

**РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ
В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ ВІД ACQUIS ЄС
ДО НАЦІОНАЛЬНОЇ ПРАКТИКИ**

Іван РУЩАК

*кандидат юридичних наук, доцент
юридичного факультету*

*ДВНЗ «Ужгородський національний університет»
м. Ужгород, Україна*

Стрімкий розвиток технологій штучного інтелекту ставить перед сучасною правовою системою принципово нові виклики, особливо у сфері кримінального судочинства. З одного боку, впровадження ШІ у правоохоронну діяльність відкриває широкі можливості для підвищення ефективності розкриття злочинів, зокрема, завдяки предиктивній аналітиці, автоматизованому аналізу великих масивів даних, розпізнаванню осіб та прискоренню рутинних процесів документування. З іншого боку, застосування цих технологій на етапі досудового розслідування неминуче породжує низку гострих питань правового, етичного та процесуального характеру.

Кримінальне право та кримінальний процес пред'являють до будь-яких інструментів розслідування особливо суворі вимоги: допустимість доказів, захист права на приватність, забезпечення справедливого суду, недискримінація та прозорість прийнятих рішень. Саме тому алгоритмічні системи, здатні впливати на долю конкретної людини, не можуть залишатися поза межами чіткого правового регулювання. Міжнародний досвід свідчить: там, де ШІ впроваджується без належних правових гарантій та механізмів контролю, виникають системні ризики порушення основоположних прав учасників кримінального провадження.

Європейський Союз став першим у світі наддержавним утворенням, яке сформувало комплексну та системну правову базу для регулювання технологій штучного інтелекту. Підхід ЄС ґрунтується на ідеї так званого «орієнтованого на людину» штучного інтелекту, тобто такого, що розвивається та застосовується з повагою до основоположних прав, демократичних цінностей і верховенства права.

Основу регуляторної архітектури ЄС у сфері ШІ становлять декілька ключових документів. Ще у 2019 році Європейська комісія оприлюднила «Етичні настанови щодо надійного штучного інтелекту»

(Ethics Guidelines for Trustworthy AI)¹, які визначили три фундаментальні вимоги до систем ШІ: законність, етичність та надійність. Ці настанови, хоча й мали рекомендаційний характер, заклали концептуальну основу для подальшого законодавчого регулювання та визначили ключові принципи, якими мають керуватися розробники і користувачі систем ШІ, від прозорості та підзвітності до поваги до приватності та недискримінації.

Центральним і найбільш значущим елементом регуляторної системи ЄС є Регламент про штучний інтелект, більш відомий як AI Act, який набрав чинності у серпні 2024 року і став першим у світі комплексним законом, що безпосередньо регулює розробку та застосування систем ШІ². AI Act запроваджує ризик-орієнтований підхід до регулювання, відповідно до якого всі системи ШІ поділяються на кілька категорій залежно від рівня потенційної небезпеки, яку вони становлять для прав і безпеки людей.

Найвищий рівень регулювання передбачено для систем із неприйнятним рівнем ризику, саме їх використання в ЄС прямо заборонено. До цієї категорії належать, зокрема, системи соціального скорингу громадян з боку державних органів, технології маніпулятивного впливу на підсвідомість людини, а також більшість застосувань систем біометричної ідентифікації в режимі реального часу у публічних місцях. Остання заборона є особливо важливою з точки зору кримінального провадження, оскільки безпосередньо стосується використання технологій розпізнавання обличчя правоохоронними органами. Втім, AI Act передбачає обмежені винятки з цієї заборони, зокрема, для пошуку жертв злочинів, запобігання конкретним терористичним загрозам або переслідування тяжких злочинів за наявності попереднього судового дозволу.

Окрему і надзвичайно важливу категорію становлять системи так званого «високого ризику», до яких AI Act відносить більшість інструментів ШІ, що застосовуються у сфері правосуддя та правоохоронної діяльності. Це, зокрема, системи предиктивної аналітики для оцінки ризику вчинення злочинів, інструменти для аналізу та перевірки доказів, системи оцінки ризику рецидиву, а також поліграфи та аналогічні технології виявлення неправдивих свідчень. Для

¹ European Commission. (2019). *Ethics guidelines for trustworthy AI*. High-Level Expert Group on Artificial Intelligence. <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>

² European Parliament & Council of the European Union. (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Official Journal of the European Union, L series. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401689

систем цієї категорії встановлені суворі вимоги: обов'язкова оцінка відповідності перед введенням в експлуатацію, ведення детальної технічної документації, забезпечення можливості нагляду з боку людини, гарантування точності та надійності, а також прозорості щодо можливостей і обмежень системи.

Окрім AI Act, регулювання ШІ в ЄС здійснюється також через суміжне законодавство. Зокрема, Загальний регламент про захист даних (GDPR) встановлює жорсткі вимоги до обробки персональних даних, у тому числі тих, що обробляються за допомогою систем ШІ. Директива про захист даних у сфері правоохоронної діяльності (Law Enforcement Directive) окремо регулює обробку персональних даних компетентними органами для цілей попередження, розслідування та переслідування злочинів. Ці акти у сукупності з AI Act формують багаторівневу систему захисту прав осіб, які можуть зазнати впливу алгоритмічних рішень у кримінальному провадженні.

Таким чином, підхід Європейського Союзу до регулювання штучного інтелекту відзначається комплексністю та послідовністю: він поєднує заборону найбільш небезпечних застосувань ШІ, суворі вимоги до систем високого ризику та загальні стандарти прозорості й підзвітності. У контексті кримінального права це означає, що будь-яке використання систем ШІ у досудовому розслідуванні має відповідати не лише вимогам процесуального законодавства, але й нормам регуляторної бази ЄС щодо безпеки, надійності та поваги до основоположних прав людини.

Загальний регламент про захист даних (GDPR) та його значення для застосування штучного інтелекту у кримінальному провадженні

Загальний регламент про захист даних (General Data Protection Regulation або GDPR), що набрав чинності у травні 2018 року, є одним із найбільш впливових нормативно-правових актів Європейського Союзу у сфері захисту персональних даних³. Хоча GDPR не регулює безпосередньо технології штучного інтелекту, його положення мають принципове значення для будь-якої діяльності, пов'язаної з обробкою персональних даних за допомогою алгоритмічних систем, у тому числі в контексті кримінального провадження та досудового розслідування.

Ключова цінність GDPR полягає у тому, що він встановлює універсальні та обов'язкові стандарти поведінки з персональними даними фізичних осіб на території ЄС незалежно від того, яким саме інструментом – людиною чи алгоритмом – ці дані обробляються. Відтак

³ European Parliament & Council of the European Union. (2016). *Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*. Official Journal of the European Union, L 119, 1–88. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>

кожного разу, коли система штучного інтелекту збирає, аналізує, зберігає або іншим чином використовує дані, що дозволяють ідентифікувати конкретну особу, вона підпадає під дію регламенту з усіма наслідками, що з цього випливають.

GDPR закріплює низку фундаментальних принципів обробки персональних даних, які безпосередньо обмежують можливості застосування ШІ у правоохоронній діяльності. Принцип законності, справедливості та прозорості вимагає, щоб обробка даних здійснювалася на чітко визначеній правовій підставі та у спосіб, зрозумілий для особи, даних якої це стосується. Принцип мінімізації даних забороняє збирати більше інформації, ніж це необхідно для досягнення конкретної законної мети. Принцип обмеження мети, у свою чергу, не дозволяє використовувати зібрані дані у цілях, відмінних від тих, для яких вони первісно збиралися. Нарешті, принцип точності зобов'язує забезпечувати актуальність та достовірність даних, що обробляються, – вимога особливо важлива в контексті кримінального розслідування, де помилки у даних можуть мати катастрофічні наслідки для підозрюваних та обвинувачених осіб.

Особливого значення для застосування систем ШІ набуває стаття 22 GDPR, яка регулює автоматизоване прийняття рішень, включаючи профілювання. Відповідно до цього положення, особа має право не бути об'єктом рішення, що ґрунтується виключно на автоматизованій обробці даних і тягне для неї правові наслідки або суттєво на неї впливає. У контексті кримінального провадження це означає, що рішення про затримання, обрання запобіжного заходу чи висунення обвинувачення не може прийматися на підставі виключно алгоритмічного висновку без належного людського контролю та оцінки. Таким чином, GDPR фактично закріплює принцип, відповідно до якого ШІ може слугувати лише допоміжним інструментом для підтримки рішень уповноваженої особи, але не їх самостійним джерелом.

Слід також зазначити, що GDPR запроваджує інститут оцінки впливу на захист даних (Data Protection Impact Assessment або DPIA), яка є обов'язковою у випадках, коли планована обробка даних може становити високий ризик для прав і свобод фізичних осіб. Масштабне систематичне спостереження за громадянами у публічних місцях, автоматизоване профілювання осіб на основі чутливих даних – усе це є типовими прикладами ситуацій, що вимагають проведення DPIA. Для правоохоронних органів, які впроваджують системи ШІ у свою діяльність, цей інструмент є важливим механізмом попереднього виявлення та мінімізації ризиків порушення прав учасників кримінального провадження.

Водночас необхідно враховувати, що сфера застосування GDPR у контексті правоохоронної діяльності має певні особливості. Для

діяльності компетентних органів з попередження, розслідування, виявлення або переслідування кримінальних правопорушень ЄС прийняв окремий спеціальний акт, а саме Директиву 2016/680 (Law Enforcement Directive), яка встановлює спеціальний режим захисту даних у цій сфері⁴. Проте це не означає виключення GDPR із правового поля: на практиці обидва акти можуть застосовуватися паралельно, наприклад, коли в рамках одного розслідування задіяні як правоохоронні органи, так і приватні суб'єкти, що надають технологічні рішення на основі ШІ.

Таким чином, GDPR виступає потужним правовим інструментом, що суттєво визначає межі допустимого використання штучного інтелекту у кримінальному провадженні. Його вимоги щодо законності обробки даних, мінімізації втручання у приватність, заборони виключно автоматизованих рішень та обов'язкової оцінки ризиків формують правові рамки, у межах яких мають функціонувати будь-які алгоритмічні системи, задіяні у досудовому розслідуванні. Дотримання цих вимог є не лише юридичним обов'язком, але й необхідною умовою для забезпечення допустимості доказів, отриманих за допомогою ШІ, та легітимності кримінального провадження загалом.

Визнання та врахування цих положень важливі, передусім, в контексті адаптації до вимог GDPR та AI Act, що є юридичним зобов'язанням України в рамках євроінтеграційного процесу. Угода про асоціацію між Україною та ЄС прямо передбачає зобов'язання щодо наближення національного законодавства у сфері захисту персональних даних до європейських стандартів⁵. Відповідно, впровадження норм, аналогічних GDPR та AI Act, є не добровільним вибором, а необхідною умовою просування України на шляху до членства в ЄС. У контексті кримінального провадження це означає, що Україна має привести у відповідність до європейських стандартів не лише загальне законодавство про захист даних, але й спеціальні норми, що регулюють збирання, зберігання та обробку персональних даних у ході досудового розслідування.

Особливої актуальності це питання набуває у зв'язку з активним впровадженням цифрових технологій у діяльність українських правоохоронних органів. Зокрема, в Україні вже функціонують або

⁴ European Parliament & Council of the European Union. (2016). *Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences (Law Enforcement Directive)*. Official Journal of the European Union, L 119, 89–131. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680>

⁵ *Association Agreement between the European Union and Ukraine*. (2014). Official Journal of the European Union, L 161. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A22014A0529%2801%29>

перебувають на стадії розробки системи відеоспостереження з елементами розпізнавання облич, бази даних для аналізу великих масивів інформації, а також різноманітні аналітичні платформи для підтримки оперативно-розшукової діяльності. Відсутність належного правового регулювання цих інструментів створює серйозні ризики для прав учасників кримінального провадження та ставить під сумнів допустимість доказів, отриманих за їх допомогою. Адаптація до стандартів ЄС дозволила б усунути ці прогалини та сформувати чіткі правові рамки для використання ІІІ у досудовому розслідуванні.

Важливим аспектом є також питання міжнародного співробітництва у кримінальних справах. Зближення правових стандартів України та ЄС у сфері захисту даних та регулювання ІІІ є необхідною передумовою для ефективної взаємодії українських правоохоронних органів з їхніми європейськими партнерами. Зокрема, передача персональних даних між Україною та державами, членами ЄС у рамках спільних розслідувань можлива лише за умови, що Україна забезпечує адекватний рівень захисту даних, порівнянний із європейськими стандартами. Відсутність такого визнання суттєво ускладнює співробітництво з Євроюстом, Європолем та іншими інституціями ЄС у сфері кримінального правосуддя.

Окремо слід наголосити на значенні адаптації *acquis* ЄС для забезпечення довіри суспільства до правоохоронної системи України. Одним із ключових викликів для українського кримінального судочинства залишається низький рівень суспільної довіри до правоохоронних органів. Впровадження прозорих, зрозумілих та відповідних міжнародним стандартам правил використання технологій ІІІ у досудовому розслідуванні здатне суттєво змінити цю ситуацію.