УДК 343.43 (043.2)

Філіппов С.О., к.психол.н., доцент,
Національна академія Державної прикордонної служби України,
м. Хмельницький, Україна

Дрюк Н.С., начальник відділення контролю другої лінії
відділу прикордонної служби «Бориспіль-1» Окремого контрольно-
пропускного пункту «Київ», м. Бориспіль, Україна

ЗАСТОСУВАННЯ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ З МЕТОЮ ПРОТИДІЇ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ НА ДЕРЖАВНОМУ КОРДОНІ

Підвищення рівня застосування різноманітних технологій, у тому числі біометричних, передбачено різними нормативно-правовими актами серед шляхів розв'язання проблеми протидії злочинності. Наприклад, відповідно до Стратегії розвитку Державної прикордонної служби у 2020 р. повинна бути завершена модернізація та укомплектованість підрозділів прикордонного контролю програмно-технічними комплексами з функціями оброблення інформації про осіб, які перетинають державний кордон, їх паспортних документів з використанням електронних носіїв інформації, у тому числі з функцією біометричного контролю. У 2018 р. в Україні створено національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства (далі - національна система). Суб'єктами національної системи є ДМС, Адміністрація Держприкордонслужби, Національна поліція, МВС, МЗС, закордонні дипломатичні установи, Мінінфраструктури, СБУ, Служба зовнішньої розвідки та Міноборони. Розпорядником системи є Державна міграційна служба.

Із середини 2000-х років у різних аеропортах світу встановлюються автоматизовані системи прикордонного контролю (Automated Border Control systems) – e-Gates (у Великій Британії та Ірландії), SmartGates (аналог в Австралії та Новій Зеландії), Parafe (у Франції), Global Entry (у США), EasyPass system (у Норвегії), J-BIS (в Японії), Smart Entry Service (у Кореї), Viajero Confiable (у Мексиці). Кількість e-Gate, розгорнутих в глобальному масштабі в аеропортах та на вокзалах Європи, Австралії, Азії та Америки збільшилась у тричі з 1 100 в 2013 році до більш ніж 3 200 в 2018 році. Подорожуючі особи самостійно проходять АВС за наявності уніфікованого за правилами ІКАО ePassport. По завершенні процесу ідентифікації відкривається турнікет для проходу. В аеропорту Дубая встановлено систему LIDAR, яка спрацьовує, коли пасажири проходять через коридор, перед тим як здати багаж. Тут в автоматичному режимі відбувається їх ідентифікація за допомогою 3D-сканування осіб. Програмне забезпечення для розпізнавання осіб працює разом з

біометричним паспортом.

Заслуговує на увагу є досвід прикордонних служб Угорщини, Греції, Латвії, якими на сухопутних кордонах у 2019 році протестовано «iBorder Ctrl» - система штучного інтелекту, яка оцінює ймовірність обману в інтерв'ю шляхом аналізу невербальних мікровиявів осіб, які проходять інтерв'ювання, застосовує удосконалений біометричний модуль для ідентифікації осіб, які перетинають кордон, виявляє людей, прихованих всередині різних транспортних засобів під час перетинання кордону, проводить перевірку даних традиційних систем (які в ЄС вважаються вже певною мірою застарілими), таких як SIS II. *Запровадження таких новацій, як iBorder Ctrl, в Україні, на наш погляд потребує внесення змін до п. 2 част. 5 ст. 2 Закону України «Про прикордонний контроль» (після слів «технічних засобів прикордонного контролю» додати слова «засоби штучного інтелекту»).*

Переваги застосування біометричних документів та систем контролю: більш високий ступінь захисту документу від підробки; можливість автоматичної перевірки приналежності власнику документа, що скорочує час на ідентифікацію особистості, збільшує швидкість даної процедури і виключає суб'єктивізм при оцінці її результатів; значний технологічний потенціал даного документа, тобто на чіп, крім ідентифікаційних даних, можуть записуватися різноманітні інші персональні дані; втрачає сенс підробка та незаконне використання електронних документів з біометричними даними; біометричні персональні дані, що збираються при оформленні електронних паспортів, можуть застосовуватися в діяльності з розслідування правопорушень.

Крім кримінальних правопорушень, пов'язаних із підробленням документів, застосування біометричних технологій є надзвичайно важливим у боротьбі з тероризмом, особливо з авіатероризмом. На цьому зосереджено основні акценти Резолюції 2396 (2017) Ради безпеки ООН. Зокрема, ст. 15 цього документа передбачено, що «держави-члени повинні розробляти і впроваджувати системи збору біометричних даних, які можуть включати ідентифікаційні біометричні дані, для відповідального і належного виявлення терористів, включаючи іноземних бойовиків-терористів». У даний час Інтерпол має біометричні дані більш як 41 000 іноземних бойовиків – терористів.

З 2013 р. у модернізованому вигляді (SIS-II) працює Шенгенська інформаційна система. SIS-II, побудована на основі трьох компонентів: центральної, національних систем та зв'язку між ними. Її функціональні параметри значно розширено, зокрема за рахунок можливості обробки біометричної інформації та її співставлення в інтегрованій системі баз (що стосується розшукуваних осіб або осіб, які не мають права перебування на території ЄС тощо) при цьому гарантує захист персональних даних.

Поза сумнівом, дієвість національної системи біометричної ідентифікації в Україні неможливо забезпечити без інтеграції з такими

міжнародними інформаційними системами, а також інтегрованого використання інформаційних систем різнорідних служб, як суб'єктів національної системи, а також взаємодії з іншими службами, що здійснюють контрольні функції: таких як служб авіабезпеки, адміністрації морських портів тощо.

Література

1. Філіппов С.О. Біометричні технології: значення для протидії транскордонній злочинності. *Вісник Національної академії Державної прикордонної служби України. Юридичні науки.* 2018. Вип. 2. URL: http://nbuv.gov.ua/UJRN/vnadpcurn_2018_2_6

2. Filippov S. Dynamics and Geographical Distinctions of Crime connected with Migrants' Moving to Europe on Different Routes. *NATO Science for Peace and Security Series E: Human and Societal Dynamics*. 2016. Amsterdam: IOS Press. Volume 129. P. 21–27.

3. Smart lie-detection system to tighten EU`s busy borders. 24 October 2018. URL: https://ec.europa.eu/research/infocentre/article_en.cfm?artid=49726.

УДК 343.353 (043.2)

Ярмиш Н.М., д.ю.н., професор,
Національна академія прокуратури України, м. Київ, Україна

ЧИ Є КОРУПЦІОНЕРАМИ СУБ'ЄКТИ ЗЛОЧИНУ, ПРЕДБАЧЕНОГО СТ. 369-2 КРИМІНАЛЬНОГО КОДЕКСУ УКРАЇНИ «ЗЛОВЖИВАННЯ ВПЛИВОМ»?

Стаття 369-2 з моменту її появи у Кримінальному кодексі України (КК України) піддавалася і піддається до сих пір жорсткій критиці. Починати цю критику можна прямо з сумнівної назви, яка дає підстави думати, що впливати на осіб, зазначених в диспозиції, нібито можна, проте в цьому слід «знати міру» – впливом не зловживати. Проблем, пов'язаних з невдалою конструкцією статті, дуже багато. Одна з найбільш суттєвих походить від посилання в примітці на нечинний Закон України «Про засади запобігання та протидії корупції» (примітка стосується поняття особи, яка виконує функції держави). Помилка походить від банальної неуважності законодавця: у відповідні примітки двох статей не внесли зміни після того, як набрав чинності Закон України «Про запобігання корупції». Незважаючи на численні звернення до Верховної Ради науковців та практичних працівників, зазначена вада досі не усунута. Це викликає подив, оскільки аналогічна помилка нещодавно виправлена щодо примітки ст. 172 КК України. А про ст. 369-2 знову забули. Ще більш дивує, що суди продовжують виносити вироки за цією статтею, порушуючи при цьому, зокрема, заборону застосовувати кримінальний закон за аналогією.