, з одного боку, вимагає втручання держави для забезпечення необхідного рівня безпеки громадян, а з іншого боку, надмірне державне втручання саме собою створює загрозу і може привести до негативних наслідків: обмеження прав людини і руйнації демократичних інститутів громадянського суспільства. Це спричиняє різнобічні наукові течії щодо правового та політичного регулювання інформаційної безпеки на національному та міжнародному рівнях і потребує подальшого детального вивчення.

Література:

1. Nay O. Can a virus undermine human rights? 2020. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7170793/

2. Хто буде стежити за тими, хто стежить за громадянами? Цифрові права в епоху корона вірусу. 2020. URL: https://www.radiosvoboda.org/a/digitalni-prava-u-sviti/30520457.html.

3. Венгеров А.Б. Право и информация в условиях автоматизации управления. М., 1978. 320 с.

4. Батурин Ю.М. Телекоммуникации и право – вопросы стратегии. Центр «Право и средства массовой информации». Серия «Журналистика и право». Вып. 2686 с.

5. Брижко В. М., Орехов А. А., Гальченко О. Н., Цимбалюк В. С. Е-будущее и информационное право. К.: Интеграл, 2002. 327 с.