УНИВЕРЗИТЕТ У БЕОГРАДУ

ФАКУЛТЕТ ОРГАНИЗАЦИОНИХ НАУКА

Небојша Б. Драговић

Унапређење модела за превенцију и рано откривање илегалних активности применом предиктивне аналитике

Докторска дисертација

Београд, 2026. године

UNIVERSITY OF BELGRADE

FACULTY OF ORGANIZATIONAL SCIENCES

Небојша Б. Драговић

Improving the Model for the Prevention and Early Detection of Illegal Activities Using Predictive Analytics

Doctoral Dissertation

Belgrade, 2026

Ментор:

др Драган Вукмировић, редовни професор Факултета организационих наука

Чланови комисије:

др Борис Делибашић, редовни професор Факултета организационих наука

др Милан Мартић, редовни професор Факултета организационих наука

др Милија Сукновић, редовни професор Факултета организационих наука

др Александар Ђоковић, ванредни професор Факултета организационих наука

др Саша Милић, научни саветник, Електротехнички институт Никола Тесла у Београду

Датум одбране:

Унапређење модела за превенцију и рано откривање илегалних активности применом предиктивне аналитике

Сажетак

Докторска дисертација се бави унапређењем модела за превенцију и рано откривање илегалних активности применом предиктивне аналитике. Полазиште истраживања је став да предиктивна полицијска аналитика не треба да буде сведена на изолован алгоритам за означавање ризичних места, лица или догађаја, већ да је треба посматрати као интегрисани систем који повезује податке, аналитичке методе, технолошку инфраструктуру, институционалне процедуре и људски контролисано одлучивање.

У раду су анализирани појам и развој полицијске аналитике, однос предиктивне полицијске аналитике и предиктивне полиције, као и предуслови за примену напредних аналитичких модела у безбедносном систему. Посебна пажња посвећена је анализи постојећих модела, њихових предности, ограничења и ризика, укључујући питања квалитета података, алгоритамске пристрасности, објашњивости, правне пропорционалности, етичке прихватљивости и људске контроле.

Централни допринос дисертације представља развој унапређеног хијерархијског модела који повезује Police Internet of Things (PIoT), односно полицијски интернет ствари, edge–fog–cloud архитектуру, моделе машинског учења, fuzzy подршку одлучивању и евалуациони оквир. Предложени модел омогућава да се оперативне, тактичке и стратешке функције раздвоје по нивоима дигиталне инфраструктуре: edge ниво подржава локалну детекцију и иницијалну обраду података, fog ниво краткорочну предикцију и тактичку координацију, док cloud ниво омогућава сложенију анализу, fuzzy подршку одлучивању, стратешко планирање и управљање ризиком.

Емпиријска подршка моделу разматрана је кроз студију случаја засновану на PIoT приступу у паметном граду. У њој су приказане две примене: предвиђање саобраћајног тока применом RNN, LSTM и GRU модела и fuzzy подршка одлучивању у разликовању физичког и сајбер-инцидента. Резултати показују да предложени приступ има функционалну и методолошку вредност, али и да његова пуна примена захтева контролисано пилот-окружење, вишекритеријумску евалуацију и јасне правне, организационе и етичке механизме контроле.

Закључује се да унапређење модела за превенцију и рано откривање илегалних активности не зависи само од избора предиктивног алгоритма, већ од изградње интегрисаног, хијерархијски организованог, евалуабилног и институционално одговорног аналитичко-оперативног система. Предложени модел не замењује постојеће полицијске процедуре алгоритмом, већ унапређује аналитичко-оперативни циклус кроз повезивање података, предикције, fuzzy/XAI подршке, људске контроле, евалуације и организационог учења.

***Кључне речи**: предиктивна полицијска аналитика, предиктивна полиција, илегалне активности, Police Internet of Things, PIoT, edge–fog–cloud архитектура, машинско учење, fuzzy логика, подршка одлучивању, људска контрола.*

Improving the Model for the Prevention and Early Detection of Illegal Activities Using Predictive Analytics

Abstract

This doctoral dissertation focuses on improving a model for the prevention and early detection of illegal activities using predictive analytics. The research is based on the premise that predictive police analytics should not be reduced to an isolated algorithm for identifying risky places, persons, or events, but should be understood as an integrated system that connects data, analytical methods, technological infrastructure, institutional procedures, and human-controlled decision-making.

The dissertation analyzes the concept and development of police analytics, the relationship between predictive police analytics and predictive policing, and the preconditions for applying advanced analytical models within the security system. Special attention is given to the analysis of existing models, including their advantages, limitations, and risks, such as data quality, algorithmic bias, explainability, legal proportionality, ethical acceptability, and human oversight.

The central contribution of the dissertation is the development of an improved hierarchical model that integrates the Police Internet of Things (PIoT), edge–fog–cloud architecture, machine learning models, fuzzy decision support, and an evaluation framework. The proposed model enables the separation of operational, tactical, and strategic functions across the levels of digital infrastructure: the edge level supports local detection and initial data processing, the fog level supports short-term prediction and tactical coordination, while the cloud level enables more complex analytics, fuzzy decision support, strategic planning, and risk management.

Empirical support for the proposed model is discussed through a case study based on the PIoT approach in a smart city environment. The case study includes two applications: traffic-flow forecasting using RNN, LSTM, and GRU models, and fuzzy decision support for distinguishing between physical and cyber incidents. The results indicate that the proposed approach has functional and methodological value and that its full implementation requires a controlled pilot environment, multi-criteria evaluation, and clearly defined legal, organizational, and ethical control mechanisms.

The dissertation concludes that improving the model for the prevention and early detection of illegal activities depends not only on the selection of a predictive algorithm but also on the development of an integrated, hierarchically organized, evaluable, and institutionally responsible analytical-operational system. The proposed model does not replace existing police procedures with an algorithm; rather, it improves the analytical-operational cycle by linking data, prediction, fuzzy/XAI support, human oversight, evaluation, and organizational learning.

Keywords*: predictive police analytics, predictive policing, illegal activities, Police Internet of Things, PIoT, edge–fog–cloud architecture, machine learning, fuzzy logic, decision support, human oversight.*

Садржај

1. Увод

1.1. Проблем и предмет истраживања

Савремено безбедносно окружење карактеришу убрзана дигитализација, масовно генерисање података, развој система вештачке интелигенције и све израженије прожимање физичког и сајбер простора. Такве промене значајно мењају услове у којима се планирају и спроводе превенција, откривање и сузбијање илегалних активности, јер безбедносни ризици више нису ограничени само на физички простор, већ све чешће настају у интеракцији физичке, дигиталне и организационе инфраструктуре (Meijer & Wessels, 2019; Joh, 2019; Dragović et al., 2026).

У таквом контексту, предиктивна аналитика представља важан истраживачки и практични правац, јер омогућава да се на основу историјских, текућих и контекстуалних података идентификују обрасци, процењују ризици и подржи благовремено одлучивање у условима сложеног и динамичног окружења (Perry et al., 2013; Oatley, 2021; Bennett Moses & Chan, 2018). Међутим, у области безбедности предиктивна аналитика не може се посматрати само као техничко питање избора алгоритма. Њена примена подразумева повезивање података, аналитичких метода, технолошке инфраструктуре, институционалних процедура, правних ограничења и људски контролисаног одлучивања (Meijer et al., 2021; Oswald et al., 2018).

Предмет овог истраживања јесте унапређење модела за превенцију и рано откривање илегалних активности применом предиктивне аналитике. У раду се модел не третира као издвојени алгоритам за означавање ризичних места, лица или догађаја, већ као интегрисани систем који обухвата прикупљање и припрему података, предикцију, подршку одлучивању, интервенцију, евалуацију исхода и организационо учење. Такав приступ је посебно значајан зато што успешност предиктивне полицијске аналитике не зависи само од тачности предвиђања, већ и од квалитета података, објашњивости модела, институционалне употребљивости, пропорционалности примене и контроле алгоритамске пристрасности (Bennett Moses & Chan, 2018; Richardson et al., 2019; Gstrein et al., 2019).

Посебан истраживачки интерес усмерен је на развој хијерархијски организованог модела предиктивне полицијске аналитике који је погодан за интелигентне градове и хибридно физичко-сајбер окружење. У том смислу, полази се од претпоставке да је потребно

превазићи уске моделе усмерене искључиво на hotspot прогнозу и развити шири оквир који повезује Police Internet of Things (PIoT) инфраструктуру, edge–fog–cloud архитектуру, моделе машинског учења, fuzzy подршку одлучивању и институционалне механизме контроле (Perry et al., 2013; Ferguson, 2020; Dragović et al., 2026).

1.2. Циљеви истраживања

Општи циљ истраживања јесте развој унапређеног модела за превенцију и рано откривање илегалних активности применом предиктивне аналитике, који је методолошки утемељен, технолошки изводљив, организационо употребљив и правно-етички прихватљив (Meijer & Wessels, 2019; Gstrein et al., 2019; Oswald et al., 2018).

У раду се користи и појам Police Internet of Things (PIoT), односно полицијски интернет ствари, којим се означава примена IoT концепта у полицијском и безбедносном контексту. PIoT подразумева повезивање сензора, камера, комуникационих система, полицијских информационих система и аналитичких модела у јединствену инфраструктуру за праћење, предвиђање, подршку одлучивању и координацију поступања.

Из овако постављеног општег циља произлазе следећи посебни циљеви:

анализа и систематизација постојећих приступа предиктивној полицијској аналитици, њихових предности, ограничења и ризика (Meijer & Wessels, 2019; Kounadi et al., 2020; Oatley, 2021);

- разјашњавање односа између појмова predictive analytics, predictive policing и превентивног деловања у безбедносном систему (Perry et al., 2013; National Institute of Justice, 2014; Meijer & Wessels, 2019);
- дефинисање унапређеног хијерархијског модела који повезује науку о подацима, предиктивну аналитику, PIoT инфраструктуру и подршку одлучивању у јединствен оквир (Dragović et al., 2026; Mohamed et al., 2021; Perera et al., 2017);
- постављање оквира за евалуацију који обухвата техничке, организационе, правне и етичке критеријуме, како би се успешност модела процењивала шире од саме

предиктивне тачности (Bennett Moses & Chan, 2018; Oswald et al., 2018; Richardson et al., 2019);

- испитивање мере у којој се предложени модел може функционално и емпиријски подржати кроз постојеће студије случаја, као и начина његовог даљег развоја кроз контролисано пилот-окружење (Dragović et al., 2026; Hunt et al., 2014; Saunders et al., 2016).

Овако дефинисани циљеви омогућавају да се истраживање усмери не само на развој технички применљивог предиктивног модела, већ и на његово уклапање у шири аналитички, организациони, правни и етички оквир савременог безбедносног система.

1.3. Истраживачке хипотезе

Полазећи од предмета и циљева истраживања, формулисане су општа и посебне истраживачке хипотезе.

Општа хипотеза гласи: могуће је унапредити модел за превенцију и рано откривање илегалних активности применом предиктивне аналитике на начин који повезује податке, аналитичке моделе, хијерархијску дигиталну инфраструктуру и људски контролисано одлучивање, уз очување правне и етичке прихватљивости (Meijer & Wessels, 2019; Oswald et al., 2018; Dragović et al., 2026).

Из опште хипотезе произлазе следеће посебне хипотезе:

X1: хијерархијски организована вертикална PIoT архитектура представља погодан оквир за превенцију, рано откривање и подршку одлучивању у интелигентном граду, јер омогућава функционално раздвајање оперативних, тактичких и стратешких активности по edge, fog и cloud нивоима (Dragović et al., 2026; Mohamed et al., 2021; Perera et al., 2017);

X2: интеграција модела машинског учења и fuzzy логике у оквиру PIoT архитектуре може унапредити краткорочну предикцију и подршку одлучивању у сложеним безбедносним сценаријима, посебно када су подаци непотпуни, конфликтни или неодређени (Dragović et al., 2026; Zadeh, 1965; Khalid et al., 2021);

X3: успешност предиктивне аналитике у безбедносном систему не може се процењивати само на основу предиктивне тачности, већ мора обухватити и квалитет података,

организациону употребљивост, објашњивост модела, правну пропорционалност и контролу алгоритамске пристрасности (Bennett Moses & Chan, 2018; Richardson et al., 2019; Gstrein et al., 2019);

X4: унапређени модел може бити институционално одржив само ако је развијен као систем подршке одлучивању са јасно дефинисаном људском контролом, а не као потпуно аутоматизован механизам безбедносне процене (Joh, 2020; Asaro, 2019; Oswald et al., 2018).

Имајући у виду интердисциплинарну природу предмета истраживања, наведене хипотезе немају исту методолошку природу. X1 и X2 имају превасходно архитектонско-аналитички карактер и разматрају се кроз концептуално моделирање и студију случаја, док X3 и X4 имају евалуационо-нормативни и институционални карактер. Због тога се X3 и X4 не проверавају искључиво квантитативним тестирањем, већ кроз теоријску анализу, правно-етичку евалуацију, анализу ризика, принципе људске контроле и процену институционалне одрживости предложеног модела.

Овако постављене хипотезе омогућавају да се предложени модел испитује истовремено са архитектонског, аналитичког, евалуационог и институционалног становишта.

1.4. Методологија истраживања

Истраживање је засновано на комбинацији теоријско-аналитичког, компаративног, концептуалног, моделског и студијско-случајног приступа. Оваква методолошка поставка произлази из интердисциплинарне природе предмета истраживања, који обухвата полицијску аналитику, предиктивну аналитику, науку о подацима, вештачку интелигенцију, PIoT инфраструктуру, подршку одлучивању и правно-етичке аспекте примене аналитичких система у безбедносном контексту.

Теоријско-аналитички приступ користи се за преглед и систематизацију релевантне домаће и иностране литературе о полицијској аналитици, предиктивној полицији, примени вештачке интелигенције у безбедности, алгоритамској пристрасности и етичко-правним ограничењима примене предиктивних система (Meijer & Wessels, 2019; Kounadi et al., 2020; Oatley, 2021). Овај приступ омогућава да се предмет истраживања постави у шири научни и институционални контекст, као и да се идентификују кључни појмови, правци развоја и отворена питања у области предиктивне полицијске аналитике.

Компаративни приступ користи се за анализу постојећих модела предиктивног полицијског рада, њихових предности, ограничења и применљивости у различитим институционалним и технолошким контекстима. Посебна пажња посвећује се разликовању модела који су усмерени на предвиђање места и времена инцидената, модела који подржавају распоређивање ресурса и модела који обухватају шири процес доношења одлука (Perry et al., 2013; Bennett Moses & Chan, 2018; Meijer et al., 2021). На тај начин се постојећи приступи не анализирају само према техничким карактеристикама, већ и према њиховој употребљивости, ограничењима, ризицима и могућности интеграције у унапређени модел.

Концептуално и моделско истраживање примењује се у дефинисању унапређеног модела за превенцију и рано откривање илегалних активности. У оквиру овог дела развија се хијерархијска PIoT архитектура и вертикални ток података, од прикупљања сигнала на edge нивоу, преко краткорочне предикције и тактичке координације на fog нивоу, до сложене анализе, fuzzy подршке одлучивању и стратешког планирања на cloud нивоу (Dragović et al., 2026; Mohamed et al., 2021; Perera et al., 2017). Овај приступ омогућава да се предиктивна аналитика посматра као део ширег система управљања безбедносним ризицима, а не као изолована техничка процедура.

У емпиријском смислу, рад се ослања на студију случаја објављеног PIoT рада, у којем су кроз две примене — прогнозирање саобраћајног тока и fuzzy подршку одлучивању — тестирани кључни архитектонски и аналитички елементи предложеног приступа (Dragović et al., 2026). Овај део не представља коначну емпиријску валидацију свих аспеката модела, већ значајну основу за процену његове функционалне изводљивости, ограничења и могућности даљег развоја кроз контролисане пилот-примене.

Посебно је важно разграничити однос ове дисертације и претходно објављеног коауторског рада Dragović et al. (2026). Наведени рад представља емпиријски и технички ослонац за студију случаја, јер у њему су приказани вертикални PIoT концепт, edge–fog–cloud архитектура, вертикални ток података, примена RNN, LSTM и GRU модела за предвиђање саобраћајног тока, као и fuzzy приступ у разликовању физичког и сајбер-инцидента. У дисертацији се ти елементи користе као доказ концепта за поједине делове предложеног модела, али се не преузимају као целокупан модел дисертације. Нови допринос дисертације огледа се у ширем теоријском и методолошком оквиру предиктивне полицијске аналитике,

систематизацији предуслова и ризика примене, развоју унапређеног хијерархијског модела као целине, дефинисању односа између података, предикције, fuzzy/XAI подршке и људске контроле, као и у постављању интегрисаног евалуационог оквира који обухвата техничке, оперативне, организационе, правно-етичке и друштвене критеријуме.

Посебан део методолошког оквира односи се на евалуацију предложеног модела. Евалуација се не заснива искључиво на техничким мерама предиктивне тачности, већ обухвата и оперативне, организационе, правне, етичке и друштвене критеријуме. На тај начин се успешност модела процењује шире од питања да ли модел даје статистички прихватљиво предвиђање, односно укључује и питања квалитета података, објашњивости, контроле пристрасности, људског надзора, институционалне употребљивости и правне пропорционалности (Bennett Moses & Chan, 2018; Oswald et al., 2018; Richardson et al., 2019).

Хипотезе које се односе на правно-етичку прихватљивост, људску контролу, објашњивост и институционалну одрживост модела не третирају се као искључиво статистички проверљиве хипотезе, већ као евалуационо-нормативне претпоставке које се испитују кроз анализу литературе, правног оквира, етичких принципа, ризика примене и захтева за одговорним доношењем одлука.

Методолошки оквир истраживања зато обухвата: анализу појмова и терминолошких разграничења, анализу развоја предиктивне полицијске аналитике, систематизацију типова података и аналитичких поступака, компаративну анализу постојећих модела, концептуално моделирање унапређене PIoT архитектуре, анализу студије случаја, постављање евалуационог оквира, као и разматрање техничких, организационих, правних и етичких услова примене предложеног модела.

1.5. Структура рада

Рад је структуриран у десет поглавља. У првом поглављу дефинисани су проблем, предмет, циљеви, истраживачке хипотезе и методолошки оквир истраживања. Друго поглавље разматра појам и развој полицијске аналитике, са посебним освртом на дескриптивну и дијагностичку аналитику као основу за сложеније аналитичке приступе. Треће поглавље посвећено је предиктивној полицијској аналитици, њеном односу према предиктивној полицији, као и развоју ка AI-native полицијској аналитици.

У четвртом поглављу анализирају се предуслови имплементације полицијске аналитике, укључујући правно-стратешке, технолошке, кадровско-организационе и етичко-безбедносне предуслове. Пето поглавље садржи анализу постојећих модела и приступа, њихових предности, ограничења и истраживачких празнина. Шесто поглавље разматра изазове и ризике у примени предиктивне и AI-native полицијске аналитике, укључујући пристрасност, непоузданост, проблем „црне кутије“, аутоматизациону пристрасност, сајбер-безбедносне ризике, правни оквир и људску контролу.

Седмо поглавље представља централни део дисертације, јер се у њему развија прототип унапређеног модела за превенцију и рано откривање илегалних активности. Осмо поглавље дефинише оквир евалуације модела, са техничким, оперативним, организационим, правно-етичким и друштвеним критеријумима. Девето поглавље представља студију случаја засновану на PIoT моделу у паметном граду и показује како се предложена архитектура може операционализовати кроз предвиђање саобраћајног тока и fuzzy подршку одлучивању. Десето поглавље садржи синтезу резултата, дискусију истраживачких хипотеза, научне, стручне и друштвене доприносе, ограничења и правце будућих истраживања. Дисертација се завршава са списком коришћене литературе и обавезним анексима.

2. Полицијска аналитика

„Предвиђање није дар који долази са неба. Оно се заснива на подацима до којих долазе они који добро познају околности, простор и понашање противника“

— парафраза према: Sun Tzu, The Art of War

2.1. Актуелна друштвено-економска кретања

Савремено друштво се суочава са интензивним друштвено-економским променама, изазваним глобалним кризама, технолошким развојем, променама у начину живота и све већим ослањањем на дигиталну инфраструктуру. Пандемија COVID-19, геополитички и оружани сукоби, економска и енергетска нестабилност, миграциона кретања и поремећаји у глобалним ланцима снабдевања утицали су на економију, структуру становништва, животне навике, поверење у институције и начине на које се јављају ризици од илегалних активности (Sneader & Singhal, 2021).

Наведене промене посебно се одражавају на урбане средине, које карактеришу висока концентрација становништва, саобраћаја, инфраструктуре, економских активности и дигиталних система. Због тога савремена полиција све више мора да развија приступ заснован на подацима, који не обухвата само класичне полицијске изворе, већ и геопросторне податке, сензорске податке, податке из система паметног града, јавних регистара, отворених извора, друштвених медија и других релевантних извора.

Табела 2.1. Утицај савремених друштвено-економских, геополитичких и технолошких криза на безбедносно окружење

Криза / промена	**Економске последице**	**Друштвене и безбедносне последице**
Избегличка и миграциона кретања	Додатни трошкови за институције; потреба за већим капацитетима јавних служби; притисак на тржиште рада и системе социјалне подршке	Промена структуре становништва; већи притисак на урбане услуге; потреба за интеграцијом, превенцијом конфликата и заштитом рањивих група
COVID-19 пандемија и здравствене кризе	Економски пад; прекид рада појединих сектора; раст рада од куће и е-трговине; поремећаји у пословању	Промена понашања грађана; ограничење кретања; пад поверења; раст дигиталних превара, злоупотреба и сајбер-ризика
Поремећаји у глобалним ланцима снабдевања	Несташице; раст цена; проблеми у транспорту робе; поремећаји у снабдевању храном, лековима, енергентима и критичним производима	Повећан ризик од сивог тржишта, шпекулација, крађа, злоупотреба у дистрибуцији и притиска на критичну инфраструктуру
Геополитички и оружани сукоби	Раст цена енергената, сировина, транспорта и хране; инфлаторни притисци; неизвесност инвестиција и тржишта	Социјална несигурност; миграциони притисци; ризик од дезинформација, радикализације, сајбер-напада и угрожавања критичне инфраструктуре
Енергетска нестабилност и ризици у стратешким транспортним коридорима	Поремећаји у снабдевању нафтом, гасом и електричном енергијом; раст трошкова производње и транспорта; притисак на јавне финансије	Повећана осетљивост друштва на кризе; ризик од социјалних тензија, протеста, саботажа, криминала у вези са енергентима и појачане потребе за заштитом критичне инфраструктуре
Убрзана дигитализација	Развој дигиталних услуга; раст зависности од ИКТ инфраструктуре; нови модели пословања и трговине	Нови облици сајбер-криминала; потреба за заштитом података; дигитални надзор; питања приватности, алгоритамске пристрасности и поверења у институције

Истовремено, развој информационо-комуникационих технологија, Big Data концепта, интернета ствари, вештачке интелигенције и генеративне вештачке интелигенције мења начин на који се безбедносни ризици препознају, анализирају, тумаче и комуницирају. Ове технологије могу унапредити способност полиције да раније уочи обрасце ризика и да рационалније усмерава ресурсе, али истовремено отварају питања приватности, пристрасности, транспарентности и одговорности. Зато одговор на новонастале изазове не може бити само увођење нових технологија, већ развој методолошки, правно, етички и организационо контролисане полицијске аналитике засноване на подацима.

2.2. Полицијска аналитика

Рад са подацима у полицијским пословима није нова појава. Иако се у ранијим периодима није могло говорити о полицијској аналитици у савременом смислу, полицијски рад је од самог почетка подразумевао прикупљање информација, препознавање образаца, повезивање догађаја и коришћење искуственог знања у откривању и спречавању криминалних активности.

Дисциплина анализе криминала појавила се након формирања лондонске Метрополитан полиције, прве модерне организоване службе за спровођење закона. Детективски огранак ове службе, формиран 1842. године, имао је задатак да користи препознавање образаца за спречавање и решавање злочина. Формалне полицијске службе основане су широм САД током педесетих година XIX века, иако је њихова употреба аналитичких техника заостајала за лондонском праксом (Bachner, 2013).

Почетком XX века америчка савезна влада почела је да прикупља националне податке који су допринели развоју статистике криминала. Статистика морталитета коришћена је за израчунавање стопа убистава, док су градови и државе током двадесетих година XX века прикупљали податке о затворским казнама и хапшењима. Године 1930. Федерални истражни биро добио је овлашћење да прикупља и користи податке о криминалу, што је створило основу за развој каснијих модела анализе криминала (Bachner, 2013).

Приликом дефинисања полицијске аналитике могуће је направити аналогију са пословном аналитиком. У општем смислу, аналитика се може посматрати као процес трансформације података у информације, информација у знање, а знања у одлуке. У литератури се често разликују дескриптивна, дијагностичка, предиктивна, прескриптивна и когнитивна аналитика (Vukmirović et al., 2022). Ова подела је корисна и за разумевање развоја полицијске аналитике, јер показује како се аналитика креће од описа онога што се догодило, преко разумевања узрока, ка предвиђању, препоруци и интелигентној подршци одлучивању.

Полицијска аналитика, у општем случају, бави се анализом криминалних и безбедносно релевантних догађаја у циљу подршке органима за спровођење закона, нарочито у истражном, тактичком, стратешком и превентивном раду (Boba, 2001). У савременом

контексту, она не обухвата само податке о већ извршеним кривичним делима, већ и податке о простору, времену, кретању, саобраћају, јавним догађајима, дигиталним активностима, инфраструктури и другим факторима који могу утицати на безбедносни ризик.

На слици 2.2.1. приказане су фазе развоја полицијске аналитике, од традиционалних, искуствено заснованих приступа до савремених облика аналитике подржаних вештачком интелигенцијом. У односу на класичну поделу аналитичких фаза, приказ је допуњен AI-native развојним правцем и генеративним AI слојем, јер генеративна вештачка интелигенција све више постаје алат за обраду неструктурираних података, синтезу информација, припрему извештаја, формулисање сценарија и подршку аналитичарима. Ови појмови се у овом поглављу само најављују, док се њихово детаљније разграничење и улога у предиктивној полицијској аналитици разматрају у наредном поглављу. Ипак, улога генеративне вештачке интелигенције мора остати помоћна и контролисана: она не може бити замена за формалну статистичку проверу, стручну полицијску процену, људску одговорност и правно утемељено одлучивање (Europol Innovation Lab, 2023; Bommasani et al., 2021).

Слика 2.2.1 Фазе развоја полицијске аналитике

Big Data концепт има посебан значај за прелазак од дескриптивне и дијагностичке аналитике ка предиктивној, прескриптивној и когнитивној аналитици, јер омогућава обраду великих, разноврсних и брзо генерисаних скупова података. У том смислу, полицијска аналитика све више користи приступе науке о подацима, машинског учења и напредне визуелизације, што је у складу са развојем Big Data концепта у званичној статистици и аналитичким системима јавног сектора (Čomić, 2019).

Генеративна вештачка интелигенција има посебну улогу у овој структури, али њену примену треба прецизно ограничити. Она може помоћи у обради великих количина текстуалних података, резимирању службених белешки, изради аналитичких извештаја, формулисању сценарија и превођењу сложених аналитичких резултата у разумљивије форме. Међутим, генеративна вештачка интелигенција не сме бити извор аутоматске полицијске сумње, нити замена за проверљиве статистичке моделе, институционалне процедуре и људску одговорност. Њена улога у полицијској аналитици мора бити помоћна, контролисана и документована, посебно због ризика од халуцинација, нетачних синтеза, пристрасности и непрозирности модела (Europol Innovation Lab, 2023; Bommasani et al., 2021).

У наставку рада дефинишу се и објашњавају основне фазе полицијске аналитике, са посебним акцентом на предиктивну полицијску аналитику као основу за развој унапређеног модела превенције и раног откривања илегалних активности.

2.3. Дескриптивна полицијска аналитика

Циљ дескриптивне полицијске аналитике је да помогне полицији и истражним органима да разумеју шта се догодило, где се догодило, када се догодило и у ком обиму. Она омогућава приказ стања, праћење трендова, идентификацију учесталих појава и почетно препознавање подручја, догађаја или категорија које захтевају додатну анализу. Подаци који се користе у дескриптивној аналитици најчешће потичу из традиционалних полицијских извора и евиденција органа за спровођење закона (Boba, 2001).

Дескриптивна аналитика представља скуп техника које описују стања из прошлости. У статистичкој и аналитичкој литератури она најчешће обухвата два нивоа (Слика 2.3.1):

- визуелизацију података;
- дескриптивну статистичку анализу.

Слика 2.3.1. Нивои дескриптивне аналитике

Визуализација и дескриптивна статистичка анализа података се међусобно допуњују, јер визуелизација омогућава брзо уочавање образаца, док дескриптивна статистичка анализа обезбеђује њихово прецизније квантитативно описивање и проверу.

2.3.1. Визуелизација

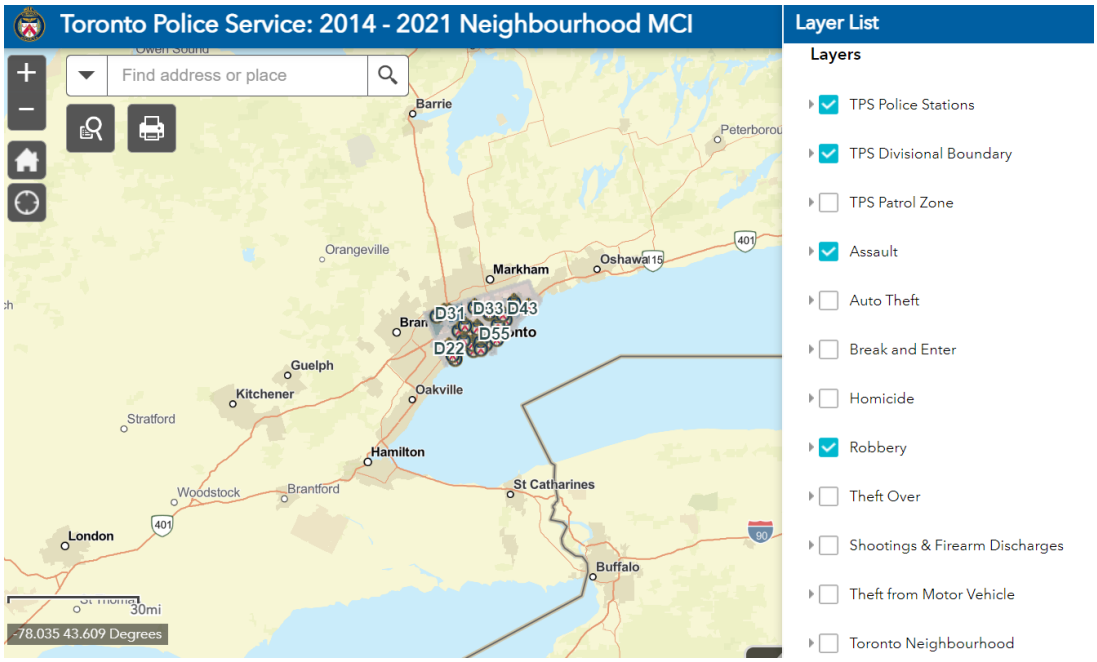
Визуелизација података подразумева представљање података помоћу табела, графикона, мапа, инфографика, интерактивних контролних табли и других визуелних форми. Њена основна сврха је да омогући брзо уочавање образаца, трендова, просторних концентрација, временских промена и потенцијалних аномалија. У области полицијске аналитике

визуелизација има посебан значај зато што полицијски рад увек има и просторну и временску димензију.

Визуелизација података, посебно временских серија и серија структура, заснива се на концептима инфографике, тако што се на брз и једноставан начин, коришћењем графикона, табела, слика и мапа, уз ограничену количину текста, добија увид у посматрану појаву кроз визуелно откривање знања (слика 2.3.2.).

Слика 2.3.2. Концепт инфографике (Čomić, 2019)

Један од типичних примера визуелизације у полицијској аналитици јесу интерактивне криминалне мапе. На њима се могу приказати догађаји према локацији, времену, типу инцидента, интензитету појаве или променама кроз време. Такви системи омогућавају да се подаци представе не само аналитичарима, већ и руководиоцима, патролним службама, локалним самоуправама и, у одређеним случајевима, јавности. На слици 2.3.3. дат је пример интерактивне мапе, која је представљена у форми „dashboard“ или „контролна табла и доступна је на званичном порталу Полицијске службе Торонта, под називом Public Safety Data Portal.



Слика 2.3.3. Главни индикатори криминала у суседствима (Public Safety Data Portal, 2022)

Коришћење мапа у полицијске сврхе има дугу историју. Прво систематско мапирање криминала везује се за XIX век, када су истраживачи почели да визуелизују податке о имовинским деликтима и да их упоређују са социо-демографским карактеристикама простора. Касније развој криминалних мапа показао је да просторни распоред криминалних активности није случајан, већ да се одређени догађаји чешће јављају у одређеним подручјима, улицама, блоковима или типовима окружења (Weisburd & McEwen, 1997).

Испитивање и тумачење образаца полицијских активности у вези са просторно-временским карактеристикама кривичних инцидената означило је развој геодемографије, геоинформатике и GIS приступа у анализи криминала. Ови приступи омогућавају повезивање полицијских података са подацима о становништву, инфраструктури, саобраћају, економским карактеристикама и другим контекстуалним факторима (Ashby & Longley, 2005; Lamnisos et al., 2019).

Геодемографија полази од претпоставке да су људи и домаћинства која живе у истом или сличном просторном окружењу често сличнији једни другима него случајно изабрани појединци из шире популације (слика 2.3.4). У полицијској аналитици овај концепт може бити користан за разумевање просторних образаца ризика, али га треба примењивати

опрезно, јер прекомерно ослањање на просторне и социо-демографске карактеристике може довести до погрешних генерализација или стигматизације одређених подручја (Webber & Burrows, 2018).

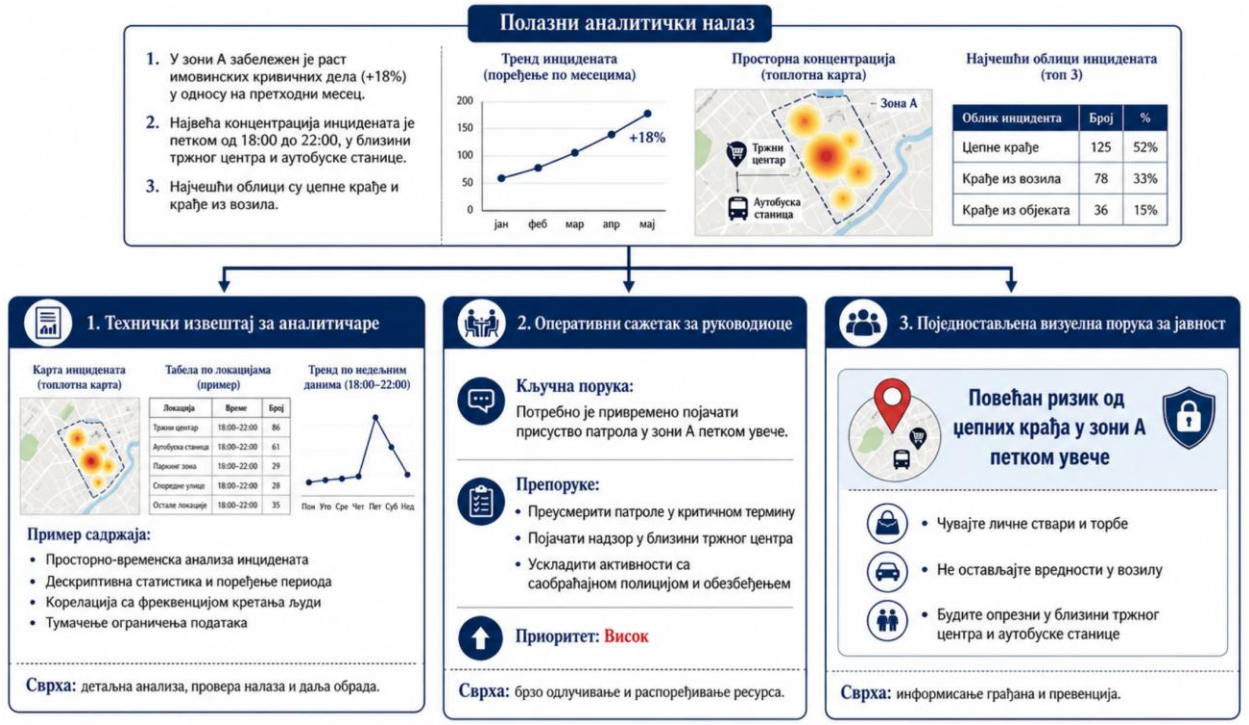
Слика 2.3.4. Геодемографија као основ за разумевање просторних образаца ризика

Истраживања о видљивим полицијским патролама показују да усмерено присуство полиције може допринети смањењу криминала, нарочито када је фокусирано на мале географске локације, односно жаришне тачке у којима је криминал концентрисан (College of Policing, 2021). Систематски преглед 65 студија и 78 тестова hot spots интервенција показује да овакво усмерено деловање ствара статистички значајна, мада просечно мала, смањења укупног криминала и нереда на циљаним локацијама (Braga et al., 2019).

Процена безбедносног ризика неке територије, међутим, не зависи само од броја становника (слика 2.3.5.). Важни фактори су и густина насељености, структура становништва, саобраћајна повезаност, функција гравитационог центра, урбана инфраструктура, типови објеката, социјална култура и динамика кретања људи. Друштвене кризе, миграције, пад животног стандарда и промене животних навика могу додатно променити просторне обрасце ризика и створити потребу за динамичнијим моделима полицијске аналитике (Sekulović, 2018).

Слика 2.3.5. Фактори процене безбедносног ризика територије

Генеративна вештачка интелигенција може имати допунску улогу у визуелизацији полицијских података. Она може помоћи аналитичарима да формулишу описе графикона, објасне уочене обрасце, припреме нацрт аналитичког извештаја, креирају наратив уз мапу ризика или предложе више начина за представљање истих резултата различитим циљним групама. На пример, исти аналитички резултат може бити представљен као технички извештај за аналитичаре, оперативни сажетак за руководиоце или поједностављена визуелна порука за јавност (слика 2.3.6).



Слика 2.3.6. Трансформација аналитичког налаза у технички, оперативни и јавни приказ

Ипак, генеративна вештачка интелигенција не сме самостално тумачити узрочност, нити закључивати о ризику без провере података, јер визуелно убедљив приказ може створити погрешан утисак о прецизности, узрочности или поузданости модела (Europol Innovation Lab, 2023; Bommasani et al., 2021).

2.3.2. Дескриптивна статистичка анализа

Дескриптивна статистичка анализа користи квантитативне и квалитативне податке у циљу описивања посматране појаве. Њена основна улога је да омогући јасан, прегледан и проверљив приказ стања: колико се одређена појава јавља, где се јавља, када се јавља, у којој мери варира и да ли се у подацима могу уочити одређени обрасци. У полицијској аналитици то може обухватити број и структуру инцидената, просторну и временску расподелу догађаја, учесталост појединих врста кривичних дела, карактеристике локација, структуру пријава, као и промене у односу на претходне периоде.

Квантитативни подаци су нумерички и могу бити мерени на ординалној, интервалној или рационалној скали. Њихова анализа најчешће обухвата мере централне тенденције, мере варијабилитета, мере облика расподеле, индексе, стопе, односе и друге показатеље који

омогућавају сажето описивање посматране појаве Табела 2.3.1 (Vuković, Vukmirović & Radojičić, 1998). У полицијском контексту, то могу бити стопе криминалитета по територијалној јединици, просечан број инцидената у одређеном временском интервалу, структура кривичних дела по категоријама, сезонске промене, као и поређења између различитих простора или периода.

Табела 2.3.1. Дозвољене статистике по мерним скалама података

Скала	**Дескриптивне мере**	**Примери статистичких поступака**
Номинална	фреквенције, проценти, модус	табеле контингенције, хи-квадрат тест
Ординална	медијана, квартили, перцентили, рангови	Спирманова корелација рангова, непараметарски тестови
Интервална	аритметичка средина, стандардна девијација, варијанса	t-тест, анализа варијансе, корелациона и регресиона анализа
Рационална	све претходне мере, стопе, односи, индекси	све наведене методе, модели временских серија, напредни статистички модели

Иако је традиционална дескриптивна статистика неопходна основа полицијске аналитике, њена примена има одређена ограничења:

- Прво, она је углавном усмерена на податке који су већ структурирани, класификовани и припремљени за анализу. То значи да најбоље функционише када су подаци у табеларном облику, са јасно дефинисаним варијаблама, категоријама и јединицама посматрања.
- Друго, традиционална статистика добро описује шта се догодило, али сама по себи не објашњава увек контекст, значење и околности у којима је догађај настао.
- Треће, њени резултати могу бити недовољно информативни ако су подаци непотпуни, неуједначено евидентирани, различито кодирани или прикупљени из више институционалних и технолошких извора.

Посебан проблем у полицијској аналитици представљају квалитативни и неструктурирани подаци. Квалитативни подаци су ненумерички и најчешће се мере на номиналној скали. У полицијској аналитици то могу бити типови инцидената, врсте кривичних дела, категорије места, описни извештаји, службене белешке, изјаве, транскрипти разговора, отворени извори и наративни записи. Ови подаци се традиционално анализирају кроз класификацију, ручно кодирање, табеле фреквенција и анализу садржаја. Међутим, такав приступ може бити спор, субјективан и тешко применљив када постоји велики број докумената, различитих формата и неуједначених начина евидентирања.

Наративни извештаји о догађајима представљају посебан изазов, јер садрже важне информације које нису увек лако претвориве у нумеричке променљиве. У једној службеној белешци могу се истовремено налазити подаци о месту, времену, понашању лица, околностима догађаја, процени ризика, сведоцима, начину извршења и могућим везама са другим догађајима. Ако се такви подаци не структурирају, они остају тешко доступни за статистичку анализу. Управо због тога се у савременој полицијској аналитици све више користе методе науке о подацима, укључујући машинско учење, дубоко учење, обраду природног језика и семантичку претрагу Oatley, 2021).

У овом контексту, генеративна вештачка интелигенција може имати важну, али помоћну улогу у припреми и тумачењу дескриптивне статистичке анализе. Њена вредност није у томе да замени статистичку обраду, већ да помогне у прелазу од неструктурираних и наративних извора ка структурираним категоријама, индикаторима и аналитичким питањима (Vukmirović, 2026).

Примена вештачке интелигенције је посебно корисна у раду са текстуалним и наративним изворима, јер може помоћи у:

- резимирању службених белешки,
- издвајању кључних тема,
- препознавању понављајућих образаца,
- формулисању почетних категорија за кодирање и
- припреми предлога структуре за даљу статистичку обраду.

На пример, ако постоји велики број службених белешки о имовинским кривичним делима, генеративна вештачка интелигенција може помоћи да се из текстуалних описа издвоје понављајуће категорије као што су: време догађаја, тип локације, начин извршења, присуство сведока, врста оштећене имовине, понашање осумњиченог или околности које се понављају. Након тога, аналитичар може те категорије проверити, формализовати и претворити у варијабле које су погодне за дескриптивну статистичку анализу. На тај начин генеративна вештачка интелигенција може да убрза припрему података и смањи терет ручног читања великог броја докумената, али не сме да преузме улогу коначног тумача података.

Генеративна вештачка интелигенција може помоћи и у комуникацији резултата дескриптивне анализе (Vukmirović & Jovanović-Milenković, 2025). Исти аналитички резултат може бити представљен као технички извештај за аналитичаре, оперативни сажетак за руководиоце или поједностављена визуелна порука за јавност. У том смислу, генеративна вештачка интелигенција може помоћи у формулисању нацрта извештаја, прилагођавању језика различитим корисницима, објашњавању графикона и табела, изради сажетака и припреми јаснијих наративних интерпретација. Међутим, садржај таквих интерпретација мора бити заснован на провереним подацима и одобрен од стране надлежног аналитичара или службеника.

Због тога генеративна вештачка интелигенција не сме бити третирана као самосталан статистички инструмент. Израчунавање дескриптивних мера, стопа, индекса, табела контингенције и других статистичких показатеља мора бити засновано на проверљивим подацима и репродуктивним аналитичким поступцима, применом статистичког софтвера, програмских језика или контролисаних аналитичких алата. Генеративна вештачка интелигенција може помоћи у припреми, описивању и објашњавању резултата, али не може заменити контролу података, статистичку проверу, стручну процену и одговорност аналитичара. Ово је посебно важно због ризика од нетачних синтеза, халуцинација, погрешног тумачења статистичких односа, преувеличавања закључака и преношења пристрасности које постоје у изворним подацима (Europol Innovation Lab, 2023; Bommasani et al., 2021).

На крају, може се закључити да дескриптивна статистичка анализа има важну улогу у полицијској аналитици јер омогућава да се сложене појаве прикажу на јасан, прегледан и проверљив начин. Она представља основу за све касније фазе анализе: без квалитетног описа података није могуће поуздано утврдити узроке, развијати предиктивне моделе или формулисати препоруке за поступање. У том смислу, генеративна вештачка интелигенција може унапредити припрему, организацију, тумачење и комуникацију аналитичких налаза, али само као подршка дескриптивној статистици, а не као њена замена.

2.4. Дијагностичка полицијска аналитика

Дијагностичка полицијска аналитика, односно полицијска дијагностика, усмерена је на разумевање зашто се одређени догађај или образац појавио. За разлику од дескриптивне аналитике, која одговара на питање шта се догодило, дијагностичка аналитика настоји да повеже људе, догађаје, места, време, имовину, околности и могуће узроке (Boba, 2001). У том процесу користе се корелациона анализа, визуелизација, мапирање, анализа мрежа, анализа садржаја и различити облици аналитичког профилисања догађаја.

У литератури се могу наћи различите класификације полицијске аналитике. Један од утицајних приступа, приказан на слици 2.4.1, разликује криминалистичко-истражну, тактичку, стратешку и административну анализу криминала (Boba, 2001). Ове врсте анализе не треба посматрати као строго одвојене, већ као међусобно повезане аналитичке функције које подржавају различите нивое полицијског рада.

Слика 2.4.1. Дескриптивно-дијагностички процеси полицијске аналитике (Boba, 2001)

Криминалистичко-истражна анализа представља процес повезивања чињеница у конкретним случајевима. Она може укључити анализу начина извршења, карактеристика жртве, места догађаја, доступних доказа, понашања осумњиченог и могућих веза са другим случајевима. Ова врста анализе посебно је значајна код серијских, сложених или тешких кривичних дела, где је потребно повезивати податке из више извора и утврђивати обрасце који нису непосредно видљиви. Описани приступ у литератури се означава као crime linkage analysis или behavioural evidence analysis, где се на основу modus operandi, избора жртве, просторних и временских образаца и понашања учиниоца повезују појединачни случајеви у серију (Turvey, 1999; Woodhams & Labuschagne, 2002; Tonkin et al., 2012).

Тактичка анализа криминала усмерена је на недавно извршене инциденте и потенцијалне криминалне активности, са циљем краткорочног развоја патролних и истражних приоритета и распореда ресурса (Boba, 2001; Beaverton Police Department, 2010; IACA, 2024). Њен циљ је да помогне у решавању текућих проблема, препознавању образаца, идентификацији истражних трагова и усмеравању патролних или истражних активности, нарочито за кривична дела која су се десила у последњим данима или недељама (Boba, 2001; Lum & Koper, 2017). Тактичка анализа посебно анализира како, када и где се догађај

догодио, као и карактеристике жртве, начина извршења, локације, времена, употребљених средстава и понашања осумњичених, како би се идентификовали обрасци и повезале серије догађаја (IACA, 2024; Boba, 2001).

Основне сврхе тактичке анализе криминала су: повезивање случајева и идентификација значајних карактеристика образаца и трендова; идентификација потенцијалних осумњичених, локација или околности повезаних са повишеним ризиком; и подршка расветљавању случајева и планирању оперативног поступања (Boba, 2001; IACA, 2024; Beaverton Police Department, 2010)

Стратешка анализа криминала усмерена је на дугорочније трендове, структуралне факторе и просторне обрасце, за разлику од тактичке анализе која се бави непосредним инцидентима и краткорочним проблемима (Boba, 2001; Beaverton Police Department, 2010; IACA, 2024). Она повезује податке о криминалу са социо-демографским, економским, урбанистичким, саобраћајним и другим факторима, често користећи више извора (полицијске евиденције, податке локалне самоуправе, здравствене и социјалне податке) како би се добила потпунија слика дугорочних проблема и новонасталих ризика (London Strategic Crime Analysis, 2022; LISC/BCJI, 2014). Циљ стратешке анализе није само решавање појединачног случаја, већ разумевање ширих образаца и подршка планирању политика, превентивних програма и распоређивању ресурса (Boba, 2001; Jones & Gwinn, 2017).

Две основне сврхе стратешке анализе криминала су

1. идентификација и анализа дугорочних проблема, као што су концентрација одређених кривичних дела, насиље, наркокриминал, крађе возила или имовински деликти;
2. процена релевантних одговора, мера и процедура, укључујући превентивне програме, организационе промене и промене у патролном раду.

Административна анализа криминала односи се на комуникацију резултата анализе са различитим стејкхолдерима. Она се не односи пре свега на статистичку анализу, већ на припрему, прилагођавање и представљање аналитичких налаза. Циљне групе могу бити руководиоци, полицијски службеници, грађани, медији, органи јавне управе, локалне

заједнице, невладине организације или други институционални актери. У овој врсти анализе посебно су важни јасноћа, тачност, правна ограничења, поверљивост и заштита осетљивих података.

Генеративна вештачка интелигенција може бити корисна управо у административној и аналитичко-комуникационој функцији, јер може помоћи у припреми различитих верзија извештаја, резимеа, објашњења и сценарија. Међутим, у криминалистичко-истражној и тактичкој анализи њена употреба мора бити посебно контролисана, јер погрешно генерисан закључак, непроверена синтеза или нетачно повезивање случајева могу имати озбиљне последице. Зато сваки AI-генерисани аналитички садржај мора бити проверен од стране овлашћеног аналитичара или службеника, уз јасно документовање извора, ограничења и степена поузданости.

2.5. Извори података у дескриптивној аналитици и полицијској дијагностици

Из прегледа коришћених метода може се закључити да се у дескриптивној аналитици и полицијској дијагностици традиционално користе полицијски извори података засновани на криминалистичко-обавештајном раду, пријавама, записницима, службеним белешкама, позивима грађана, евиденцијама и оперативним сазнањима (Boba, 2001; Ratcliffe, 2007). Ови извори обухватају пре свега евиденције о пријављеним кривичним делима и прекршајима, calls for service, извештаје патролних и истражних службеника, као и интерне аналитичке и обавештајне производе.

Међутим, савремена полицијска аналитика све више користи и друге изворе података који нису директно настали у полицијском систему, али могу бити релевантни за разумевање безбедносних образаца и контекста ризика (Malleson & Andresen, 2015; Gstrein et al., 2019). Такви извори могу обухватити (слика 2.5.1.):

- званичне статистичке податке (демографске, економске, здравствене);
- демографске и социо-економске податке на нивоу насеља или мањих просторних јединица;
- геопросторне податке и слојеве у ГИС системима (урбанистичка структура, инфраструктура, јавни простори);

- податке о саобраћају и кретању (саобраћајни детектори, GPS, јавни превоз);
- податке из система паметног града и IoT уређаја (камере, сензори, паметна расвета, интелигентно управљање саобраћајем);
- финансијске, пореске и административне податке, у мери у којој је њихова употреба правно дозвољена;
- податке из отворених извора и јавних регистара;
- податке са друштвених медија и других он-лајн платформи (ambient population, просторна перцепција безбедности);
- сензорске, видео и аудио податке из система надзора и мониторинга;
- наративне извештаје, службене белешке и друге неструктуриране текстове који се могу анализирати техникама обраде природног језика (NLP).

Слика 2.5.1. Извори података у дескриптивној аналитици и полицијској дијагностици

Посебну пажњу треба посветити квалитету сензорских, IoT и PIoT података. Иако ови подаци могу значајно унапредити просторну и временску осетљивост полицијске аналитике, они не смеју бити третирани као аутоматски поуздани или неутрални. Сензори могу производити шум, непотпуне записе, дупликате, погрешна мерења, временски неусклађене сигнале или податке настале услед техничког квара, лоше калибрације, слабог мрежног сигнала или прекида у комуникацији. Поред тога, у безбедносном контексту мора се узети у обзир и могућност намерне манипулације подацима, као што су spoofing, лажни сигнали, компромитовање уређаја или убацивање нетачних података у систем. Због тога сензорски и PIoT подаци морају проћи поступке валидације, филтрирања, временског усклађивања, провере интегритета и поређења са другим изворима пре него што се користе у дијагностичкој или предиктивној аналитици.

Употреба ових извора значајно повећава аналитички потенцијал, али истовремено захтева јасна правила о законитости обраде, сврси употребе, минимизацији података, заштити приватности, квалитету података и спречавању пристрасности (Brayne, 2017; Babuta & Oswald, 2019; Richardson et al., 2019). Посебно је важно правити разлику између података који су погодни за опис стања (descriptive), података који могу указати на узроке (diagnostic) и података који се смеју користити у предиктивним моделима (predictive), јер сврха обраде, правни основ и ризици нису исти у свим случајевима (Gstrein et al., 2019; Babuta & Oswald, 2019). Не може сваки доступан податак бити легитиман или користан у полицијској аналитици; напротив, неконтролисано преузимање и повезивање података може довести до кршења права, систематске пристрасности и губитка поверења јавности.

2.6. Закључна разматрања о дескриптивној аналитици и полицијској дијагностици

Дескриптивна аналитика и полицијска дијагностика представљају полазну основу савремене полицијске аналитике. Иако се често посматрају као нижи или почетни нивои аналитике, њихова улога је суштинска, јер без поузданог описа стања, разумевања контекста и повезивања релевантних фактора није могуће развијати валидне предиктивне моделе, нити формулисати одговорне препоруке за поступање. Дескриптивна аналитика омогућава да се утврди шта се догодило, где, када и у ком обиму, док полицијска дијагностика настоји да објасни зашто се одређени догађај или образац појавио, који

фактори су са њим повезани и како се различити догађаји, лица, простори, времена и околности међусобно односе.

У овој глави показано је да се дескриптивна полицијска аналитика не може свести само на статистичке табеле и статичне извештаје. Њен развој је тесно повезан са визуелизацијом података, криминалним мапама, геоинформационим системима, геодемографским приступом и анализом просторних образаца ризика. Визуелизација омогућава брзо уочавање концентрација, трендова и аномалија, док дескриптивна статистичка анализа обезбеђује прецизније квантитативно описивање и проверу уочених образаца. Посебан значај има просторна димензија, јер безбедносни ризик не зависи само од броја становника, већ и од густине насељености, структуре становништва, саобраћајне повезаности, функције гравитационог центра, урбане инфраструктуре, типова објеката, социјалне културе и динамике кретања људи.

Друштвено-економске кризе, миграције, пад животног стандарда, промене животних навика, убрзана дигитализација и развој паметних градова додатно усложњавају просторне и временске обрасце ризика. Због тога савремена полицијска аналитика мора да се ослања не само на традиционалне полицијске изворе података, као што су пријаве, записници, службене белешке, позиви грађана, евиденције и оперативна сазнања, већ и на допунске изворе података: званичну статистику, геопросторне податке, демографске и социо-економске показатеље, податке о саобраћају и кретању, IoT и сензорске податке, податке из система паметног града, отворене изворе, јавне регистре, друштвене медије и неструктуриране текстуалне изворе. Управо повезивање ових извора омогућава да се безбедносни ризици сагледају као просторни, временски, друштвени, технолошки и организациони феномени.

Истовремено, традиционална дескриптивна статистика има одређена ограничења. Она најбоље функционише када су подаци структурирани, уједначено евидентирани и припремљени за анализу. Међутим, у полицијском раду велики део релевантних информација налази се у неструктурираним или полу-структурираним облицима: службеним белешкама, описним извештајима, изјавама, транскриптима, наративним записима, видео и аудио садржајима, као и подацима из отворених извора. Такви подаци често садрже важне информације о начину извршења, околностима догађаја, понашању

учесника, типу локације, процени ризика и могућим везама са другим догађајима, али нису одмах погодни за класичну статистичку обраду. Зато се у савременој полицијској аналитици све више користе методе науке о подацима, машинског учења, обраде природног језика, семантичке претраге и напредне визуелизације.

У том контексту, генеративна вештачка интелигенција може имати значајну, али искључиво помоћну и контролисану улогу. Она може помоћи у резимирању службених белешки, издвајању кључних тема, препознавању понављајућих образаца, предлагању почетних категорија за кодирање, припреми структуре за даљу статистичку анализу и прилагођавању аналитичких резултата различитим корисницима. Исти аналитички резултат може бити представљен као технички извештај за аналитичаре, оперативни сажетак за руководиоце или поједностављена визуелна порука за јавност. Међутим, генеративна вештачка интелигенција не сме бити извор самосталне полицијске сумње, нити замена за проверу података, статистичку анализу, стручну полицијску процену, правно утемељено одлучивање и институционалну одговорност. Њена употреба мора бити документована, проверљива и подложна људској контроли, посебно због ризика од халуцинација, нетачних синтеза, погрешног тумачења узрочности и репродуковања постојећих пристрасности у подацима.

Полицијска дијагностика, као други ниво анализе, омогућава да се подаци не посматрају само као збир евидентираних догађаја, већ као систем односа између људи, места, времена, начина извршења, имовине, околности и институционалног контекста. Криминалистичко-истражна, тактичка, стратешка и административна анализа криминала показују да полицијска аналитика има више функција: подршку истрази, препознавање образаца, планирање ресурса, процену дугорочних проблема и комуникацију аналитичких налаза различитим стејкхолдерима. На тај начин дескриптивна и дијагностичка аналитика припремају податке, појмове, индикаторе и обрасце који су неопходни за развој предиктивне полицијске аналитике.

На основу анализе литературе и приказаних концепата може се закључити да дескриптивна и дијагностичка аналитика већ садрже почетне елементе предикције. Анализа простора омогућава једнодимензионално разумевање питања где се ризик концентрише. Анализа времена и простора омогућава дводимензионално разумевање питања где и када се

одређени ризици јављају. Анализа времена, простора, догађаја и контекста омогућава вишедимензионално разумевање питања где, када, како и зашто се ризици појављују. Управо овај прелаз — од описа стања, преко разумевања узрока, ка препознавању образаца и процени будућег ризика — представља основу за предиктивну полицијску аналитику.

Овим се отвара простор за наредно поглавље, у којем се предиктивна полицијска аналитика не посматра само као техничко предвиђање будућих инцидената, већ као део ширег циклуса разумевања, одлучивања, превентивног деловања и евалуације исхода. Тек када полицијске управе и други актери безбедности разумеју просторне, временске, друштвене, технолошке и организационе обрасце ризика, могу планирати мере које не реагују само на последице, већ делују на услове у којима ризици настају (Bachner, 2013).

3. Предиктивна полицијска аналитика

У претходном поглављу размотрене су дескриптивна аналитика и полицијска дијагностика као прве две фазе полицијске аналитике. Њихова основна улога је да омогуће разумевање догађаја који су се већ десили: где су се догодили, када су се догодили, у ком обиму су се јавили и који фактори могу објаснити њихов настанак. На тај начин ове фазе обезбеђују неопходну основу за развој предиктивне полицијске аналитике. За разлику од њих, предиктивна полицијска аналитика усмерена је ка процени будућих ризика, односно ка питању шта би се могло догодити, где, када и под којим условима. Њена сврха није само предвиђање могућих инцидената, већ подршка благовременом, превентивном и пропорционалном полицијском деловању.

3.1. Предиктивна полицијска аналитика и предиктивна полиција

Полицијска аналитика не замењује конвенционалне полицијске методе, већ их унапређује применом напредних статистичких модела, алгоритама машинског учења, геопросторне анализе и система подршке одлучивању (National Institute of Justice, 2014). Последњих година све већи број полицијских управа широм света примењује различита софтверска и аналитичка решења за подршку у доношењу одлука, нарочито у области ефикаснијег распоређивања ресурса, усмеравања патрола, препознавања просторних и временских образаца криминала и превентивног деловања (Ratcliffe, 2004).

У научној и стручној литератури за ову област најчешће се користи термин „предиктивна полиција“ (енг. predictive policing). Међутим, у овој дисертацији као основни термин користи се „предиктивна полицијска аналитика“, јер он прецизније означава аналитички део процеса: прикупљање, припрему, обраду и анализу података, развој модела, тумачење резултата и припрему информација за доносиоце одлука. Термин „предиктивна полиција“ је шири, јер поред аналитичке компоненте обухвата и оперативну примену резултата, организацију полицијског поступања, распоређивање ресурса, избор превентивних мера, правне и етичке услове примене, као и евалуацију исхода предузетих мера.

Имајући у виду наведено, у овој дисертацији прави се разлика између појмова „предиктивна полицијска аналитика“ и „предиктивна полиција“. Предиктивна полицијска аналитика

означава аналитички део процеса: систематизацију и интеграцију података, примену статистичких, алгоритамских и метода вештачке интелигенције, развој модела, процену ризика, тумачење резултата и припрему аналитичких налаза за доносиоце одлука. Предиктивна полиција је шири појам, јер поред аналитичке компоненте обухвата и оперативну примену резултата, организацију полицијског поступања, распоређивање ресурса, избор превентивних мера, правне и етичке услове примене, као и евалуацију исхода.

Због тога ће се у наставку дисертације као основни термин користити „предиктивна полицијска аналитика“, када се говори о моделима, подацима, методама, аналитичком процесу и процени ризика. Термин „предиктивна полиција“ користиће се када се разматра шири институционални и оперативни контекст, односно када се говори о примени аналитичких резултата у полицијском раду или када се преноси уобичајени термин из међународне литературе — predictive policing.

Слика 3.1.1. Развојни нивои полицијске аналитике као основа предиктивне полиције

Као што је приказано на слици 3.1.1, предиктивна полицијска аналитика не настаје изоловано, већ се развија на основу претходних аналитичких нивоа. Дескриптивна полицијска аналитика обезбеђује одговор на питање шта се догодило, дијагностичка полицијска аналитика помаже да се разуме зашто се нешто догодило, док предиктивна компонента настоји да процени шта би се могло догодити у будућности. На тај начин се повећава вредност информација и ствара основа за благовремено, превентивно и пропорционално полицијско деловање.

У досадашњој пракси, предиктивна полиција је често била усмерена на прве фазе полицијске аналитике: дескриптивну и дијагностичку анализу, односно на прикупљање, систематизацију и обраду широког спектра структурираних и неструктурираних података у циљу бољег разумевања трендова, образаца и жаришних тачака криминала. Ове фазе су неопходне, јер без поузданог описа онога што се догодило и разумевања узрока и контекста није могуће развити валидне предиктивне моделе. Тек на тој основи предиктивна полицијска аналитика може да пређе са питања шта се догодило и зашто се догодило на питање шта би се могло догодити, где, када и под којим условима.

Посебан правац даљег развоја представља **AI-native полицијска аналитика**, односно полицијска аналитика изворно заснована на вештачкој интелигенцији. У овој дисертацији овај појам се користи као концептуална ознака за приступ у којем вештачка интелигенција, машинско учење, IoT/PIoT инфраструктура, хијерархијска обрада података и системи подршке одлучивању нису само додатни технолошки алати, већ интегрисани елементи аналитичког циклуса. Иако термин AI-native полицијска аналитика још увек није устаљен у научној и стручној литератури, у савременој пракси већ се могу уочити сродни приступи, као што су AI-driven policing software, AI-supported policing и AI in policing, који указују на све већу интеграцију вештачке интелигенције у полицијске процесе, од анализе података и препознавања образаца до подршке одлучивању и превентивном деловању (Innefu Lab, 2025; National Policing Institute, 2026).

Овакав развој треба посматрати у ширем контексту foundation модела, великих језичких модела и савремених система вештачке интелигенције, који отварају значајне могућности за обраду неструктурираних података, синтезу информација, претрагу докумената, припрему извештаја и подршку аналитичарима, али истовремено носе ризике нетачних

синтеза, пристрасности, непрозирности и неодговарајуће употребе у осетљивим институционалним контекстима (Bommasani et al., 2021; Europol Innovation Lab, 2023). Такав приступ већ се развија у контексту паметних градова и Police Internet of Things (PIoT) архитектуре, где се оперативно праћење, тактичко предвиђање и стратешко одлучивање повезују кроз edge, fog и cloud нивое обраде података (Dragović et al., 2026). Ипак, AI-native полицијска аналитика мора бити схваћена као систем подршке људском одлучивању, а не као механизам аутоматизоване полицијске процене или самосталног доношења одлука.

3.2. Дефинисање предиктивне полицијске аналитике

Преглед дефиниција предиктивне полиције и предиктивне полицијске аналитике дат је на основу анализе доступне стручне и научне литературе.

Предиктивна полиција је одскора тема стручних и научних радова. Најстарији документ који говори о предиктивној полицији датира из 2010. године. Тема је била посебно заступљена у широком спектру криминолошких часописа, али и у часописима који се баве информатиком, нарочито Big Data приступом, током 2017. и 2018. године (Meijer & Wessels, 2019). Поред тога, могу се пронаћи резултати (углавном америчких и британских) студија, који су се претежно бавиле евалуацијом успешности предиктивне полиције. Што се тиче академских књига, RAND корпорација је објавила две најзначајније публикације из ове области (Perry et al., 2013; Hunt, Saunders & Hollywood, 2014). Најважнији светски издавачи су објављивали књиге или поглавља књиге која се односе на предиктивну полицију. Доступни конференцијски радови су са конференција о рачунарству и информатици и криминалистици.

Према очекивању, из прегледа и анализе литературе може се закључити да јединствена дефиниција предиктивне полицијске аналитике не постоји али се може извући пресек њених кључних карактеристика, за које је постигнут консензус (Meijer & Wessels, 2019).

Многи радови указују на то да предиктивни рад полиције подразумева примену квантитативних метода и техника за предвиђање **где** би се криминалне активности могле појавити у (скорој) будућности (Camacho-Collados & Liberatore, 2015).

Један број аутора проширује дефиницију предиктивне полиције увођењем концепта „**где и када**“, (не само „где“): „Предиктивна полиција је концепт који је изграђен на премиси да је могуће предвидети где и када ће се злочини поново догодити у будућности коришћењем софистициране компјутерске анализе информација о раније почињеним злочинима“ (Norton, 2013).

Perry et al. (2013) користе мало другачију концептуализацију која се не фокусира само на место и време, већ и на **идентификацију појединаца** – потенцијалних починилаца: „Предиктивна полиција је примена аналитичких метода – посебно квантитативних техника - у циљу идентификације вероватне мете за полицијску интервенцију ради спречавања криминала или решавања прошлих злочина на бази статистичких предвиђања”

Већина аутора истиче проблем пристрасности и праведности алгоритма на којима се заснива предиктивна полиција, транспарентности технологија, као и правна и етичка питања (Vuković, Čisar, Kuk & Popović, 2021).

Водећи рачуна о проблему, предмету и циљевима истраживања, у овој дисертацији користи се следећа дефиниција:

Предиктивна полицијска аналитика представља приступ полицијском раду заснован на подацима, који обухвата систематизацију, интеграцију и анализу података из различитих извора, применом статистичких, алгоритамских и метода вештачке интелигенције, у циљу процене повећане вероватноће појаве криминалних и других безбедносно релевантних активности у одређеном простору, времену, контексту или у вези са одређеним обрасцима понашања. Сврха оваквог приступа није аутоматско доношење полицијских одлука, већ подршка развоју превентивних мера, тактичком и стратешком планирању, ефикаснијем распоређивању ресурса и раном откривању ризика, уз обавезну људску контролу, правну утемељеност, етичку прихватљивост и проверљивост аналитичких поступака.

У односу на ужу дефиницију предиктивне полицијске аналитике, која се најчешће заснива на анализи података о претходно извршеним кривичним делима, овде се полази од ширег схватања предиктивне полицијске аналитике. Она не обухвата само податке о криминалним активностима, већ и геопросторне, временске, демографске, социо-економске, саобраћајне, сензорске, IoT, административне, отворене и неструктуриране податке који могу бити

релевантни за разумевање безбедносног ризика. Због тога се уместо појма прикупљање података наглашава систематизација и интеграција података, јер аналитички процес не подразумева само преузимање података, већ њихово повезивање, чишћење, структурирање, контекстуализацију и припрему за моделовање и одлучивање.

Овако дефинисана предиктивна полицијска аналитика може се приказати као систем који повезује више група извора података, аналитичке методе, процену ризика, примену резултата и контролне механизме. На слици 3.2.1. приказан је концептуални оквир предиктивне полицијске аналитике, у којем се посебно наглашава да резултат аналитике није аутоматска полицијска одлука, већ подршка људском, правно утемељеном и проверљивом одлучивању.

Слика 3.2.1. Концептуални оквир предиктивне полицијске аналитике

Као што је приказано на слици 3.2.1, предиктивна полицијска аналитика није изолован алгоритам, већ повезан аналитички систем. Њен улаз чине различити извори података: полицијске евиденције, геопросторни и временски подаци, демографски и социо-економски показатељи, сензорски и IoT/PIoT подаци, административни и отворени подаци, као и неструктурирани текстуални, сликовни и видео садржаји. Ови подаци се систематизују, интегришу и анализирају применом статистичких, алгоритамских и метода вештачке интелигенције.

Излаз такве анализе није коначна одлука, већ процена повећане вероватноће безбедносно релевантних активности у одређеном простору, времену, контексту или у вези са одређеним обрасцима понашања. Та процена може да подржи превентивне мере, тактичко и стратешко планирање, распоређивање ресурса и рано откривање ризика. Међутим, целокупан процес мора бити ограничен јасним контролним механизмима: људском контролом, правном утемељеношћу, етичком прихватљивошћу, проверљивошћу поступака и забраном аутоматског доношења полицијских одлука.

У односу на оригиналну дефиницију (Meijer & Wessels, 2019), уместо процеса прикупљања података о криминалу, у овој дисертацији наглашава се систематизација, интеграција и анализа података. Разлог за то је што аналитички процес не подразумева само преузимање података, већ њихово повезивање, чишћење, структурирање, контекстуализацију и припрему за моделовање и одлучивање. Поред тога, предмет анализе нису само подаци о већ извршеном криминалу, већ и шири скуп података који могу бити релевантни за разумевање безбедносног ризика и рано откривање илегалних активности.

3.3. Улога података у предиктивној полицијској аналитици

Предиктивна полицијска аналитика не ослања се само на податке о већ извршеним кривичним делима, већ користи шири скуп података који могу бити релевантни за разумевање и процену безбедносног ризика. У претходном поглављу приказано је да савремена полицијска аналитика, поред традиционалних полицијских извора, све више укључује геопросторне, временске, демографске, социо-економске, административне, сензорске, IoT/PIoT, видео, аудио, текстуалне и отворене податке. У овом поглављу

нагласак више није на самом набрајању извора, већ на начину на који се ти подаци систематизују, интегришу и користе за процену будућег ризика.

У том смислу, подаци у предиктивној полицијској аналитици имају другачију функцију него у дескриптивној и дијагностичкој аналитици. У дескриптивној аналитици они служе да се опише шта се догодило, а у дијагностичкој да се разуме зашто се одређени догађај или образац појавио. У предиктивној аналитици исти или проширени скупови података користе се за процену где, када, у ком контексту и под којим условима може доћи до повећаног ризика од криминалних или других безбедносно релевантних активности.

Због тога се у овој дисертацији посебно наглашава разлика између доступности података и њихове аналитичке употребљивости. Не може сваки доступан податак бити аутоматски укључен у предиктивни модел. Подаци морају бити релевантни за предмет анализе, правно дозвољени за обраду, методолошки проверљиви, довољно квалитетни и употребљени на начин који не производи неоправдану пристрасност, стигматизацију простора или угрожавање права грађана. Посебно је важно разликовати податке који су погодни за опис стања, податке који помажу у разумевању узрока и податке који се могу оправдано користити за предиктивно моделовање.

Развој вештачке интелигенције додатно проширује могућности предиктивне полицијске аналитике, нарочито у раду са великим, разноврсним и неструктурираним подацима (Oatley, 2021). Машинско учење, обрада природног језика, анализа слика и видео-записа, семантичка претрага и модели за препознавање образаца могу унапредити способност система да уочи правилности које нису лако видљиве класичним аналитичким приступима. Међутим, ови алати не мењају суштински захтев да предиктивна полицијска аналитика мора бити проверљива, контролисана и усмерена на подршку одлучивању, а не на аутоматско доношење полицијских одлука.

Посебно место у савременом развоју има генеративна вештачка интелигенција. Њена улога у предиктивној полицијској аналитици није да самостално предвиђа ризик или означава појединце, групе или просторе као сумњиве. Генеративна вештачка интелигенција може бити корисна као помоћни слој у припреми података, резимирању наративних извора, издвајању релевантних тема, формулисању аналитичких питања, припреми сценарија,

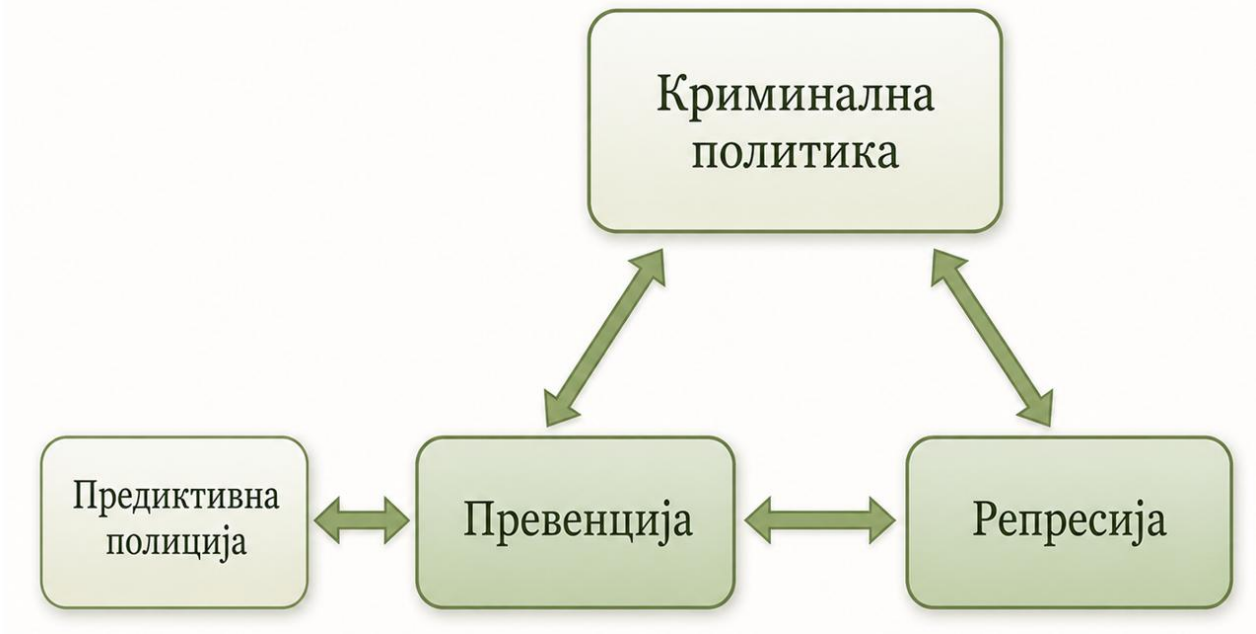
објашњавању резултата модела и прилагођавању извештаја различитим корисницима. Она може допринети бржем преласку од неструктурираних извора ка структурираним категоријама и индикаторима, али сваки такав резултат мора бити проверен, документован и одобрен од стране стручног аналитичара или овлашћеног службеника.

На основу прегледа и анализе литературе може се закључити да појам „предиктивна полиција“ у савременим радовима све чешће има шире значење од саме статистичке прогнозе криминалних активности. Он обухвата и елементе прескриптивне, когнитивне и AI-native аналитике, посебно када се предиктивни модели повезују са системима подршке одлучивању, IoT/PIoT инфраструктуром, сензорским подацима и алгоритмима вештачке интелигенције. Ипак, у овој дисертацији термин „предиктивна полицијска аналитика“ користи се као прецизнији израз за аналитички део тог процеса, док се термин „предиктивна полиција“ користи за шири оперативни, организациони и институционални концепт који обухвата и примену аналитичких резултата у полицијском раду.

3.4. Предиктивна полиција и превенција

Основна карактеристика предиктивне полиције као ширег оперативног концепта јесте усмеравање полицијског рада ка превенцији и раном откривању илегалних, односно криминалних активности. Ово означава померање полицијског приступа са реактивног ка превентивном деловању. Превенција криминала може се дефинисати као предвиђање, препознавање и процена ризика од криминала, као и покретање активности ради његовог отклањања или смањења (Fennelly, 2020).

Уколико су дилеме и постојале, у многим научним и стручним радовима је наглашено да се предиктивна полиција може сматрати обликом превентивног рада полиције (слика 3.4.1) - „превенција усмерена ка узроцима ризика“ (*upstream prevention*) (Van Brakel & De Hert, 2011; Bennett Moses & Chan, 2018; Meijer & Wessels, 2019).



Слика 3.4.1. Превентивна улога предиктивне полиције

Може се извући паралела у пословима и задацима полицијске аналитике према остварењу полицијских циљева: **Тактички** циљеви се остварују расветљавањем кривичних дела, применом дескриптивне и дијагностичке аналитике, док се предиктивна, а нарочито прескриптивна и когнитивна аналитика баве остваривањем **стратешких** полицијских циљева (Stupar, 2021).

Као што је приказано на слици 3.4.2, превенција криминала заснива се на три основна стратешка оквира: примарној превенцији, стратегијама кривичног правосуђа и стратегијама спровођења закона (Bachner, 2013). Сваки од ових оквира има различит предмет деловања, али сви заједно чине интегрисан приступ смањењу ризика од криминалног понашања и унапређењу безбедности.

Слика 3.4.2. Три стратешка оквира превенције криминала

Први стуб односи се на примарну превенцију и усмерен је на смањење фактора ризика који могу допринети криминалном понашању. Други стуб обухвата стратегије кривичног правосуђа, чији је циљ спречавање повратa код познатих преступника. Трећи стуб чине стратегије спровођења закона, које су усмерене на смањење вероватноће да се кривично дело догоди у одређеном простору и времену (слика 3.4.3).

Слика 3.4.3. Предиктивне полицијске методе у оквиру стратегија спровођења закона
Извор: адаптирано према Perry et al. (2013).

Као што је приказано на слици 3.4.3, предиктивне полицијске методе у оквиру стратегија спровођења закона могу се груписати у четири основне категорије: методе предвиђања злочина, методе предвиђања преступника, методе предвиђања идентитета починилаца и методе предвиђања жртава злочина. Оваква класификација показује да се предиктивна полицијска аналитика не своди искључиво на процену места и времена извршења кривичних дела, већ обухвата и шири спектар аналитичких приступа усмерених на разумевање ризика, учесника и околности у којима се криминалне активности могу јавити.

Посебан значај ове поделе огледа се у томе што различите категорије метода подразумевају различите врсте података, аналитичких поступака и нивоа осетљивости. Док су методе предвиђања злочина најчешће усмерене на просторне и временске обрасце, методе предвиђања преступника, починилаца и жртава отварају сложенија питања приватности, законитости, правичности и ризика од алгоритамске пристрасности. Због тога је неопходно да се њихова примена заснива на јасним правним и етичким оквирима, као и на обавезној људској контроли у тумачењу и употреби аналитичких резултата.

3.5. Процес предиктивне полицијске аналитике

Предиктивна полицијска аналитика може се посматрати као процес који повезује прикупљање и систематизацију података, аналитичку обраду, процену будућег ризика, полицијско поступање и евалуацију исхода. У том смислу, она не представља само техничку примену алгоритма за предвиђање, већ шири аналитичко-оперативни циклус у којем се подаци претварају у информације, информације у процену ризика, а процена ризика у основу за превентивно и пропорционално полицијско деловање.

У литератури се процес предиктивне полицијске аналитике често приказује као низ међусобно повезаних фаза. Овај приступ одговара моделима у којима се предиктивна полицијска аналитика описује као низ фаза од прикупљања података, преко анализе и дизајна интервенције, до мерења утицаја на криминал и повратне корекције модела (Perry et al., 2013; National Institute of Justice, 2014; Fitzpatrick et al., 2019).

У поједностављеном облику, овај процес обухвата четири основне целине: прикупљање и интеграцију података, анализу и предвиђање, полицијско поступање и кривични поступак, односно накнадну институционалну обраду догађаја. Фазе процеса предиктивне полицијске аналитике приказане су на слици 3.5.1.

Слика 3.5.1. Процес предиктивне полицијске аналитике

Извор: адаптирано према E&Y (2018)

Прва фаза односи се на прикупљање, систематизацију и интеграцију података. У овој фази користе се подаци из полицијских евиденција, пријава, позива грађана, оперативних сазнања, службених белешки, али и подаци из ширег окружења, као што су геопросторни, саобраћајни, демографски, социо-економски, административни, сензорски и IoT/PIoT подаци. Циљ ове фазе није само акумулација података, већ њихово повезивање, чишћење, стандардизација, контекстуализација и припрема за аналитичку обраду. Квалитет ове фазе директно утиче на квалитет свих каснијих аналитичких резултата.

Друга фаза обухвата анализу и предвиђање. У њој се применом статистичких метода, машинског учења, геопросторне анализе, временских серија, класификационих модела, кластеризације, анализе образаца и других аналитичких поступака процењује вероватноћа појаве безбедносно релевантних догађаја. У зависности од циља анализе, предвиђање може бити усмерено на простор, време, тип догађаја, обрасце понашања, потенцијалне преступнике, идентитет починилаца или ризик од виктимизације. Излаз ове фазе није „готова одлука“, већ аналитички налаз: процена ризика, мапа жаришта, листа приоритета, сценарио могућег развоја догађаја или препорука за даље поступање.

Трећа фаза односи се на полицијско поступање. У овој фази аналитички резултати постају основ за планирање и реализацију конкретних мера: усмеравање патрола, појачано присуство на ризичним локацијама, превентивни рад у заједници, праћење одређених образаца, сарадњу са другим службама или прилагођавање тактичких и оперативних планова. Ова фаза је посебно осетљива јер се аналитичка процена мора превести у поступање које је законито, сразмерно, оправдано и недискриминаторно. Због тога предиктивна полицијска аналитика не сме да функционише као механизам аутоматског одлучивања, већ као систем подршке овлашћеним службеницима и руководиоцима.

Четврта фаза обухвата кривични поступак, институционалну обраду догађаја и повратну информацију. Уколико полицијско поступање доведе до откривања или спречавања кривичног дела, резултати поступања улазе у формалне евиденције, извештаје, доказни материјал и кривичноправни процес. Истовремено, исходи поступања, успешност интервенција, тачност предикција, неочекивани догађаји и евентуалне грешке постају нови подаци који се могу користити за унапређење модела. На тај начин процес предиктивне

полицијске аналитике није затворен линеарни ток, већ динамичан циклус учења и корекције.

Посебно је важно нагласити да се у овом процесу одлуке могу мењати на основу нових сазнања. Ако анализа покаже повећан ризик на одређеној локацији, полиција може привремено променити распоред ресурса. Ако накнадни подаци покажу да се ризик није реализовао, да је дошло до померања жаришта или да је првобитна процена била недовољно поуздана, одлука се мора кориговати. Управо та способност прилагођавања представља једну од кључних предности предиктивне полицијске аналитике у односу на статичне аналитичке извештаје.

Упоређивањем овог модела са OSCE моделом криминалистичко-обавештајног циклуса може се закључити да предиктивна полицијска аналитика не напушта конвенционалне полицијске концепте, већ их надограђује (Organization for Security and Co-operation in Europe [OSCE], 2017).Криминалистичко-обавештајни циклус традиционално обухвата усмеравање, прикупљање, обраду, анализу, дистрибуцију и употребу обавештајних сазнања. Предиктивна полицијска аналитика задржава ову основну логику, али је проширује применом већих и разноврснијих скупова података, напредних аналитичких метода, алгоритамских модела, машинског учења и система подршке одлучивању.

Слика 3.5.2. Криминалистичко-обавештајни циклус у раду полиције

Извор: адаптирано према OSCE (2017).

Сличност између ова два приступа показује да предиктивна полицијска аналитика није потпуно нова логика полицијског рада, већ савремени технолошки и методолошки развој постојећег обавештајно-аналитичког приступа. Разлика је у томе што предиктивна полицијска аналитика у већој мери користи податке у реалном или скоро реалном времену, интегрише више извора, примењује напредне моделе предвиђања и омогућава бржу корекцију поступања на основу повратних информација.

У условима паметних градова и хибридног физичко-сајбер окружења, овај процес добија додатну технолошку димензију. PIoT архитектура омогућава да се поједине фазе процеса распореде по различитим нивоима обраде: edge ниво може подржати прикупљање и прелиминарну обраду података са камера, сензора и IoT уређаја; fog ниво може подржати краткорочну аналитику, координацију и тактичко одлучивање; док cloud ниво омогућава дугорочну интеграцију података, стратешку анализу, евалуацију и управљање моделима. На тај начин процес предиктивне полицијске аналитике постаје хијерархијски организован систем подршке одлучивању.

На основу наведеног може се издвојити и трећи, савремени приступ, који се може означити као AI-native предиктивна полицијска аналитика. За разлику од класичног криминалистичко-обавештајног циклуса, који се ослања на прикупљање, обраду, анализу и употребу обавештајних сазнања, и за разлику од предиктивне полицијске аналитике, која уводи статистичке и алгоритамске моделе предвиђања, AI-native приступ подразумева да су вештачка интелигенција, машинско учење, обрада природног језика, анализа слика и видео-записа, IoT/PIoT инфраструктура и системи подршке одлучивању уграђени у саму архитектуру аналитичког процеса.

AI-native приступ не значи да вештачка интелигенција самостално управља полицијским поступањем, нити да замењује стручну процену полицијских службеника. Напротив, његова основна вредност је у томе што омогућава бржу обраду великих и разноврсних скупова података, препознавање сложених образаца, праћење промена у реалном или скоро реалном времену, подршку тактичком и стратешком одлучивању и континуирану евалуацију ефеката предузетих мера. У том смислу, AI-native предиктивна полицијска аналитика представља технолошки и методолошки развијенији облик подацима вођеног полицијског рада.

Овај приступ је посебно значајан у условима паметних градова, у којима се безбедносни ризици више не јављају само у физичком простору, већ и на пресеку физичког и сајбер окружења. Камере, сензори, системи паметног саобраћаја, геопросторни подаци, јавни регистри, дигитални трагови, службене белешке, наративни извештаји и други извори могу бити повезани у јединствен аналитички оквир. У таквом оквиру edge ниво може подржати прикупљање и прелиминарну обраду података, fog ниво краткорочну аналитику и тактичку координацију, док cloud ниво омогућава дугорочну интеграцију, стратешку анализу, управљање моделима и евалуацију исхода.

AI-native предиктивна полицијска аналитика зато се може разумети као трећи развојни ниво у односу на конвенционални криминалистичко-обавештајни циклус и класичну предиктивну аналитику. Први приступ је усмерен на обавештајни циклус и институционално поступање; други приступ додаје моделе предвиђања и процену будућег ризика; трећи приступ интегрише вештачку интелигенцију, хијерархијску дигиталну инфраструктуру, системе подршке одлучивању и континуирано учење из повратних информација. Ипак, у сва три приступа мора остати очувано основно начело: аналитички резултат је подршка одлучивању, а не замена за правно утемељено, етички прихватљиво и људски контролисано полицијско поступање.

Слика 3.5.3. Развој од криминалистичко-обавештајног циклуса ка AI-native предиктивној полицијској аналитици

Као што је приказано на слици 3.5.3, развој предиктивне полицијске аналитике може се разумети као прелаз од класичног криминалистичко-обавештајног циклуса, преко процеса предиктивне полицијске аналитике, ка AI-native приступу. Тај развој не подразумева напуштање основне логике полицијског рада, већ њено технолошко и методолошко унапређење кроз напредну обраду података, хијерархијску инфраструктуру и системе подршке одлучивању. Детаљније разграничење предиктивне, прескриптивне, когнитивне и AI-native аналитике дато је у наредном одељку.

3.6. Развој ка AI-native полицијској аналитици

У претходним деловима овог поглавља предиктивна полицијска аналитика разматрана је као процес који омогућава процену будућег ризика на основу података, статистичких метода, алгоритамских модела и аналитичке интерпретације. Међутим, у савременим условима развоја паметних градова, IoT/PIoT инфраструктуре, машинског учења и система подршке одлучивању, предиктивна полицијска аналитика све чешће постаје део ширег аналитичког система који обухвата и прескриптивне, когнитивне и AI-native компоненте.

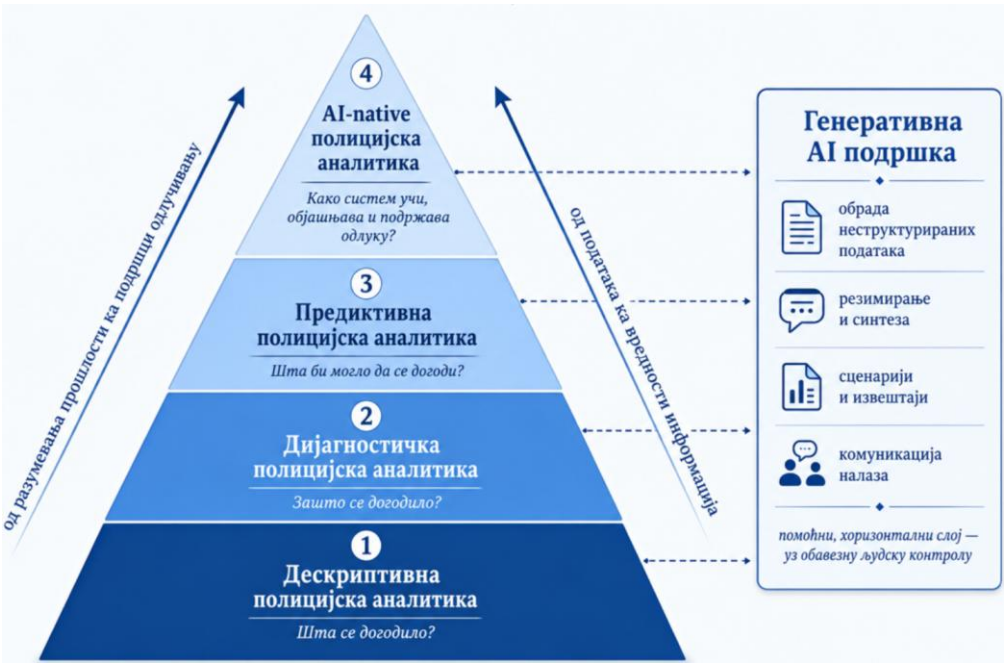
Предиктивна полицијска аналитика одговара на питање шта би могло да се догоди, где, када и под којим условима. Њен основни производ је процена ризика, односно идентификација образаца, простора, временских интервала, догађаја или понашања који указују на повећану вероватноћу криминалних или других безбедносно релевантних активности. Она зато представља прелаз од разумевања прошлости ка процени будућности, али сама по себи не даје коначну препоруку шта треба предузети.

Прескриптивна полицијска аналитика иде корак даље и настоји да одговори на питање шта треба предузети. Она се не задржава само на процени ризика, већ предлаже могуће мере, алтернативе поступања, приоритете, сценарије и распоред ресурса. У полицијском контексту, то може да подразумева предлог промене патролних рута, усмеравање ресурса ка одређеним просторима и временским интервалима, избор превентивних активности, симулацију последица различитих интервенција или процену односа између очекиваних ефеката и расположивих капацитета. Због тога прескриптивна аналитика мора бити повезана са системима подршке одлучивању, оперативним ограничењима, правним правилима и контролом људског одлучивања.

Когнитивна полицијска аналитика подразумева виши ниво аналитичке подршке, у којем систем не само да обрађује податке и предлаже опције, већ учи из претходних исхода, препознаје сложене обрасце, повезује различите врсте података и помаже у тумачењу резултата. Она се ослања на методе машинског учења, дубоког учења, обраде природног језика, анализе слике и видео-записа, семантичке претраге и објашњиве вештачке интелигенције. У том смислу, когнитивна аналитика може подржати аналитичаре у раду са великим, разноврсним и неструктурираним подацима, али њени резултати морају остати предмет стручне провере и институционалне одговорности.

AI-native полицијска аналитика представља савремени развојни правац у којем вештачка интелигенција није само додатни алат у појединачним фазама анализе, већ је уграђена у саму архитектуру аналитичког система. То значи да се подаци, алгоритми, модели, сензорска инфраструктура, IoT/PIoT уређаји, edge–fog–cloud обрада, системи подршке одлучивању, објашњивост модела и људска контрола посматрају као делови јединственог аналитичко-оперативног окружења. У таквом приступу, edge ниво може подржати прикупљање и прелиминарну обраду података у реалном времену, fog ниво краткорочно предвиђање и тактичку координацију, док cloud ниво омогућава дугорочну интеграцију података, стратешку анализу, управљање моделима и евалуацију исхода.

Развој полицијске аналитике може се приказати као постепени прелаз од дескриптивне и дијагностичке аналитике, преко предиктивне аналитике, ка AI-native полицијској аналитици. У том развоју вештачка интелигенција не представља издвојену фазу која замењује претходне облике аналитике, већ технолошки и методолошки слој који омогућава бржу обраду података, препознавање сложених образаца, објашњавање резултата и подршку одлучивању. Ова логика приказана је на слици 3.6.1.



Слика 3.6.1. Развој ка AI-native полицијској аналитици

Као што је приказано на слици 3.6.1, AI-native полицијска аналитика не укида претходне нивое аналитике, већ их надограђује. Дескриптивна аналитика обезбеђује разумевање онога што се догодило, дијагностичка аналитика настоји да објасни зашто се догодило, а предиктивна полицијска аналитика процењује шта би се могло догодити. AI-native аналитика додаје могућност да систем учи из података, повезује различите изворе, објашњава резултате и подржава одлучивање у хијерархијском, подацима вођеном окружењу. Иако на слици нису посебно издвојене прескриптивна и когнитивна аналитика, оне су садржане у прелазу од предиктивне процене ка интелигентној подршци одлучивању.

Посебно је важно што је генеративна вештачка интелигенција на слици приказана као помоћни, хоризонтални слој, а не као самосталан ниво полицијског одлучивања. Њена улога је да помогне у обради неструктурираних података, резимирању и синтези информација, припреми сценарија и извештаја, као и у комуникацији аналитичких налаза. Међутим, генеративна вештачка интелигенција не сме бити извор самосталне полицијске сумње, нити механизам за аутоматизовано доношење одлука. Сваки AI-генерисани садржај мора бити проверен, документован и стављен у контекст формалних процедура, стручне процене и људске контроле.

Разлика између ових нивоа може се сажети на следећи начин: предиктивна полицијска аналитика процењује шта би се могло догодити; прескриптивна аналитика предлаже шта би требало предузети; когнитивна аналитика помаже систему и аналитичарима да уче, повезују и тумаче сложене обрасце; док AI-native полицијска аналитика све наведене компоненте интегрише у хијерархијски, подацима вођен и технолошки подржан систем одлучивања.

Овако схваћен развој не значи напуштање класичне полицијске аналитике, нити замену полицијског службеника алгоритмом. Напротив, он подразумева методолошко и технолошко унапређење постојећих аналитичких и обавештајних процеса, уз очување основног принципа да аналитички резултат представља подршку одлучивању, а не коначну одлуку. Управо зато развој AI-native полицијске аналитике мора истовремено да обухвати техничке, методолошке, организационе, правне и етичке услове примене.

Да би се јасније разграничили развојни нивои полицијске аналитике, у табели 3.1 приказана је разлика између дескриптивно-дијагностичке аналитике, класичне предиктивне аналитике и AI-native полицијске аналитике. Ова подела не подразумева потпуно раздвојене фазе, већ развојну логику у којој сваки наредни ниво надограђује претходни.

Табела 3.1. Разлика између дескриптивно-дијагностичке, класичне предиктивне и AI-native полицијске аналитике

Ниво аналитике	**Основна функција**	**Карактеристична обележја**	**Типични ризици и ограничења**
Дескриптивна и дијагностичка полицијска аналитика	Описивање и разумевање онога што се већ догодило.	Ослања се на полицијске евиденције, пријаве, мапе криминала, дескриптивну статистику, визуелизацију, анализу образаца и дијагностичко повезивање догађаја, места, времена и околности.	Ограничена је на прошле и већ евидентиране догађаје; зависи од квалитета и потпуности евиденција; може недовољно објаснити динамичне и скривене обрасце ризика.
Класична предиктивна полицијска аналитика	Процена будућег ризика на основу историјских и контекстуалних података.	Користи статистичке моделе, просторно-временску анализу, hotspot приступе, risk terrain modeling, класификационе моделе и алгоритме машинског учења. Усмерена је на питања где, када и под којим условима може доћи до повећаног ризика.	Осетљива је на пристрасност и непотпуност историјских података; често је усмерена на један аналитички задатак; може створити ризик од прекомерног ослањања на алгоритамску процену.
AI-native полицијска аналитика	Интегрисана, хијерархијска и адаптивна подршка одлучивању у подацима вођеном окружењу.	Повезује машинско учење, дубоко учење, NLP, анализу слика и видео-записа, IoT/PIoT инфраструктуру, edge–fog–cloud обраду, XAI, fuzzy логику, генеративну вештачку интелигенцију и континуирано учење из повратних информација.	Повећава ризике непрозирности, халуцинација, аутоматизационе пристрасности, сајбер-рањивости, прекомерног надзора и правно-етичке неприхватљивости ако није праћена људском контролом, објашњивошћу и институционалном ревизијом.

Из приказане табеле се види да AI-native полицијска аналитика не представља једноставну замену класичне предиктивне аналитике, већ њено проширење у сложенији аналитичко-оперативни систем. Док класична предиктивна аналитика настоји да процени будући ризик, AI-native приступ настоји да повеже прикупљање података, предикцију, објашњавање, препоруку, људску контролу и евалуацију исхода у јединствен циклус. Управо због тога

овај приступ има већи потенцијал, али и веће ризике, што захтева посебну пажњу у погледу објашњивости, правне пропорционалности, етичке прихватљивости и институционалне одговорности.

3.7. Закључна разматрања о предиктивној полицијској аналитици

У овом поглављу предиктивна полицијска аналитика разматрана је као аналитичко-оперативни приступ који надограђује дескриптивну и дијагностичку полицијску аналитику. Док дескриптивна аналитика омогућава разумевање онога што се догодило, а дијагностичка аналитика настоји да објасни зашто се одређени догађај или образац појавио, предиктивна полицијска аналитика усмерена је ка процени шта би се могло догодити у будућности, где, када и под којим условима. Њена основна сврха није замена конвенционалних полицијских метода, већ подршка благовременом, превентивном и пропорционалном полицијском деловању. Због тога примена алгоритамских модела у полицијском раду мора бити праћена проценом пропорционалности, јасним процедурама одговорности и могућношћу независне провере аналитичких резултата (Oswald et al., 2018).

Посебно је наглашено да предиктивну полицијску аналитику не треба изједначити са појединачним алгоритмом или софтверским решењем. Она представља шири систем који обухвата прикупљање, систематизацију и интеграцију података, примену статистичких, алгоритамских и метода вештачке интелигенције, процену ризика, припрему аналитичких налаза, подршку одлучивању, полицијско поступање и евалуацију исхода. У том процесу подаци добијају другачију улогу него у дескриптивној аналитици: они више не служе само описивању стања, већ постају основ за процену будућег ризика и планирање превентивних мера.

У поглављу је показано и да је појам предиктивне полиције шири од предиктивне полицијске аналитике. Предиктивна полицијска аналитика односи се на аналитички део процеса, док предиктивна полиција обухвата и оперативну примену резултата, организацију поступања, распоређивање ресурса, правни оквир, етичку контролу и евалуацију ефеката. Због тога је у овој дисертацији оправдано користити термин „предиктивна полицијска аналитика“ када се говори о моделима, подацима, методама и

аналитичком процесу, а термин „предиктивна полиција“ када се разматра шири институционални и оперативни контекст.

Разматрање односа предиктивне полиције и превенције показало је да се предиктивне полицијске методе најчешће сврставају у оквир стратегија спровођења закона, али да њихов значај превазилази само питање реактивног деловања. Оне могу подржати примарну превенцију, тактичко планирање, рано откривање ризика, усмеравање ресурса и спречавање ескалације мањих проблема у озбиљније безбедносне претње. При томе се мора водити рачуна да предиктивни налаз не сме сам по себи бити основ за репресивно поступање, већ мора бити проверен, контекстуализован и употребљен у складу са законом, принципом сразмерности и стручном проценом.

Упоређивање процеса предиктивне полицијске аналитике са криминалистичко-обавештајним циклусом показује да предиктивна полицијска аналитика не напушта конвенционалне полицијске концепте, већ их методолошки и технолошки надограђује. Основна логика усмеравања, прикупљања, обраде, анализе, дистрибуције и употребе обавештајних сазнања остаје важна, али се проширује већим и разноврснијим скуповима података, напредним аналитичким методама, машинским учењем, системима подршке одлучивању и повратним информацијама које омогућавају корекцију модела и поступања.

У савременом контексту паметних градова, IoT/PIoT инфраструктуре и хибридног физичко-сајбер окружења, предиктивна полицијска аналитика све више се развија ка AI-native приступу. Тај приступ подразумева да вештачка интелигенција, машинско учење, сензорски подаци, edge–fog–cloud обрада, објашњивост модела и људска контрола буду интегрисани у јединствен аналитичко-оперативни систем. Ипак, овај развој не значи аутоматизацију полицијског одлучивања, већ унапређење капацитета аналитичара, руководилаца и полицијских службеника да на основу проверљивих података доносе благовремене, одговорне и правно утемељене одлуке.

На основу свега наведеног може се закључити да превенција и рано откривање илегалних активности не могу бити сведени на техничко питање изградње алгоритма. Предиктивна полицијска аналитика представља системски модел у којем подаци, технологија, организација, правни оквир, етичка правила, безбедност система и поверење јавности

морају деловати као функционална целина. Управо зато наредно поглавље разматра предуслове имплементације полицијске аналитике, кроз правно-стратешке, технолошке, кадровско-организационе и етичко-безбедносне аспекте.

4. Предуслови имплементације полицијске аналитике

Полазећи од закључка да предиктивна полицијска аналитика представља системски, а не само технички модел, у овом поглављу разматрају се кључни предуслови њене имплементације. Да би модел за превенцију и рано откривање илегалних активности био применљив, поуздан и друштвено прихватљив, неопходно је да подаци, технологија, организација, право и поверење јавности делују као функционална целина (Meijer & Wessels, 2019; Perry et al., 2013). Због тога се предуслови имплементације посматрају кроз четири међусобно повезане групе: правно-стратешке, технолошке, кадровско-организационе и етичко-безбедносне предуслове (слика 4.1).

Слика 4.1. Четири међусобно повезане групе предуслова имплементације предиктивне полицијске аналитике

Слика 4.1 приказује да имплементација предиктивне полицијске аналитике зависи од четири међусобно повезане групе предуслова: правно-стратешких, технолошких, кадровско-организационих и етичко-безбедносних. Њихова међузависност указује на то да успешна примена полицијске аналитике не може бити сведена само на технолошку

спремност, већ захтева усклађеност правног оквира, организационих капацитета, заштите права, информационе безбедности и поверења јавности.

Основна теза овог поглавља је да модел може бити технички тачан, али организационо неупотребљив или правно неприхватљив. У безбедносном систему грешка модела није само статистички проблем, већ може постати оперативни, правни и друштвени проблем, јер се аналитички резултати непосредно одражавају на приоритизацију поступања, распоређивање ресурса и интензитет надзора над појединим просторима или групама (Bennett Moses & Chan, 2018; Ferguson, 2017; Meijer & Wessels, 2019). Зато се унапређени модел пројектује као контролисан систем подршке одлучивању, а не као аутоматизована замена за полицијског службеника или руководиоца, што је посебно важно у домену јавне безбедности (Oswald et al., 2018; Joh, 2020).

4.1. Правно-стратешки предуслови

Правно-стратешки оквир треба да дефинише ко прикупља податке, које податке сме да користи, у коју сврху, колико дуго се подаци чувају, ко има приступ резултатима модела и како се проверава законитост употребе аналитичких резултата. У контексту полицијске аналитике посебно су важни принципи законитости, сврхе обраде, минимизације података, тачности, ограничења чувања, интегритета и поверљивости, јер управо од тих принципа зависи да ли ће аналитички систем остати у границама легитимне јавне власти (Gstrein et al., 2019; Vogiatzoglou, 2019; Albrecht, 2020).

Унапређени модел треба да буде усклађен са националним прописима о заштити података о личности, полицијским овлашћењима, информационој безбедности, критичној инфраструктури и електронској управи. Уколико се користе подаци из камера, сензора, саобраћајних система, јавних регистара или приватних извора, мора се предвидети формална процедура процене оправданости и пропорционалности, јер управо ту настаје највећи ризик од прекомерне обраде података и ширења надзора изван првобитне сврхе (Oswald et al., 2018; Gstrein et al., 2019; Brayne, 2017). Та процедура треба да садржи опис сврхе, врсту података, правни основ, процену ризика по права грађана и мере ублажавања ризика.

Пре увођења модела неопходно је предвидети формалну процену утицаја на права грађана и заштиту података, као и процедуру периодичне ревизије која би проверавала да ли се подаци и резултати модела користе у складу са првобитно дефинисаном сврхом. Ово је посебно важно у полицијском контексту, јер подаци који су формално доступни не морају увек бити методолошки оправдани, правно пропорционални или етички прихватљиви за употребу у предиктивном моделовању.

Стратешки оквир има двоструку улогу. Прво, обезбеђује институционалну подршку и континуитет, јер модел предиктивне полицијске аналитике не може зависити од појединачних пројеката и ентузијазма мањег броја службеника (Perry et al., 2013; Meijer et al., 2021). Друго, дефинише приоритете: који облици илегалних активности се анализирају, који нивои ризика имају предност и како се резултати аналитике преводе у оперативне активности. Без таквог оквира, и технички напредан систем може постати институционално нестабилан, спорно легитиман и тешко одржив у пракси (Ferguson, 2020; Gstrein et al., 2019).

4.2. Технолошки предуслови

Технолошки предуслови обухватају инфраструктуру за прикупљање, складиштење, интеграцију, обраду, визуелизацију и заштиту података. У класичном приступу подаци се често чувају у изолованим системима, различитим форматима и различитим нивоима квалитета, што значајно умањује аналитичку вредност и отежава примену модела машинског учења (Demchenko et al., 2013; Oatley, 2021). За унапређени модел потребна је архитектура која омогућава контролисано повезивање полицијских извора, административних извора, сензорских система, геопросторних података и релевантних података из паметног града (Prislan & Slak, 2018; Joh, 2019).

У овом раду се као технолошка основа предлаже вертикална архитектура полицијског интернета ствари, односно Police Internet of Things (PIoT), развијена из концепта паметних градова. Њена предност је у томе што раздваја ниво брзе локалне реакције, ниво тактичке координације и ниво стратешког одлучивања. Edge ниво може подржати прикупљање и прелиминарну обраду података у реалном или скоро реалном времену, fog ниво краткорочну аналитику, координацију и тактичко одлучивање, док cloud ниво омогућава

дугорочну интеграцију података, стратешку анализу, управљање моделима и евалуацију исхода (Dragović et al., 2026).

Оваква архитектура је значајна зато што се безбедносни ризици у паметним градовима више не јављају само у физичком простору, већ и на пресеку физичког и сајбер окружења. Камере, сензори, системи паметног саобраћаја, геопросторни подаци, јавни регистри, дигитални трагови, службене белешке, наративни извештаји и други извори могу бити повезани у јединствен аналитички оквир. Међутим, управо због такве повезаности неопходно је обезбедити контролу приступа, заштиту података, јасно дефинисане токове обраде и механизме за проверу интегритета података.

Поред саме инфраструктуре, технолошки предуслови подразумевају и висок квалитет података, стандардизацију метаподатака, интероперабилност, геопросторну прецизност и редовно тестирање тачности модела. У супротном, аналитички систем може производити оперативно уверљиве, али суштински погрешне резултате, посебно када су подаци непотпуни, историјски искривљени или селективно прикупљани (Richardson et al., 2019; Babuta & Oswald, 2019; Joshi et al., 2021).

4.3. Кадровско-организациони предуслови

Полицијска аналитика заснована на подацима захтева тимски рад различитих профила. Поред аналитичара који разумеју криминалистичке податке, потребни су стручњаци за базе података, машинско учење, информациону безбедност, географске информационе системе, право и комуникацију са јавношћу, јер само таква интердисциплинарна структура омогућава да се аналитички резултати претворе у поуздане и одговорне оперативне одлуке (Casey et al., 2014; Oatley & Ewart, 2011; Meijer et al., 2021). Организационо, неопходно је јасно разграничити улоге: ко припрема податке, ко развија модел, ко одобрава његову употребу, ко тумачи резултате и ко одговара за оперативну одлуку.

Кључна организациона претпоставка је људска контрола. Модел треба да израчуна вероватноће, индексе ризика, приоритете и препоруке, али коначну одлуку мора донети овлашћени службеник. То је посебно важно у случајевима где су подаци непотпуни, где је потребно контекстуално знање или где би аутоматизована одлука могла да доведе до дискриминације, прекомерног надзора или погрешног усмеравања ресурса (Oswald et al.,

2018; Babuta & Oswald, 2019; Joh, 2020). Из тог разлога организациона структура мора да обезбеди не само техничку подршку, већ и јасне процедуре одобравања, документовања и ревизије сваке значајне аналитичке интервенције (Bennett Moses & Chan, 2018; Ferguson, 2018).

Кадровско-организациони предуслови обухватају и развој аналитичке културе унутар институције. Предиктивна полицијска аналитика не може бити успешно имплементирана ако се њени резултати посматрају као „готова истина“ или као технички налог за поступање. Напротив, аналитички резултати морају бити предмет стручне интерпретације, провере и контекстуализације. Зато је неопходно развијати обуке за аналитичаре, руководиоце и полицијске службенике који ће користити резултате модела, како би разумели његове могућности, ограничења, ризике и услове примене.

Посебан значај има међуинституционална сарадња. Модел који користи податке из више извора не може функционисати без јасних споразума о размени података, процедура за контролу приступа, заједничких стандарда и механизама координације. Уколико се организациони аспекти занемаре, постоји ризик да технолошки развијен модел остане изолован, неприхваћен у пракси или недовољно повезан са стварним потребама полицијског поступања.

4.4. Етичко-безбедносни предуслови имплементације

Етичко-безбедносни предуслови представљају самосталан и неизоставан предуслов примене полицијске аналитике, јер формална законитост и техничка ефикасност саме по себи нису довољне да обезбеде друштвену прихватљивост система. У литератури се посебно издвајају принципи правичности, недискриминације, објашњивости, транспарентности, одговорности, људског надзора и пропорционалности (Asaro, 2019; Adadi & Berrada, 2018; Alikhademi et al., 2021; Gstrein et al., 2019).

Принцип правичности подразумева да модел не сме систематски неповољно третирати одређене друштвене групе, насеља или категорије лица само зато што су историјски подаци већ били оптерећени селективним полицијским праксама. Познато је да „прљави подаци“ и историјски неравномерно поступање полиције могу произвести „лоша предвиђања“, чиме

се постојеће неједнакости не исправљају већ репродукују у дигиталном облику (Richardson et al., 2019; Angwin et al., 2016; Brayne et al., 2015).

Принцип објашњивости значи да резултати модела морају бити разумљиви онима који их користе и онима на које се њихова примена односи. У полицијском окружењу није довољно да модел има високу предиктивну снагу; неопходно је разумети због чега је одређени простор, догађај или образац означен као ризичан, јер без тога изостаје реална могућност стручне провере и одговорног поступања (Adadi & Berrada, 2018; Berk, 2021; Oswald et al., 2018).

Принцип транспарентности не значи потпуно откривање свих техничких детаља система, већ постојање јасно дефинисаних правила о сврси употребе, врстама података, нивоу аутоматизације, надзору над системом и поступку приговора. Тамо где се полицијска аналитика уводи без транспарентних правила, јавља се растуће неповерење јавности, као и опасност да се технологија доживи као инструмент скривеног или несразмерног надзора (Bakke, 2018; Ferguson, 2017; Couchman, 2019).

Принцип одговорности захтева да у сваком тренутку буде јасно ко одговара за избор података, развој модела, верификацију резултата и доношење коначне одлуке. Алгоритам не може бити носилац правне или етичке одговорности; одговорност мора остати на институцији и овлашћеним службеницима који систем примењују (Bennett Moses & Chan, 2018; Joh, 2020; Meijer et al., 2021).

Најзад, принцип пропорционалности и људског надзора има посебан значај у полицијској аналитици. Чак и када модел идентификује статистички повишен ризик, реакција институције мора бити сразмерна, правно утемељена и подложна људској процени, јер је реч о области у којој једнострано ослањање на аутоматизоване препоруке може довести до озбиљних повреда права и слобода (Oswald et al., 2018; Gstrein et al., 2019; Strikwerda, 2020).

Поред етичких принципа, етичко-безбедносни предуслови обухватају и заштиту информационог система, контролу приступа, интегритет података, заштиту од неовлашћене обраде, сајбер-безбедност и праћење потенцијалних злоупотреба аналитичких резултата. У полицијској аналитици безбедност система није само техничко питање, већ услов поверења

у модел, јер компромитовани подаци, неовлашћени приступ или манипулација резултатима могу произвести погрешне оперативне одлуке и угрозити права грађана.

4.5. Предуслови у Републици Србији

У Републици Србији постоје поједини важни предуслови за постепени развој унапређеног модела: развијени су поједини елементи електронске управе, постоје институционални регистри, полицијски информациони системи, геопросторни подаци и све већа распрострањеност градских камера и сензорских система, што може представљати основу за постепени развој аналитичке инфраструктуре. Међутим, кључни изазови су у повезивању извора, стандардизацији података, правној контроли приступа, квалитету метаподатака, интероперабилности и изградњи кадровских капацитета, што је у складу и са ширим увидима о изазовима савремене предиктивне полицијске аналитике (Vuković et al., 2021; Meijer & Wessels, 2019; Babuta & Oswald, 2019).

Ипак, стварни ниво спремности за имплементацију не може се проценити само на основу постојања појединачних система и извора података, већ захтева посебну анализу правних основа, техничке повезаности, квалитета података, организационих процедура и кадровских капацитета у институцијама које би биле укључене у примену модела. Због тога се имплементација не предлаже као једнократно увођење комплексног система, већ као фазни процес (слика 4.5.1).

Слика 4.5.1. Фазни приступ имплементацији унапређеног модела полицијске аналитике у Републици Србији

На слици 4.5.1 приказан је предложени фазни приступ имплементацији унапређеног модела полицијске аналитике у Републици Србији.

Прва фаза обухвата правну и организациону припрему, попис извора података и дефинисање индикатора ризика. Друга фаза подразумева пилот-примену модела на ограниченој територији или за ограничен тип инцидената. Трећа фаза односи се на евалуацију резултата, корекцију модела и постепено проширење примене, док четврта фаза обухвата институционализацију, стандардизацију и редовну ревизију модела. Оваква структура указује на то да се имплементација предлаже као постепен, контролисан и проверљив процес.

Прва фаза, правна и организациона припрема, обухвата попис извора података, анализу правних основа, дефинисање индикатора ризика, утврђивање надлежности и израду процедура за приступ, обраду и употребу података. У овој фази посебно је важно одредити које податке је дозвољено користити, за коју сврху, под којим условима и уз које мере заштите.

Друга фаза подразумева пилот-пројекат на ограниченој територији или за ограничен тип инцидената. Сврха пилота није само тестирање техничке тачности модела, већ и провера организационе употребљивости, разумљивости резултата, квалитета података, реакције корисника и могућих правних и етичких ризика. Ограничена примена омогућава да се грешке уоче пре шире институционалне употребе.

Трећа фаза обухвата евалуацију, корекцију модела и постепено проширење примене. У овој фази треба анализирати тачност предикција, корисност аналитичких резултата, ефекте на распоређивање ресурса, могуће пристрасности и пропорционалност предузетих мера. На основу тих налаза модел се коригује, допуњује и прилагођава стварним потребама полицијског рада.

Четврта фаза односи се на институционализацију, стандардизацију и редовну ревизију модела. То подразумева успостављање трајних процедура, стандарда квалитета података, правила за одговорност и контролу, као и механизама за периодично преиспитивање оправданости и ефеката модела. Оваква логика одговара препорукама да се предиктивни системи у полицији уводе опрезно, експериментално и под сталном контролом (Perry et al., 2013; Hunt et al., 2014; Saunders et al., 2016).

4.6. Закључна разматрања поглавља

Предуслови имплементације показују да унапређени модел није само аналитички алгоритам. Он представља управљачки и технолошки оквир који мора бити законит, објашњив, безбедан и оперативно употребљив (Meijer & Wessels, 2019; Gstrein et al., 2019; Joh, 2020). Успешна примена зависи од тога да ли се подаци могу претворити у поуздану информацију, информација у одлуку, а одлука у пропорционалну и правовремену полицијску акцију. Управо зато је од пресудног значаја да се модел развија као институционално контролисан систем подршке одлучивању, а не као самостални механизам аутоматизованог управљања безбедношћу (Oswald et al., 2018; Asaro, 2019; Ferguson, 2020).

Правно-стратешки предуслови обезбеђују легитимитет, сврху, надлежности и контролу примене модела. Технолошки предуслови обезбеђују инфраструктуру, квалитет података, интероперабилност, заштиту система и могућност обраде података у реалном или скоро

реалном времену. Кадровско-организациони предуслови обезбеђују да се аналитички резултати правилно тумаче, проверавају и користе у оперативном поступању. Етичко-безбедносни предуслови обезбеђују да примена модела не угрози права грађана, не репродукује постојеће пристрасности и не доведе до непропорционалног или нетранспарентног полицијског поступања.

На основу наведеног може се закључити да имплементација унапређеног модела предиктивне полицијске аналитике захтева постепен, контролисан и евалуиран приступ. Уместо једнократног увођења сложеног система, потребно је развити фазни модел имплементације који почиње правном и организационом припремом, наставља се пилот-применом, евалуацијом и корекцијом, а завршава институционализацијом и редовном ревизијом. Само такав приступ може обезбедити да модел буде не само технички изводљив, већ и правно одржив, организационо употребљив, етички прихватљив и друштвено легитиман.

Овако дефинисани предуслови представљају основу за наредну фазу истраживања, у којој се постојећи модели предиктивне полицијске аналитике могу анализирати не само према техничкој тачности, већ и према њиховој правној одрживости, организационој употребљивости, етичкој прихватљивости и могућности практичне имплементације.

5. Анализа постојећих приступа и модела предиктивне полицијске аналитике

У претходним поглављима показано је да предиктивна полицијска аналитика не може бити сведена на примену једног алгоритма, већ представља систем који повезује податке, аналитичке методе, технолошку инфраструктуру, институционалне процедуре и људски контролисано одлучивање. Због тога анализа постојећих приступа и модела у овом поглављу није усмерена само на њихову предиктивну тачност, већ и на њихову применљивост у полицијском раду, могућност интеграције у PIoT архитектуру, степен објашњивости, осетљивост на пристрасност, етичку прихватљивост и оперативну употребљивост.

Циљ овог поглавља је да се систематизују главне групе постојећих модела и приступа који могу бити релевантни за превенцију и рано откривање илегалних активности, као и да се идентификују њихове предности, ограничења и могућности примене у унапређеном моделу који се развија у овој дисертацији. Посебан акценат ставља се на питање да ли постојећи модели могу да подрже не само предвиђање ризика, већ и одговорно доношење одлука, пропорционално полицијско поступање, евалуацију исхода и институционално учење.

5.1. Критеријуми анализе постојећих модела

Анализа постојећих модела има за циљ да покаже које групе приступа могу бити корисне за превенцију и рано откривање илегалних активности, као и у којим аспектима је потребно њихово даље унапређење. Поређење се врши према већем броју критеријума: врсти улазних података, просторној и временској резолуцији, способности рада у реалном или квази-реалном времену, предиктивној тачности, објашњивости, осетљивости на пристрасност, потребним техничким и кадровским ресурсима, могућности интеграције у PIoT архитектуру и оперативној употребљивости (Kounadi et al., 2020; Meijer & Wessels, 2019).

Ови критеријуми произлазе из претходно дефинисаног разумевања предиктивне полицијске аналитике као аналитичко-оперативног система, а не као изолованог техничког решења. Модел који постиже добру статистичку или предиктивну тачност, али није објашњив, није правно одржив, није организационо употребљив или се не може интегрисати у постојеће институционалне процесе, не може се сматрати довољним за

примену у области јавне безбедности. Због тога се у овој дисертацији постојећи модели анализирају кроз шири скуп критеријума који обухвата техничке, методолошке, организационе, правне и етичке аспекте.

Постојећи приступи и модели предиктивне полицијске аналитике могу се груписати у четири шире категорије, што је приказано на слици 5.1.1.

Слика 5.1.1. Подела постојећих приступа и модела предиктивне полицијске аналитике

Слика 5.1.1 приказује четири шире категорије постојећих приступа и модела предиктивне полицијске аналитике: статистичке и просторно-временске моделе, моделе машинског учења и напредне аналитике, когнитивне и објашњиве моделе подршке одлучивању, као и AI-native, PIoT и технологије у настајању. Приказ истовремено указује на развојни ток од описивања прошлости, преко препознавања образаца и предвиђања, ка препоруци, адаптивном учењу и интеграцији у хијерархијске системе подршке одлучивању.

Оваква подела одговара логичном развоју полицијске аналитике и у складу је са ширим развојем аналитике у јавном сектору, али и са специфичностима полицијског рада, у којем аналитички резултати морају бити проверљиви, пропорционални и употребљиви у реалним оперативним условима (Lam, 2014; Mittal, 2020).

5.2. Статистички и просторно-временски модели

Статистички и просторно-временски модели представљају полазну основу за велики број каснијих приступа предиктивној полицијској аналитици. Они обухватају дескриптивну статистику, анализу временских серија, регресионе моделе, анализу просторних концентрација, hotspot анализу, као и основне моделе класификације и ризика (Ferreira, 2012; Andresen et al., 2017). Њихова основна предност је релативна једноставност, објашњивост и могућност формалног тестирања хипотеза, због чега су погодни за почетну анализу, идентификацију трендова и креирање базних модела са којима се пореде сложенији алгоритми (Ashby & Longley, 2005; Boba, 2001).

У полицијској аналитици статистички модели имају важну улогу у разумевању просторне и временске расподеле инцидената. Они могу показати где се одређени типови догађаја најчешће јављају, у којим временским интервалима се ризик повећава, како се интензитет појаве мења кроз време и да ли постоје статистички значајне разлике између различитих просторних целина. На тај начин ови модели обезбеђују основу за мапирање ризика, праћење трендова и почетно усмеравање полицијских ресурса.

Посебан значај имају модели просторне концентрације криминала, јер бројна истраживања показују да се криминални догађаји не распоређују равномерно у простору, већ се концентришу у одређеним улицама, блоковима, насељима или типовима урбаног окружења. Ови модели су погодни за идентификацију жаришних тачака и за процену просторних образаца ризика, али њихова употреба мора бити опрезна, јер прекомерно ослањање на историјски регистроване догађаје може довести до репродукције постојећих образаца полицијског поступања и до стигматизације одређених простора.

Ограничење традиционалних статистичких модела је у томе што често претпостављају релативну стабилност појава, једноставнију структуру података и ограничен број предиктора. У савременом безбедносном окружењу подаци се све више добијају из камера, сензора, мобилних уређаја, друштвених медија, административних база, отворених извора и геопросторних система. Такви подаци су велики по обиму, разноврсни по структури, често брзо настају и могу бити неструктурирани или полу-структурирани. Због тога су

потребни модели који могу да функционишу у динамичном, временски зависном и мултимодалном окружењу (Dumbill, 2013; Demchenko et al., 2013; Oatley, 2021).

У контексту ове дисертације, статистички и просторно-временски модели имају двоструку улогу. Прво, они представљају основу за разумевање података, описивање почетних образаца и проверу квалитета улазних података. Друго, они служе као базни модели, односно као полазиште за поређење са сложенијим моделима машинског учења, fuzzy логике и AI-native аналитике. Без овог нивоа није могуће поуздано проценити да ли сложенији модел заиста доноси додатну вредност или само повећава техничку сложеност.

5.3. Модели машинског учења и напредне аналитике

Модели машинског учења омогућавају препознавање сложенијих образаца и нелинеарних односа у подацима. У ову групу спадају алгоритми класификације, кластеризације, ансамбл методе, неуронске мреже, модели за прогнозирање временских серија и модели дубоког учења (Falade et al., 2019; Hassani et al., 2021). У полицијској аналитици они се могу користити за откривање жаришта, предвиђање временских интервала повећаног ризика, класификацију пријава, анализу текста, детекцију објеката на видео-снимцима, процену приоритета интервенције и уочавање сложених образаца који нису лако видљиви класичним статистичким приступима (Wang et al., 2017; Feng et al., 2019; Khatun et al., 2021).

Предност ових модела је у способности да обрађују већи број променљивих, да уочавају нелинеарне зависности и да се прилагођавају сложенијим структурама података. Уместо да се ослањају искључиво на унапред дефинисане статистичке претпоставке, модели машинског учења могу препознати обрасце који произлазе из самих података. То их чини погодним за примену у окружењима у којима се подаци брзо мењају, долазе из различитих извора и садрже комбинацију структурираних, полу-структурираних и неструктурираних информација.

Објављени радови о применама дубоког учења и Big Data аналитике у безбедности и паметним градовима показују посебну употребљивост рекурентних неуронских мрежа, као што су RNN, LSTM и GRU модели, за краткорочно предвиђање просторних и временских образаца, укључујући криминалитет, кретање људи, саобраћајне токове и друге показатеље урбане динамике (Sun et al., 2021; Vinodhini et al., 2020). У контексту ове дисертације, ова

логика се проширује: саобраћајни ток није само питање саобраћајне полиције, већ може бити индикатор урбане динамике, масовних окупљања, кризних ситуација и потенцијалног премештања полицијских ресурса (Tian et al., 2020; Wawrzyniak et al., 2018).

Због тога се временске серије посматрају као једна од компоненти ширег безбедносног модела. Машинско учење у таквом моделу служи за откривање комплексних зависности између кретања људи, возила, просторних карактеристика, временских промена и појава од безбедносног значаја (Pramanik et al., 2017; Fitzpatrick et al., 2019). Уколико се ови модели повежу са сензорским системима, камерама, саобраћајним детекторима и геопросторним подацима, они могу подржати краткорочне прогнозе и тактичко одлучивање у реалном или скоро реалном времену.

Ипак, модели машинског учења имају значајна ограничења. Они захтевају висок квалитет података, довољну количину релевантних опсервација, адекватну класну равнотежу, редовно ажурирање и контролу пристрасности. Уколико су улазни подаци непотпуни, историјски искривљени или резултат селективног поступања, алгоритам може произвести формално прецизне, али друштвено неприхватљиве резултате. Због тога се у литератури све више наглашава да машинско учење у полицијском контексту мора бити праћено објашњивошћу, ревизијом података, проценом пропорционалности и људском контролом (Richardson et al., 2019; Meijer & Wessels, 2019; Mohler et al., 2018).

У предложеном моделу дисертације, модели машинског учења имају највећи значај на нивоу краткорочне предикције, препознавања образаца и тактичке подршке. Они могу бити посебно корисни на fog нивоу PIoT архитектуре, где је потребно брзо обрађивати податке, препознавати трендове и припремати аналитичке улазе за доносиоце одлука. Међутим, они не могу самостално решити питање институционалне примене, правне прихватљивости и етичке контроле, због чега морају бити интегрисани у шири систем подршке одлучивању.

5.4. Когнитивни и објашњиви модели подршке одлучивању

Когнитивни и објашњиви модели подршке одлучивању представљају виши ниво аналитичке подршке, јер не обухватају само предвиђање, већ и препоруку, образложење препоруке, процену несигурности и учење из повратних информација. У контексту ове дисертације, когнитивне технологије не третирају се као потпуно аутономна полиција, већ

као напредни системи подршке одлучивању који треба да помогну аналитичарима, руководиоцима и полицијским службеницима у разумевању сложених ситуација (Schatsky et al., 2015; Berk, 2021).

Ови модели могу комбиновати више извора података, више аналитичких метода и више нивоа одлучивања. Њихова основна вредност је у томе што могу повезати предиктивне резултате са контекстом, ограничењима и могућим мерама поступања. Уместо да модел само означи простор или временски интервал као ризичан, когнитивни приступ настоји да помогне у разумевању зашто је ризик повећан, који фактори су допринели процени, колико је процена сигурна и које мере би могле бити примерене.

У овој групи посебно место имају концепти објашњиве вештачке интелигенције (XAI). Објашњивост је у полицијској аналитици посебно важна зато што аналитички резултати могу утицати на распоређивање ресурса, интензитет надзора и приоритет полицијског поступања. Због тога није довољно да модел има високу предиктивну тачност; неопходно је да корисници могу разумети основне разлоге препоруке, ограничења модела и степен несигурности резултата (Adadi & Berrada, 2018; Das et al., 2021).

Фази логика има посебно место у оквиру когнитивних и објашњивих модела, јер омогућава формализацију експертског знања у ситуацијама у којима су појаве неодређене, а подаци непотпуни, контрадикторни или различитог квалитета. За разлику од класичне бинарне одлуке, fuzzy приступ омогућава да се ситуације означе као „низак“, „средњи“ или „висок“ ризик, односно као случајеви у којима је потребна додатна провера пре интервенције (Khalid et al., 2021; Shalaginov, 2018).

Овај приступ је погодан за комбиновање техничких индикатора, полицијског искуства и организационих правила. Он омогућава да експлицитно знање, као што су прописане процедуре и формални критеријуми, буде повезано са имплицитним знањем, као што су искуство службеника и процена ситуационог контекста. То је посебно важно код сложених, мулти-критеријумских безбедносних одлука, где један показатељ ретко може бити довољан за оправдано поступање (Bachner, 2013; Casey et al., 2014).

Когнитивни и објашњиви модели, међутим, имају и своја ограничења. Они су често сложени за развој, захтевају пажљиву валидацију и могу створити лажан утисак сигурности

ако се њихови резултати представљају као неутралне или објективне препоруке. Посебан ризик настаје када се објашњење модела користи као формално оправдање одлуке, без стварног разумевања ограничења података и аналитичког поступка. Зато ови модели морају бити праћени документовањем, провером, људском контролом и јасним процедурама одговорности (Oswald et al., 2018; Bennett Moses & Chan, 2018).

У предложеном моделу дисертације, когнитивни и објашњиви модели имају значајну улогу на нивоу подршке одлучивању, нарочито у cloud делу PIoT архитектуре. Они могу помоћи у стратешкој анализи, процени сложених сценарија, комбиновању различитих извора података и формулисању препорука које нису само статистички засноване, већ и разумљиве, проверљиве и прилагођене институционалном контексту.

5.5. AI-native, PIoT и технологије у настајању

Технологије у настајању у овој дисертацији не посматрају се као посебни предиктивни модели у ужем смислу, већ као инфраструктурне и аналитичке платформе које омогућавају развој сложенијих модела предиктивне полицијске аналитике. Оне укључују напредне IoT системе, edge/fog/cloud архитектуре, дигиталне близанце, проширену и виртуелну реалност, аутономне платформе, напредну видео аналитику и моделе генеративне вештачке интелигенције (Radenković & Kočović, 2017; UNICRI, 2019; Morley, 2020).

Потенцијал ових технологија је значајан, јер омогућавају обраду података у реалном времену, локалну предобраду на edge или fog нивоу, тесну интеграцију са инфраструктуром паметног града и повезивање физичких и дигиталних извора података. У полицијском контексту, ови системи се могу користити за напредну видео аналитику, детекцију сумњивог понашања, препознавање образаца кретања, симулацију сценарија помоћу дигиталних близанаца и подршку одлучивању у ситуацијама високог ризика путем проширене и виртуелне реалности (Doan et al., 2021).

Посебан значај има PIoT архитектура, јер омогућава да се различите аналитичке функције распореде по хијерархијским нивоима. Edge ниво може бити погодан за прикупљање и прелиминарну обраду података са камера, сензора и IoT уређаја. Fog ниво може подржати краткорочну предикцију, тактичку координацију и брзу реакцију на промене у окружењу. Cloud ниво може бити задужен за дугорочну интеграцију података, стратешку анализу,

управљање моделима и fuzzy подршку одлучивању. Оваква вертикална структура омогућава јасније раздвајање оперативних, тактичких и стратешких функција у полицијској аналитици (Dragović et al., 2026).

У том смислу, PIoT приступ представља један од могућих праваца превазилажења фрагментације постојећих модела. Он омогућава да се оперативно праћење, тактичко предвиђање и стратешко одлучивање распореде по хијерархијским edge, fog и cloud нивоима. Такав приступ повезује машинско учење, временске серије, fuzzy подршку одлучивању и вертикални ток података у јединствену архитектуру погодну за паметне градове и хибридно физичко-сајбер окружење (Dragović et al., 2026).

AI-native полицијска аналитика представља даљи развој у овом правцу. Она подразумева да вештачка интелигенција није само додатни алат у појединачним фазама анализе, већ интегрисани део архитектуре аналитичког система. У таквом приступу, машинско учење, видео аналитика, обрада природног језика, генеративна вештачка интелигенција, XAI, fuzzy логика и системи подршке одлучивању могу функционисати као повезани слојеви једног аналитичко-оперативног окружења.

Ипак, технологије у настајању носе и повећане ризике. Њихова примена може повећати осетљивост на сајбер-нападе, угрозити приватност, отежати објашњење модела, створити зависност од добављача, повећати трошкове одржавања и отворити питања надзора, пропорционалности и јавног поверења (Biliri et al., 2017; King et al., 2020; Wilson, 2019). Због тога се у предложеном моделу технологије у настајању посматрају као инфраструктурна и аналитичка подршка, али не као самосталан основ за полицијско поступање.

У предложеном моделу, AI-native, PIoT и технологије у настајању имају улогу интеграционе платформе. Њихов задатак није да замене полицијску процену или правно утемељено одлучивање, већ да омогуће бржу обраду података, боље повезивање извора, краткорочно предвиђање, стратешку анализу и проверљиву подршку одлучивању. Њихова примена је оправдана само ако је праћена робусном сајбер-безбедношћу, правном усклађеношћу, етичком проценом, објашњивошћу и људском контролом (Mitchell et al., 2020; Yamin et al., 2020).

5.6. Синтеза предности и ограничења постојећих модела

Анализа постојећих група модела показује да свака од њих има одређену вредност за развој унапређеног модела, али и јасна ограничења. Статистички и просторно-временски модели обезбеђују објашњиву и проверљиву основу, али су ограничени у раду са великим, разноврсним и неструктурираним подацима. Модели машинског учења омогућавају препознавање сложених образаца и краткорочну предикцију, али захтевају висок квалитет података, контролу пристрасности и додатне механизме објашњивости. Когнитивни и објашњиви модели подршке одлучивању омогућавају рад са неизвесношћу и интерпретацију резултата, али су сложени за развој и валидацију. AI-native, PIoT и технологије у настајању омогућавају интеграцију података и рад у реалном или скоро реалном времену, али отварају питања сајбер-безбедности, приватности, трошкова и институционалне контроле.

Из табеле 5.1. се може закључити да ниједна група модела сама по себи није довољна за развој унапређеног модела предиктивне полицијске аналитике. Статистички модели обезбеђују објашњивост и почетну проверу, машинско учење обезбеђује предиктивну снагу, когнитивни и објашњиви модели омогућавају тумачење и подршку одлучивању, док PIoT и технологије у настајању обезбеђују инфраструктурну основу за хијерархијску интеграцију. Због тога унапређени модел треба да буде хибридан: да комбинује предности више приступа, али уз јасне механизме контроле, објашњивости, евалуације и људског надзора.

Табела 5.1. Синтеза група постојећих модела и њихова улога у унапређеном моделу

Група модела	Примери	Предности	Ограничења	Улога
Статистички и просторно-временски модели	регресија, временске серије, просторне концентрације, hotspot анализа (Ferreira, 2012; Ashby & Longley, 2005)	објашњивост, једноставност, тестирање хипотеза, базна анализа (Boba, 2001)	ограничена обрада сложених и неструктурираних података; осетљивост на претпоставке модела (Demchenko et al., 2013)	почетна анализа, опис образаца, бенчмарк за сложеније моделе
Модели машинског учења и напредне аналитике	класификација, кластеризација, ансамбли, RNN/LSTM/GRU, дубоко учење (Falade et al., 2019; Sun et al., 2021)	препознавање сложених образаца, рад са већим бројем предиктора, краткорочна предикција (Hassani et al., 2021)	захтевају квалитетне податке, контролу пристрасности и додатну објашњивост (Richardson et al., 2019)	краткорочна предикција, fog ниво PIoT архитектуре, тактичка подршка
Когнитивни и објашњиви модели подршке одлучивању	fuzzy системи, XAI, системи препорука, модели процене несигурности (Adadi & Berrada, 2018; Joh, 2019; Khalid et al., 2021)	рад са неизвесношћу, подршка одлучивању, формализација експертског знања (Berk, 2021; Oswald et al,. 2018).	сложена валидација, потреба за људском контролом и јасном одговорношћу (Oswald et al., 2018)	cloud ниво, fuzzy подршка одлучивању, стратешка анализа
AI-native, PIoT и технологије у настајању	PIoT, edge/fog/cloud, видео аналитика, дигитални близанци, генеративна AI (King et al., 2020; Yamin et al., 2020; Dragović et al., 2026)	интеграција паметног града, реално или скоро реално време, вертикални ток података, повезивање физичког и сајбер простора (Biliri et al., 2017; Dragović et al., 2026)	сајбер-ризици, трошкови, приватност, зависност од инфраструктуре и добављача (King et al., 2020; Wilson, 2019)	инфраструктура унапређеног модела, интеграција edge–fog–cloud нивоа, AI-native развој

5.7. Истраживачке празнине и импликације за унапређени модел

Критички преглед постојећих модела указује на неколико важних истраживачких празнина. Прво, велики број модела усмерен је на предвиђање места или времена будућих инцидената, али знатно мање на интеграцију предвиђања са оперативном одлуком, односно на трансформацију аналитичког резултата у конкретну, пропорционалну и проверљиву интервенцију (Perry et al., 2013; Saunders et al., 2016; Fitzpatrick et al., 2019). Ово је значајно ограничење, јер сама предикција не доводи до превенције ако није повезана са одговарајућим поступањем, контролом и евалуацијом исхода.

Друго, модели се често тестирају на историјским подацима без довољно јасног плана организационе имплементације. Због тога многи системи остају на нивоу пилот-пројеката или експерименталних алата без трајнијег институционалног упоришта (Bachner, 2013; Meijer & Wessels, 2019). У области полицијског рада то је посебно проблематично, јер модел мора бити употребљив у реалним оперативним условима, са јасно дефинисаним улогама, процедурама, надлежностима и механизмима одговорности.

Треће, проблем пристрасности се понекад третира као споредно питање, иако управо он може одлучити о прихватљивости система. „Прљави подаци“, селективно историјско поступање полиције и неједнако евидентирање догађаја могу довести до лоших предвиђања и репродукције постојећих неједнакости (Richardson et al., 2019; Angwin et al., 2016; Babuta & Oswald, 2019). Због тога унапређени модел мора укључити контролу квалитета података, процену пристрасности и механизме независне провере резултата.

Четврто, недостају модели који у довољној мери повезују физички и сајбер простор паметног града у јединствену полицијску архитектуру. Савремени безбедносни ризици све чешће настају у интеракцији физичке инфраструктуре, дигиталних система, сензорских мрежа, саобраћајних токова, камера, јавних регистара и онлајн активности. Због тога модели који су ограничени само на историјске евиденције криминала нису довољни за хибридно физичко-сајбер окружење (Prislan & Slak, 2018; Joh, 2019; Yamin et al., 2020).

Пето, постојећи модели често недовољно разликују нивое одлучивања. Оперативне одлуке захтевају брзу реакцију и податке у реалном или скоро реалном времену; тактичке одлуке захтевају краткорочну предикцију и координацију ресурса; стратешке одлуке захтевају

дугорочну интеграцију података, анализу трендова и процену ефеката. Уколико се ови нивои не раздвоје, постоји ризик да исти модел буде непримерено коришћен за различите типове одлука.

На основу ових празнина, унапређени модел треба да буде:

- хијерархијски, јер различите одлуке имају различите временске рокове и различите последице;
- интероперабилан, јер мора повезати више извора података и више институционалних система;
- објашњив, јер резултати морају бити разумљиви аналитичарима, руководиоцима и овлашћеним службеницима;
- евалуабилан, јер се његова успешност мора мерити не само техничким метрикама, већ и стварним доприносом превенцији, пропорционалности поступања и поверењу јавности;

  контролисан, јер мора обезбедити људску проверу, правну утемељеност, заштиту података и етичку прихватљивост.

Ове кључне карактеристике унапређеног модела синтетички су приказане на слици 5.7.1.

Слика 5.7.1. Кључне карактеристике унапређеног модела предиктивне полицијске аналитике

Као што је приказано на слици 5.7.1, унапређени модел не треба разумети као изоловани технички алгоритам, већ као системску целину у чијем су средишту међусобно повезане карактеристике неопходне за његову примену у реалном полицијском окружењу (Bennett Moses & Chan, 2018). Хијерархијска структура модела омогућава разликовање оперативног, тактичког и стратешког нивоа одлучивања; интероперабилност омогућава повезивање хетерогених извора података и институционалних система; објашњивост обезбеђује разумљивост резултата и њихову употребљивост у процесу одлучивања; евалуабилност омогућава мерење стварних ефеката модела; док контролисаност обезбеђује људску проверу, правну утемељеност, заштиту података и етичку прихватљивост (Gstrein, Bunnik, & Zwitter, 2019). Управо у међусобној повезаности ових елемената огледа се логика унапређеног модела који треба да превазиђе ограничења постојећих приступа.

У том смислу, унапређени модел који се развија у овој дисертацији треба да превазиђе ограничења уских hotspot приступа и да понуди шири оквир за превенцију и рано откривање илегалних активности. Тај оквир треба да повеже статистичке и просторно-временске моделе, машинско учење, fuzzy подршку одлучивању, објашњивост, PIoT архитектуру и механизме институционалне контроле. На тај начин предиктивна полицијска аналитика може бити развијена као хијерархијски, подацима вођен и људски контролисан систем подршке одлучивању, погодан за услове паметних градова и хибридног физичко-сајбер окружења (Adadi & Berrada, 2018; Meijer & Wessels, 2019; Gstrein et al., 2019; Dragović et al., 2026).

Овако дефинисане истраживачке празнине представљају непосредан основ за наредно поглавље, у којем се развија унапређени модел за превенцију и рано откривање илегалних активности применом предиктивне полицијске аналитике. Тај модел треба да задржи предности постојећих приступа, али да их интегрише у јединствену архитектуру која повезује предикцију, подршку одлучивању, евалуацију и институционалну одговорност.

Да би се јасније показало у чему се огледа унапређење предложеног модела у односу на постојеће приступе, у табели 5.2 приказано је поређење кључних елемената система. Поређење не подразумева да постојећи модели немају научну и практичну вредност, већ указује на то да су они најчешће развијани као парцијална решења: као модели за hotspot анализу, risk terrain modeling, предвиђање преступника или жртава, или као IoT архитектуре без јасне полицијске, евалуационе и институционалне спецификације. Унапређени модел који се предлаже у овој дисертацији настоји да те елементе повеже у јединствен хијерархијски, евалуабилан и људски контролисан систем подршке одлучивању.

Табела 5.2. Елементи унапређења предложеног модела у односу на постојеће приступе

Елемент	Стање у постојећим моделима	Решење у овом раду
Подаци	Често се користе историјске полицијске евиденције, пријављени инциденти, hotspot подаци и ограничени просторно-временски показатељи. У генеричким IoT моделима подаци се углавном третирају технички, без довољне полицијске и институционалне контекстуализације.	Повезују се полицијски, геопросторни, саобраћајни, сензорски, IoT/PIoT, административни, отворени и контекстуални подаци. Наглашава се да подаци морају бити правно дозвољени, методолошки оправдани, квалитетни и употребљиви за безбедносну процену.
Архитектура	Hotspot и risk terrain модели најчешће су аналитички поступци без јасне хијерархије. Генерички IoT модели не разликују довољно оперативне, тактичке и стратешке полицијске функције.	Уводи се вертикална PIoT архитектура заснована на edge–fog–cloud нивоима. Edge ниво подржава локално прикупљање и иницијалну обраду, fog краткорочну предикцију и тактичку координацију, а cloud сложенију анализу, fuzzy/XAI подршку, евалуацију и стратешко одлучивање.
Аналитички слој	Постојећи приступи су често усмерени на један задатак: hotspot анализу, risk terrain факторе, класификацију, предвиђање преступника или предвиђање жртава.	Комбинују се статистичка и просторно-временска анализа, машинско учење, временске серије, fuzzy логика и XAI. Вредност није у једном алгоритму, већ у повезивању више аналитичких функција у циклус података, предикције, одлуке и учења.
Одлучивање	Аналитички резултат се често своди на листу ризичних места, лица или периода. Веза између предикције, одлуке, пропорционалности и одговорности није увек довољно разрађена.	Аналитички резултат се третира као улаз у систем подршке одлучивању, а не као аутоматска полицијска одлука. Fuzzy модул и XAI користе се за објашњење ризика, структурирање препоруке и подршку људском одлучивању.
Евалуација	Евалуација је често усмерена на техничку тачност, грешку предвиђања или квалитет класификације. Мање се разматрају оперативна, организациона, правно-етичка и друштвена вредност.	Уводи се интегрисани евалуациони оквир са техничком, оперативном, организационом, правно-етичком, друштвеном и развојном димензијом. Успешност се процењује кроз тачност, употребљивост, објашњивост, пропорционалност, контролу пристрасности и поверење јавности.
Људска контрола	Људска контрола се често подразумева, али није увек формално уграђена у модел. То повећава ризик од аутоматизационе пристрасности и прекомерног ослањања на алгоритамске препоруке.	Људска контрола се поставља као услов институционалне одрживости. Модел не замењује службеника, аналитичара или руководиоца, већ им пружа проверљиву, документовану и објашњиву подршку.
Институционална применљивост	Многи модели су развијени као технички или истраживачки алати, без довољне разраде услова примене у конкретном полицијском систему.	Модел се повезује са правно-стратешким, технолошким, кадровско-организационим и етичко-безбедносним предусловима. Тиме се поставља као институционално контролисан оквир, а не као изоловано софтверско решење.

Из приказаног поређења може се закључити да се унапређење предложеног модела не огледа у томе што се уводи један нови алгоритам, већ у томе што се постојећи аналитички, технолошки и организациони елементи повезују у јединствену архитектуру. У том смислу, предложени модел превазилази ограничења уских hotspot или risk-based приступа, као и ограничења генеричких IoT решења која нису прилагођена полицијском контексту. Његов допринос је у интеграцији PIoT архитектуре, предиктивне аналитике, fuzzy/XAI подршке, евалуационог оквира и људске контроле у систем који је погодан за даљу пилот-проверу у реалном институционалном окружењу.

5.8. Закључна разматрања поглавља

У овом поглављу анализирани су постојећи приступи и модели предиктивне полицијске аналитике, са циљем да се утврди у којој мери они могу допринети развоју унапређеног модела за превенцију и рано откривање илегалних активности. Анализа је показала да постојећи модели имају значајну вредност, али и јасна ограничења, посебно када се посматрају у контексту савремених паметних градова, хибридног физичко-сајбер окружења, великих и разноврсних извора података, правно-етичких ограничења и потребе за људски контролисаним одлучивањем.

Статистички и просторно-временски модели представљају неопходну основу предиктивне полицијске аналитике. Њихова вредност је у томе што омогућавају описивање трендова, анализу просторних концентрација, препознавање жаришних тачака и формирање базних модела за поређење са сложенијим приступима. Међутим, њихова ограничења постају изражена у условима великих, динамичних, полу-структурираних и неструктурираних података, као и у ситуацијама у којима је потребно брзо реаговање на промене у реалном или скоро реалном времену.

Модели машинског учења и напредне аналитике омогућавају препознавање сложених образаца, нелинеарних односа и краткорочних промена у подацима. Они су посебно значајни за предвиђање ризика, анализу временских серија, класификацију пријава, детекцију образаца у видео и текстуалним подацима и тактичку подршку полицијском поступању. Ипак, ови модели захтевају висок квалитет података, контролу пристрасности,

редовну валидацију и објашњивост, јер у супротном могу произвести формално прецизне, али оперативно или етички проблематичне резултате.

Когнитивни и објашњиви модели подршке одлучивању представљају важан корак ка повезивању предиктивних резултата са стварним процесом одлучивања. Њихова улога није само да укажу на повећани ризик, већ и да помогну у тумачењу резултата, процени несигурности, формулисању препорука и подршци доносиоцима одлука. Посебно место у овој групи имају fuzzy логика и објашњива вештачка интелигенција, јер омогућавају рад са неодређеним, непотпуним и контекстуално зависним подацима. Међутим, сложеност ових модела захтева јасне процедуре валидације, документовања, контроле и одговорности.

AI-native, PIoT и технологије у настајању омогућавају да се предиктивна полицијска аналитика развије као хијерархијски и подацима вођен систем подршке одлучивању. Њихова вредност је у интеграцији различитих извора података, обради у реалном или скоро реалном времену, повезивању физичког и сајбер простора и раздвајању оперативног, тактичког и стратешког нивоа одлучивања. Посебно је значајна PIoT архитектура, јер омогућава да се edge ниво користи за прикупљање и прелиминарну обраду података, fog ниво за краткорочну аналитику и тактичку координацију, а cloud ниво за дугорочну интеграцију, стратешку анализу и подршку сложеном одлучивању. Ипак, такви системи отварају и нове ризике, укључујући сајбер-безбедност, приватност, зависност од инфраструктуре, трошкове одржавања и потребу за јасном институционалном контролом.

Критички преглед постојећих приступа показао је да ниједна група модела сама по себи није довољна за потребе унапређеног модела који се развија у овој дисертацији. Статистички модели обезбеђују објашњиву основу, модели машинског учења обезбеђују предиктивну снагу, когнитивни и објашњиви модели обезбеђују подршку тумачењу и одлучивању, док PIoT и AI-native приступ обезбеђују инфраструктуру за хијерархијску интеграцију. Због тога унапређени модел мора бити хибридан, односно мора повезати више аналитичких и технолошких приступа у јединствен, контролисан и евалуабилан систем.

На основу спроведене анализе издвојено је више истраживачких празнина. Постојећи модели су често усмерени на предвиђање места или времена будућих инцидената, али недовољно на повезивање предикције са пропорционалном и проверљивом интервенцијом.

Такође, многи модели се тестирају на историјским подацима без јасног плана организационе имплементације, што ограничава њихову употребљивост у реалним полицијским условима. Посебан проблем представља пристрасност података, јер историјске неједнакости, селективно поступање и неуједначено евидентирање догађаја могу довести до лоших предвиђања и репродукције постојећих неправилности. Поред тога, недовољно су развијени модели који повезују физички и сајбер простор паметног града у јединствену полицијску архитектуру и који јасно разликују оперативни, тактички и стратешки ниво одлучивања.

Из наведених разлога, унапређени модел треба да буде хијерархијски, интероперабилан, објашњив, евалуабилан и контролисан. Хијерархијска структура је неопходна зато што различите одлуке имају различите временске рокове, ниво детаљности и последице. Интероперабилност је неопходна зато што модел мора повезати више извора података и више институционалних система. Објашњивост је неопходна зато што резултати морају бити разумљиви аналитичарима, руководиоцима и овлашћеним службеницима. Евалуабилност је неопходна зато што успешност модела не сме бити мерена само техничким метрикама, већ и стварним доприносом превенцији, пропорционалности поступања и поверењу јавности. Контролисаност је неопходна зато што модел мора обезбедити људску проверу, правну утемељеност, заштиту података и етичку прихватљивост.

На основу свега наведеног може се закључити да унапређени модел предиктивне полицијске аналитике треба да превазиђе ограничења уских hotspot приступа и да понуди шири оквир за превенцију и рано откривање илегалних активности. Тај оквир треба да интегрише статистичке и просторно-временске моделе, машинско учење, fuzzy подршку одлучивању, објашњиву вештачку интелигенцију, PIoT архитектуру и механизме институционалне контроле. Само на тај начин предиктивна полицијска аналитика може бити развијена као хијерархијски, подацима вођен и људски контролисан систем подршке одлучивању, погодан за услове паметних градова и хибридног физичко-сајбер окружења.

Закључци овог поглавља представљају непосредан основ за наредно поглавље, у којем се развија унапређени модел за превенцију и рано откривање илегалних активности применом предиктивне полицијске аналитике. Док је у овом поглављу показано шта постојећи

приступи могу да понуде и где су њихова ограничења, наредно поглавље треба да покаже како се њихове предности могу интегрисати у јединствену архитектуру која повезује предикцију, подршку одлучивању, евалуацију, институционалну одговорност и контролисану примену у реалном безбедносном окружењу.

6. Изазови и ризици у примени предиктивне и AI-native полицијске аналитике

Развој предиктивне полицијске аналитике и њен прелазак ка AI-native приступу отварају значајне могућности за унапређење превенције, раног откривања ризика, боље расподеле ресурса и подршке одлучивању. Међутим, исти развој истовремено отвара и нове ризике, јер се полицијски рад све више ослања на велике скупове података, алгоритамске моделе, сензорску инфраструктуру, генеративну вештачку интелигенцију и системе подршке одлучивању. Због тога изазови примене предиктивне полицијске аналитике не могу бити сведени само на питање предиктивне тачности или техничке ефикасности, већ морају обухватити и питања пристрасности, непоузданости, објашњивости, одговорности, сајбер-безбедности, заштите података, људске контроле и поверења јавности.

У претходном поглављу показано је да унапређени модел треба да буде хијерархијски, интероперабилан, објашњив, евалуабилан и контролисан. Управо ове карактеристике представљају одговор на главне ризике који се јављају у савременој предиктивној полицијској аналитици. Одсуство хијерархијске структуре може довести до мешања оперативних, тактичких и стратешких одлука; недостатак интероперабилности до фрагментације података или неконтролисаног повезивања извора; недовољна објашњивост до непрозирних и тешко проверљивих резултата; одсуство евалуабилности до свођења успешности модела само на техничке метрике; а недостатак контроле до погрешног разумевања алгоритамске процене као основа за аутоматизовано полицијско поступање. Овај однос карактеристика унапређеног модела и ризика који настају у њиховом одсуству приказан је на слици 6.1.

Слика 6.1. Карактеристике унапређеног модела као одговор на ризике предиктивне полицијске аналитике

Слика 6.1 приказује однос између кључних карактеристика унапређеног модела и ризика који настају уколико те карактеристике нису обезбеђене. Хијерархијска структура модела умањује ризик мешања оперативних, тактичких и стратешких одлука; интероперабилност спречава фрагментацију података и неконтролисано повезивање извора; објашњивост омогућава проверу и разумевање резултата; евалуабилност спречава да се успешност модела сведе само на техничке метрике; док контролисаност обезбеђује да алгоритамска процена не буде схваћена као самосталан основ за аутоматизовано полицијско поступање. На тај начин приказане карактеристике представљају механизме ублажавања главних аналитичких, организационих, правних и етичких ризика у савременој предиктивној полицијској аналитици.

6.1. Пристрасност као централни ризик предиктивне полицијске аналитике

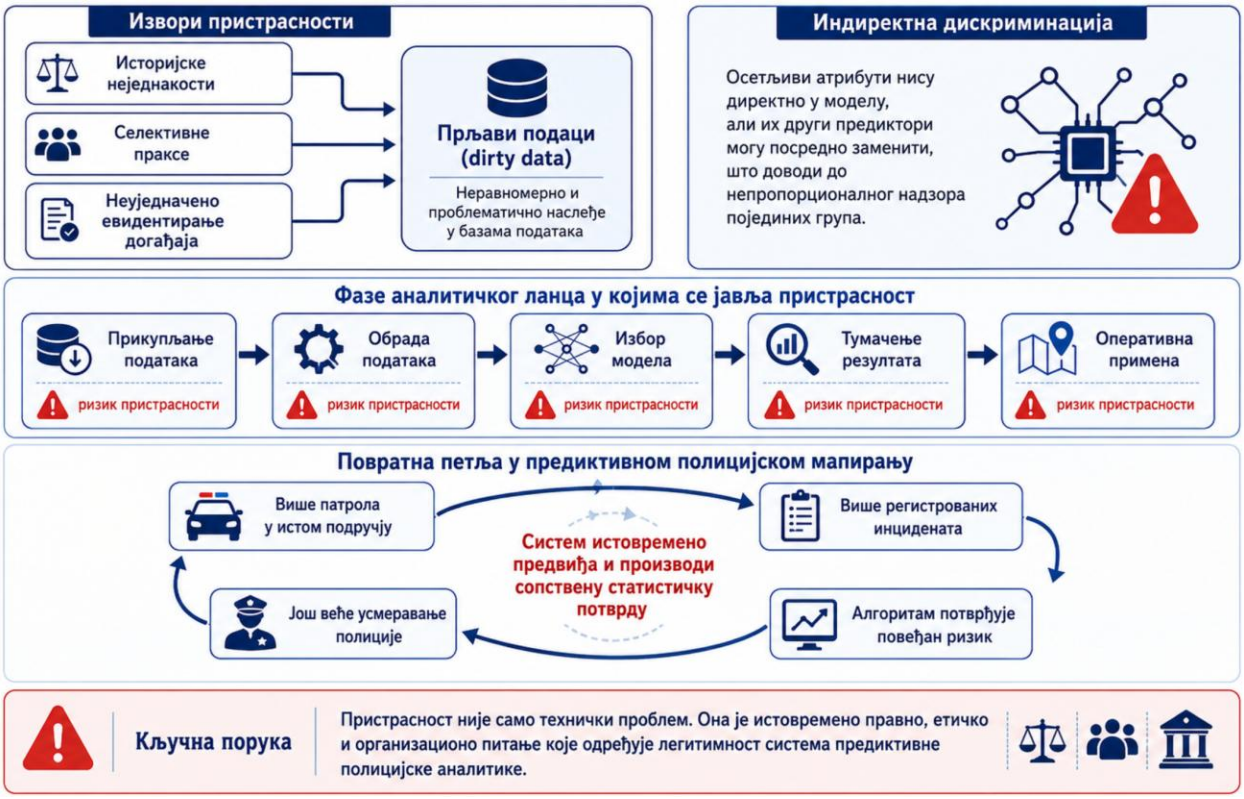
Проблем пристрасности представља једно од централних питања предиктивне полицијске аналитике, јер алгоритам није неутралан уколико су подаци на којима се обучава и контекст у коме се примењује већ оптерећени историјским неједнакостима, селективним праксама или неуједначеним евидентирањем догађаја. Пристрасност се може јавити у свим фазама аналитичког ланца: од прикупљања података, преко њихове обраде и избора модела, до тумачења резултата и оперативне примене (Richardson et al., 2019; Babuta & Oswald, 2019; Meijer & Wessels, 2019). Због тога питање пристрасности није само техничко, већ истовремено правно, етичко и организационо питање, које одређује легитимност читавог система предиктивне аналитике (Ferguson, 2017; Gstrein et al., 2019).

Кључан извор пристрасности су такозвани „прљави подаци“ (dirty data), односно подаци настали у условима у којима је полицијско поступање већ било неравномерно, селективно или повезано са кршењем права. Систематске повреде грађанских права и селективно полицијско деловање остављају трагове у базама података, па се те неједнакости могу неприметно уградити у моделе који се на тим подацима обучавају (Richardson et al., 2019). Чак и када алгоритам формално не користи осетљиве атрибуте, као што су етничка припадност, пол или социоекономски статус, други предиктори могу деловати као њихове замене, што доводи до индиректне дискриминације или непропорционалне изложености појединих група надзору (Angwin et al., 2016; Selbst, 2017).

У контексту предиктивног полицијског мапирања, пристрасност се може манифестовати кроз прекомерно усмеравање патрола ка већ познатим насељима или групама. Веће присуство полиције у одређеном простору доводи до већег броја регистрованих прекршаја и инцидената, што затим алгоритам може тумачити као потврду повећаног ризика. На тај начин се ствара повратна петља у којој систем истовремено предвиђа и производи сопствену статистичку потврду (Brantingham et al., 2018; Brayne, 2017; Mugari & Obioha, 2021).

Описани механизам показује да пристрасност у предиктивној полицијској аналитици не настаје само у једној фази, нити се може свести искључиво на техничку грешку алгоритма.

Она може бити присутна у изворима података, у начину њихове обраде, у избору модела, у тумачењу резултата и у оперативној примени. Посебно је ризична повратна петља у којој повећано присуство полиције у одређеном подручју доводи до већег броја регистрованих инцидената, што затим алгоритам може тумачити као потврду повећаног ризика. Овај процес приказан је на слици 6.1.1.



Слика 6.1.1. Извори и механизми репродукције пристрасности у предиктивној полицијској аналитици

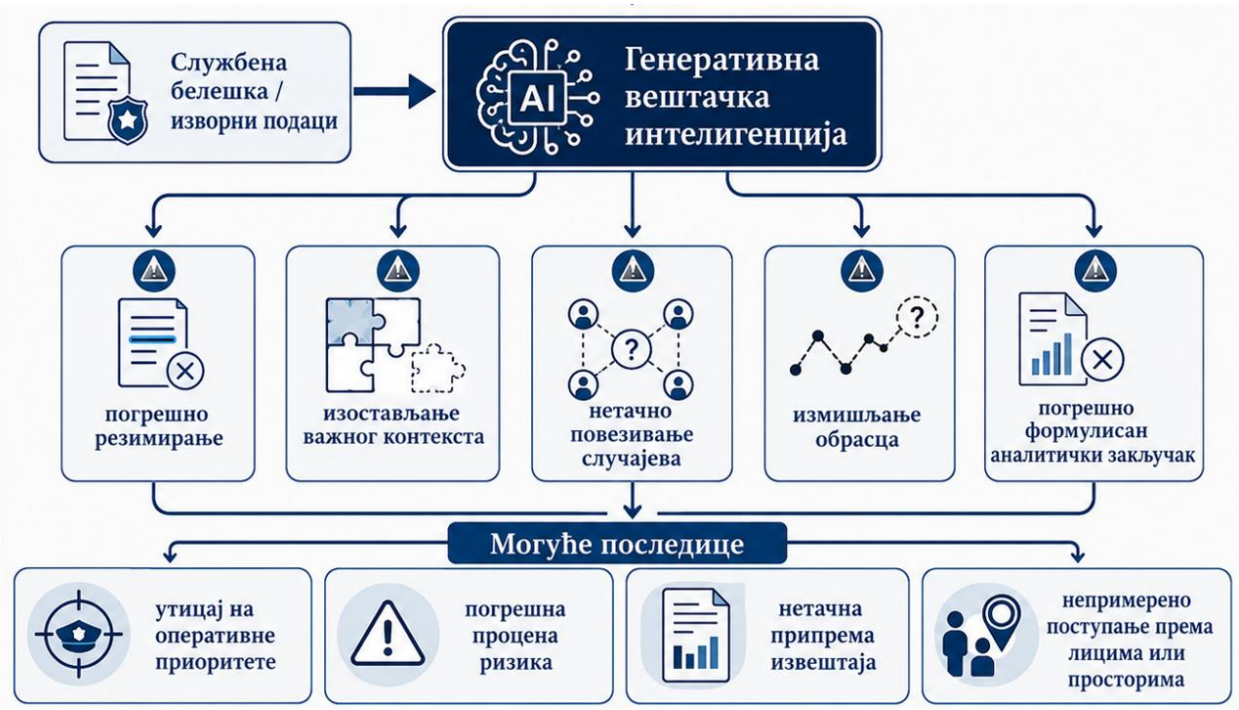
Слика 6.1.1 приказује да пристрасност може настати из историјских неједнакости, селективних пракси и неуједначеног евидентирања догађаја, који се затим претварају у „прљаве податке“ и улазе у аналитички ланац. Пристрасност се може јавити у свакој фази тог ланца: прикупљању података, обради података, избору модела, тумачењу резултата и оперативној примени. Посебно је важан приказ повратне петље у предиктивном полицијском мапирању, јер показује како више патрола у истом подручју може довести до већег броја регистрованих инцидената, што алгоритам затим тумачи као потврду повећаног ризика и основ за још веће усмеравање полиције. На тај начин пристрасност постаје не само

технички проблем, већ правно, етичко и организационо питање које утиче на легитимност целог система.

6.2. Непоузданост, халуцинације и ризици генеративне вештачке интелигенције

У AI-native полицијској аналитици посебан ризик представља употреба генеративне вештачке интелигенције и великих језичких модела. За разлику од класичних статистичких или предиктивних модела, генеративни модели могу произвести текст, резиме, сценарио или објашњење које делује уверљиво, али није нужно тачно, проверљиво или засновано на изворним подацима. Ова појава се у литератури означава као халуцинација, односно генерисање садржаја који је језички уверљив, али фактички нетачан, непоткрепљен или измишљен (Huang et al., 2025; Tonmoy et al., 2024).

У полицијском контексту овај ризик је посебно осетљив. Ако генеративна вештачка интелигенција погрешно резимира службену белешку, изостави важан контекст, нетачно повеже случајеве, измисли образац или погрешно формулише аналитички закључак, последице могу бити много озбиљније него у уобичајеним административним задацима. Погрешна синтеза може утицати на оперативне приоритете, процену ризика, припрему извештаја, па чак и на поступање према конкретним лицима или просторима. Описани ризици и њихове могуће последице у полицијском контексту приказани су на слици 6.2.1.



Слика 6.2.1. Халуцинације и ризици генеративне вештачке интелигенције у полицијској аналитици

На слици 6.2.1 је приказано да се ризици генеративне вештачке интелигенције у полицијском контексту јављају онда када систем вештачке интелигенције погрешно резимира изворне податке, изостави важан контекст, нетачно повеже случајеве, „измисли“ образац или погрешно формулише аналитички закључак. Такве грешке могу имати директне последице на оперативне приоритете, процену ризика, припрему извештаја и поступање према лицима или просторима. Зато садржај генерисан вештачком интелигенцијом мора бити проверљив, повезан са изворним подацима и потврђен од стране овлашћеног аналитичара или службеника.

Због тога генеративна вештачка интелигенција у предиктивној полицијској аналитици не сме имати улогу самосталног извора сумње, нити улогу аутономног тумача ризика. Њена примена може бити оправдана само као помоћни слој: за резимирање, претраживање, класификацију, припрему нацрта извештаја, формулисање питања или објашњавање већ проверених резултата. Сваки садржај генерисан вештачком интелигенцијом мора бити проверљив, повезан са изворним подацима, документован и одобрен од стране овлашћеног аналитичара или службеника.

6.3. Феномен „црне кутије“ и проблем објашњивости

Један од најважнијих изазова у примени сложених алгоритамских модела јесте феномен „црне кутије“. Овај проблем настаје када модел даје резултат, процену или препоруку, али корисници не могу јасно да разумеју како је до тог резултата дошло. У полицијској аналитици то је посебно проблематично, јер аналитички резултат може утицати на распоређивање ресурса, појачани надзор, приоритизацију интервенција или процену ризика по лица и просторе.

Објашњива вештачка интелигенција (XAI) настоји да овај проблем ублажи тако што резултате модела представља у облику који је разумљив аналитичарима, руководиоцима, надзорним органима и, у одређеној мери, јавности (Adadi & Berrada, 2018; Berk, 2021). Међутим, објашњивост не значи само техничку могућност приказа важности променљивих или визуелизације одлуке. У полицијском контексту, објашњивост мора бити повезана са правном оправданошћу, пропорционалношћу и могућношћу да човек процени да ли је аналитички резултат употребљив у конкретној ситуацији. Ова веза између објашњивости, правне оправданости, пропорционалности и људске процене приказана је на слици 6.3.1.

Слика 6.3.1. Кључне димензије објашњивости аналитичког резултата у полицијском контексту

Слика 6.3.1 приказује да објашњивост у полицијској аналитици не треба схватити искључиво као техничку особину модела, већ као шири услов његове употребљивости. Да би аналитички резултат био прихватљив у полицијском контексту, он мора бити правно оправдан, пропорционалан циљу и степену ризика, као и довољно јасан да човек може да процени његову релевантност, поузданост и употребљивост пре доношења одлуке. То значи да се XAI не своди само на објашњење „зашто је модел нешто предвидео“, већ и на питање „да ли је тај резултат дозвољено, разумно и оправдано користити у конкретној ситуацији“.

Посебан ризик представља ситуација у којој се „објашњење“ користи само као формално оправдање већ донете или аутоматски предложене одлуке. Ако корисници не разумеју ограничења модела, квалитет података и могуће изворе грешке, чак и објашњив модел може

створити лажан осећај сигурности. Због тога објашњивост мора бити повезана са евалуацијом, контролом и обуком корисника.

У том смислу, објашњивост није додатна, пожељна особина модела, већ један од основних услова његове одговорне примене. Само модел чији су резултати разумљиви, проверљиви и критички тумачени може бити укључен у систем подршке одлучивању без опасности да алгоритамска процена буде некритички прихваћена као објективна и коначна. Управо зато XAI у предиктивној и AI-native полицијској аналитици мора бити повезан са људском контролом, правним оквиром и институционалном одговорношћу.

6.4. Аутоматизациона пристрасност и прекомерно ослањање на алгоритам

Поред пристрасности података и модела, важан изазов у предиктивној и AI-native полицијској аналитици представља и **аутоматизациона пристрасност**, односно склоност корисника да претерано верују алгоритамској препоруци само зато што је произведена од стране технолошког система. У јавном сектору и безбедносном одлучивању овај проблем је посебно значајан, јер службеници могу прихватити резултат модела као објективнији, прецизнији или неутралнији од сопствене стручне процене, чак и онда када постоје упозоравајући знаци да је резултат непотпун, контекстуално погрешан или заснован на проблематичним подацима (Alon-Barkat & Busuioc, 2023).

У полицијском раду овај ризик може довести до ситуације у којој аналитички резултат постаје фактички налог за поступање, иако је формално представљен само као препорука. Такав развој је посебно ризичан код система који приказују индексе ризика, мапе жаришта, листе приоритета или препоруке за распоређивање ресурса, јер визуелно убедљиви и технички прецизни прикази могу прикрити методолошку несигурност, ограничења података или непотпун контекст. У таквим околностима постоји опасност да се алгоритамска процена третира као „објективна истина“, а не као један од улаза у процес одлучивања.

Посебан проблем настаје када се људска контрола сведе на формално потврђивање резултата модела. Уколико службеник нема довољно знања да разуме ограничења модела, нема приступ објашњењу резултата, нема увид у квалитет података или нема институционалну подршку да доведе у питање алгоритамску препоруку, тада људски надзор постаје само привидан. У том случају одговорност се формално задржава на човеку, али се стварна логика одлучивања помера ка систему који није довољно проверен, објашњен или контролисан.

Разлика између **формалне** и **стварне људске контроле** у AI-native полицијској аналитици приказана је на слици 6.4.1.

Слика 6.4.1. Проблем људске контроле у AI-native полицијској аналитици

Слика 6.4.1. илуструје аналитички ток од података и AI система, преко алгоритамске препоруке, до људске контроле и оперативне одлуке. Посебно је наглашена разлика између **формалне контроле**, у којој службеник само потврђује излаз система без критичке ревизије, и **стварне контроле**, у којој аналитичар активно проверава податке, контекст,

објашњење резултата и правну оправданост препоруке. Приказ такође показује да формална контрола повећава ризик од аутоматизационе пристрасности, погрешних приоритета, несразмерног поступања и губитка поверења, док стварна контрола доприноси одговорној, пропорционалној и контролисаној примени аналитичких резултата.

Зато људска контрола мора бити **стварна, а не формална**. То значи да овлашћени службеник или аналитичар мора имати могућност да резултат модела прихвати, доведе у питање, допуни, одложи или одбаци. Да би то било могуће, неопходно је да резултат буде објашњив, да су познати извори података, да су документована ограничења модела и да постоји јасна процедура за проверу спорних или неочекиваних резултата. Људска контрола зато подразумева не само присуство човека у процесу, већ и његову стварну способност да донесе информисану, правно утемељену и пропорционалну одлуку.

Унапређени модел предиктивне полицијске аналитике мора зато бити пројектован тако да не подстиче некритичко прихватање алгоритамских препорука. Напротив, систем треба да омогући приказ степена несигурности, објашњење кључних фактора који су утицали на резултат, упозорења о ограничењима података и јасно раздвајање аналитичке препоруке од оперативне одлуке. Само на тај начин може се спречити да алгоритамска процена преузме улогу самосталног основа за полицијско поступање.

Аутоматизациона пристрасност показује да ризици предиктивне полицијске аналитике не настају само у подацима или алгоритму, већ и у начину на који људи користе резултате модела. Због тога се техничка тачност модела мора посматрати заједно са организационом културом, обуком корисника, процедурама одговорности и могућношћу критичког преиспитивања резултата. У том смислу, људска контрола није завршна формалност у аналитичком процесу, већ један од кључних механизама заштите од погрешног, несразмерног или некритичког полицијског поступања.

6.5. Сајбер-безбедносни и инфраструктурни ризици

Развој предиктивне и AI-native полицијске аналитике подразумева све веће ослањање на дигиталну инфраструктуру, умрежене изворе података, cloud окружења, сензорске системе, видео-надзор, IoT/PIoT уређаје и системе подршке одлучивању. Због тога се ризици више не односе само на аналитички модел и квалитет података, већ и на безбедност читаве

техничке архитектуре у којој се подаци прикупљају, преносе, обрађују, чувају и користе. У таквом окружењу сајбер-безбедност постаје саставни део поузданости и легитимности предиктивне полицијске аналитике, а не само пратеће техничко питање (King et al., 2020; Wilson, 2019).

У контексту паметних градова и PIoT архитектуре, безбедносни ризици могу настати у свакој тачки инфраструктурног ланца. Сензори, камере, edge уређаји, комуникационе мреже, fog чворови и cloud платформе могу бити изложени неовлашћеном приступу, саботажи, манипулацији подацима, прекиду рада или злонамерном убацивању лажних сигнала. Ако се, на пример, компромитују сензорски подаци, систем може добити погрешну слику о кретању људи, саобраћајном оптерећењу или просторним обрасцима ризика, што затим може довести до погрешних предикција и непримереног полицијског поступања (Yamin et al., 2020; Prislan & Slak, 2018).

Посебно су осетљиви ризици који се односе на интегритет података. Предиктивна полицијска аналитика у великој мери зависи од тачности, конзистентности и правовремености података који улазе у систем. Уколико су подаци измењени, непотпуни, дуплирани или временски померени, аналитички модел може дати резултате који делују технички исправно, али су суштински погрешни. У AI-native окружењу овај ризик постаје још већи, јер се грешке или злонамерне измене могу аутоматски преносити кроз више подсистема и утицати на већи број аналитичких и оперативних одлука. Због тога заштита интегритета података представља један од кључних предуслова за одговорну примену ових система (Meijer et al., 2021; King et al., 2020).

Код PIoT система посебан ризик представља поузданост сензорских и комуникационих података. Уколико су сензори неисправни, лоше калибрисани, изложени физичком оштећењу, преоптерећени или компромитовани, модел може добити технички формално обрадиве, али суштински погрешне улазне податке. Такав проблем је посебно опасан зато што алгоритам може произвести уверљиву предикцију на основу нетачних или манипулисаних сигнала. Ризици као што су шум у подацима, spoofing, губитак пакета, временска кашњења, неусклађеност извора, неовлашћени приступ уређајима и убацивање лажних података морају бити третирани као део безбедносне евалуације модела. Због тога је неопходно предвидети техничке контроле интегритета података, аутоматско откривање

аномалија у сензорским токовима, упоређивање више извора, логовање измена, периодичну калибрацију уређаја и процедуре искључивања непоузданих извора из модела.

Поред тога, велика међусобна повезаност система повећава и ризик од такозваног „ефекта домина“. Када је више извора и подсистема технички интегрисано, рањивост или отказ једног дела инфраструктуре може изазвати проблеме у читавом систему. На пример, прекид у комуникационој мрежи, квар edge уређаја или напад на cloud платформу може успорити или онемогућити прикупљање и обраду података, што директно утиче на благовременост предикције и квалитет подршке одлучивању. Зато AI-native полицијска аналитика мора бити пројектована као отпоран и вишеслојан систем, са механизмима резервног функционисања, сегментације мреже, контроле приступа и евидентирања критичних догађаја.

Сајбер-безбедносни ризици не исцрпљују се само у техничком нападу споља. Подједнако су важни и унутрашњи ризици: неовлашћена употреба података, прекорачење овлашћења, недовољна контрола приступа, недовољна евиденција активности корисника и непостојање јасне поделе одговорности. У полицијском контексту, где се често обрађују осетљиви подаци о лицима, догађајима, просторима и понашањима, свака злоупотреба система може имати озбиљне правне, етичке и безбедносне последице. Због тога техничке мере заштите морају бити праћене организационим процедурама, јасним правилима приступа, обуком корисника и редовним ревизијама система (Wilson, 2019; Meijer et al., 2021).

У условима AI-native полицијске аналитике посебну пажњу треба посветити и безбедности модела вештачке интелигенције. Поред класичних ризика по инфраструктуру, појављују се и ризици као што су манипулација улазним подацима, „тровање“ скупа за обуку, намерно изазивање погрешних класификација и компромитовање модела тако да даје пристрасне или нетачне резултате. Ови ризици су посебно значајни у системима који користе машинско учење, дубоко учење и аутоматизовану обраду великих количина података, јер се напади или грешке не морају одмах уочити, а могу имати кумулативне последице по рад читавог система.

Због свега наведеног, сајбер-безбедност у предиктивној и AI-native полицијској аналитици мора се посматрати као структурни услов њене примене. То подразумева заштиту

поверљивости, интегритета и доступности података, заштиту комуникационих канала, аутентификацију и ауторизацију корисника, сегментацију инфраструктуре, резервне механизме рада, редовно тестирање рањивости, евидентирање приступа и јасну поделу одговорности. Само уколико је техничка инфраструктура отпорна, контролисана и проверљива, аналитички модел може имати реалну вредност у оперативном и стратешком раду полиције.

У том смислу, сајбер-безбедносни и инфраструктурни ризици не смеју бити третирани као споредно техничко питање, већ као један од кључних елемената укупне поузданости система. У супротном, чак и методолошки добар и правно прихватљив аналитички модел може постати непоуздан ако је смештен у рањиво, лоше контролисано или недовољно безбедно техничко окружење. Управо зато унапређени модел предиктивне полицијске аналитике мора истовремено повезати аналитичку вредност, инфраструктурну отпорност и институционалну одговорност.

6.6. Правни ризици, заштита података и регулаторни оквир

Предиктивна и AI-native полицијска аналитика морају бити усклађене са правним оквиром који регулише полицијска овлашћења, заштиту података о личности, информациону безбедност, пропорционалност, забрану дискриминације и заштиту основних права. У области јавне безбедности техничка изводљивост модела није довољна сама по себи. Чак и када аналитички систем има високу предиктивну тачност, његова примена може бити правно неприхватљива ако није заснована на јасном правном основу, ако није сразмерна легитимном циљу, ако није транспарентно документована или ако не постоји могућност људске контроле и накнадне провере.

Посебан значај има чињеница да се у савременим регулаторним оквирима AI системи који се користе у области спровођења закона, процене ризика, биометријске идентификације, анализе понашања или подршке одлучивању најчешће третирају као системи високог ризика. У европском регулаторном оквиру ова логика је посебно видљива у Уредби о вештачкој интелигенцији, односно Regulation (EU) 2024/1689, која уводи ризично заснован приступ и посебне обавезе за високоризичне AI системе (European Parliament and Council of the European Union, 2024). То значи да њихова примена мора бити праћена јасним

процедурама, проценом утицаја, контролом квалитета података, техничком и организационом документацијом, људским надзором, механизмима одговорности и редовном ревизијом. У полицијском контексту ови захтеви имају посебну тежину, јер резултати модела могу утицати на распоређивање ресурса, интензитет надзора, приоритет интервенција и поступање према конкретним лицима или просторима.

Правни оквир примене предиктивне и AI-native полицијске аналитике мора бити посматран и у контексту правила о заштити података у области кривичног правосуђа и спровођења закона. Directive (EU) 2016/680 посебно регулише заштиту физичких лица у погледу обраде података о личности од стране надлежних органа у сврхе спречавања, истраге, откривања или гоњења кривичних дела и извршења кривичних санкција (European Parliament and Council of the European Union, 2016). Ово је важно зато што се предиктивна полицијска аналитика често ослања управо на податке који настају у безбедносном, полицијском, кривичноправном или административном контексту, па њихова употреба мора бити ограничена сврхом, законита, документована и подложна контроли.

Шири међународни оквир додатно наглашава да системи вештачке интелигенције морају бити усклађени са људским правима, демократијом и владавином права. Оквирна конвенција Савета Европе о вештачкој интелигенцији, људским правима, демократији и владавини права из 2024. године поставља управо овај принцип као полазиште за развој и употребу AI система (Council of Europe, 2024). За полицијску аналитику то значи да модел не сме бити процењиван само према техничкој ефикасности, већ и према томе да ли његова употреба поштује законитост, пропорционалност, недискриминацију, право на приватност, могућност контроле и институционалну одговорност.

Употреба AI у полицијском раду отвара више правних питања. Прво питање односи се на правни основ обраде: који орган има овлашћење да користи одређене податке, у коју сврху и под којим условима. Друго питање односи се на сврху обраде: подаци прикупљени за једну намену не могу се неконтролисано користити за друге аналитичке или предиктивне сврхе без јасног правног основа и процене сразмерности. Треће питање односи се на одговорност: мора бити јасно ко је одговоран за избор података, развој модела, валидацију резултата, тумачење препоруке и коначну оперативну одлуку. Ова три питања приказана су на слици 6.6.1.

Слика 6.6.1. Кључна правна питања примене AI у полицијском раду

Извор: аутор.

Слика 6.6.1 приказује да легитимна примена AI у полицијском раду почива на три међусобно повезана правна услова. Први је постојање јасног правног основа обраде, односно овлашћења надлежног органа да користи одређене податке. Други је ограничење сврхе, које спречава да се подаци прикупљени за једну намену неконтролисано користе за друге аналитичке или предиктивне сврхе. Трећи је јасна одговорност, која подразумева да се у свакој фази мора знати ко је одговоран за избор података, развој модела, валидацију резултата, тумачење препоруке и коначну оперативну одлуку. На тај начин слика наглашава да законитост, ограничење сврхе и одговорност представљају основу правно одрживе примене AI у полицијској аналитици.

Питање одговорности је посебно важно зато што алгоритам не може бити носилац правне одговорности. Одговорност мора остати на институцији и овлашћеним службеницима који систем развијају, одобравају, користе, тумаче и контролишу. Bennett Moses и Chan (2018) наглашавају да алгоритамска предвиђања у полицији морају бити посматрана кроз

претпоставке на којима почивају, начин евалуације и механизме одговорности. Слично томе, Oswald et al. (2018) указују да алгоритамски модели процене ризика у полицијском контексту морају бити повезани са експерименталном провером, пропорционалношћу и јасним границама употребе.

Посебно је важно питање оспоривости и проверљивости резултата. Ако је лице, група или простор било предмет алгоритамске процене, мора постојати могућност да се провери на основу којих података, критеријума и процедура је процена настала. То не значи да сви технички детаљи система морају бити јавно доступни, нарочито ако би то угрозило безбедност или открило осетљиве оперативне методе. Међутим, морају постојати интерни механизми документације, ревизије и контроле. У супротном, постоји ризик да алгоритамска процена постане непрозирна основа за поступање, без стварне могућности да се утврди да ли је резултат био тачан, сразмеран, законит и релевантан у конкретном случају.

Заштита података о личности представља један од централних правних услова примене предиктивне полицијске аналитике. Ови системи могу обрађивати податке из полицијских евиденција, административних извора, геопросторних база, камера, сензора, IoT/PIoT уређаја, отворених извора и других дигиталних трагова. Управо због тога морају се применити принципи минимизације података, ограничења сврхе, тачности, ограничења чувања, контроле приступа, интегритета и поверљивости. Подаци који су технички доступни нису самим тим и правно оправдани за употребу у предиктивном моделовању.

У AI-native окружењу посебан проблем представља повезивање више извора података. Интеграција полицијских, административних, сензорских, саобраћајних, геопросторних и других података може повећати аналитичку вредност система, али истовремено може довести до ширења надзора, секундарне употребе података и стварања профила који превазилазе првобитну сврху прикупљања. Зато интероперабилност не сме бити схваћена као неконтролисано повезивање свих доступних извора, већ као правно и организационо контролисан процес у коме је за сваки извор података јасно дефинисано зашто се користи, ко му приступа, колико дуго се чува и како се спречава злоупотреба.

Правни ризици су посебно изражени када се аналитички резултат приближава појму индивидуализоване сумње. Предиктивни модел може указати на повећан ризик у одређеном простору, времену или обрасцу понашања, али статистички ризик сам по себи не може заменити конкретан правни основ за полицијско поступање. Berman (2019) управо указује на проблем индивидуализоване сумње у доба великих података, јер статистички изведена процена може изгледати уверљиво, али не мора бити довољна као правни основ за поступање према конкретном лицу. Уколико се алгоритамска процена користи као непосредан основ за интервенцију, без додатне провере и контекстуалне процене, постоји ризик да се превентивна аналитика претвори у непропорционалан или правно спор надзор.

Због тога сваки систем предиктивне и AI-native полицијске аналитике мора имати механизам процене утицаја на права и слободе. Та процена треба да обухвати врсте података који се користе, сврху обраде, могуће ризике по приватност, могућност дискриминације, степен аутоматизације, мере људског надзора, начин документовања одлука и механизме накнадне контроле. Gstrein et al. (2019) истичу да су етички, правни и друштвени изазови предиктивне полиције неодвојиви од питања надзора, одговорности, приватности и легитимитета. Посебно је важно да се процена утицаја не спроводи једнократно, само пре увођења система, већ периодично, јер се модели, подаци, правни услови и друштвени ризици могу мењати током времена.

Регулаторни оквир треба да обухвати и јасно раздвајање аналитичке препоруке од оперативне одлуке. Аналитички систем може указати на повећани ризик, предложити приоритет, означити простор или издвојити образац који захтева пажњу, али коначна одлука мора остати у надлежности овлашћеног службеника. Та одлука мора бити правно утемељена, пропорционална, документована и подложна контроли. У супротном, постоји ризик да формално људски контролисан систем у пракси постане механизам аутоматизованог одлучивања.

Поред заштите података и људског надзора, потребни су и механизми транспарентности и институционалне одговорности. Транспарентност не подразумева откривање осетљивих оперативних метода или безбедносно критичних детаља, већ постојање јасних правила о томе у које сврхе се систем користи, ко је овлашћен да га користи, које категорије података се обрађују, који су механизми контроле и како се спречавају злоупотребе. Meijer et al.

(2021) показују да употреба алгоритама у бирократским организацијама зависи од институционалног контекста, пракси рада и начина на који организација прихвата, тумачи и примењује алгоритамске резултате. Због тога правни оквир мора бити повезан са организационим процедурама, обуком, ревизијом и јасном поделом надлежности.

Уколико ови механизми нису јасно дефинисани, постоји ризик да се технички систем употребљава као инструмент непрозирног или несразмерног надзора. Такав развој би могао угрозити поверење јавности, довести до правних спорова, појачати ризик од дискриминације и ослабити легитимитет полицијске аналитике. Зато се правни и регулаторни оквир не сме посматрати као ограничење технолошког развоја, већ као услов да се предиктивна полицијска аналитика примењује на начин који је законит, сразмеран, проверљив и друштвено прихватљив.

На основу наведеног, унапређени модел мора бити пројектован као систем у коме су правни захтеви уграђени у саму архитектуру, а не додати накнадно. То подразумева контролу приступа, евидентирање активности, документацију модела, процену утицаја, ограничење сврхе, објашњивост, људски надзор и редовну ревизију. Само такав приступ омогућава да предиктивна и AI-native полицијска аналитика буду не само технички ефикасне, већ и правно одрживе, етички прихватљиве и институционално легитимне.

6.6.1. Позиционирање предложеног модела у односу на GDPR и EU AI Act

Посебан значај за примену предиктивне и AI-native полицијске аналитике имају правила која се односе на профилисање, аутоматизовано одлучивање и употребу високоризичних система вештачке интелигенције. У контексту GDPR оквира, односно европских правила о заштити података о личности, посебно је важно да аналитички систем не производи одлуке које су засноване искључиво на аутоматизованој обради и које могу имати правне или слично значајне последице по лице. Иако се полицијска обрада података у ЕУ у великој мери уређује и посебним правилима за надлежне органе, начела законитости, сврхе обраде, минимизације података, тачности, ограничења чувања, безбедности и људске контроле остају суштински релевантна за сваки модел који може утицати на права грађана.

У том смислу, предложени модел се не поставља као систем за аутоматизовано доношење полицијских одлука, већ као систем подршке одлучивању. Аналитички резултат, ризични

сигнал или fuzzy препорука не смеју сами по себи бити основ за полицијску интервенцију, већ морају бити предмет људске провере, контекстуализације, правне процене и институционалног одобрења. Ово је посебно важно зато што предиктивна полицијска аналитика може укључивати податке о простору, времену, кретању, инцидентима, инфраструктури, јавним догађајима и другим факторима који, ако се неконтролисано повежу, могу створити ризик од прекомерног профилисања, непропорционалног надзора или дискриминаторних ефеката.

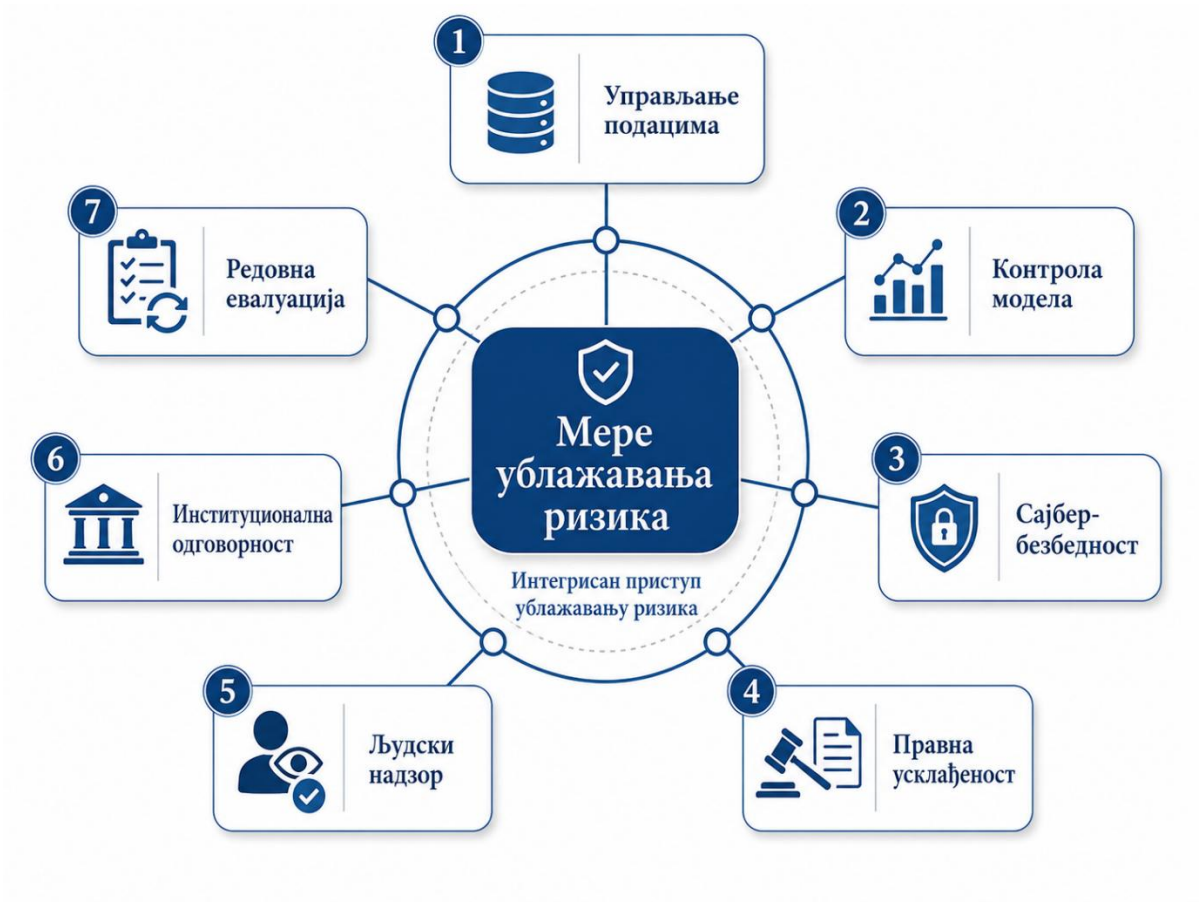
Додатно, EU AI Act уводи ризично заснован приступ регулисању система вештачке интелигенције. Предиктивни системи који се користе у области јавне безбедности, полицијског поступања или процене ризика могу се, у зависности од конкретне сврхе, података, нивоа аутоматизације и последица по лица, посматрати као системи високог ризика. Због тога је за предложени модел важно да већ у фази дизајна буде усклађен са захтевима који се односе на управљање подацима, транспарентност, објашњивост, људски надзор, робусност, безбедност и могућност ревизије.

Предложени евалуациони оквир у овој дисертацији директно одговара таквој регулаторној логици. Техничка евалуација односи се на тачност, стабилност, латенцију и робусност модела. Правно-етичка евалуација обухвата правни основ, пропорционалност, заштиту података, контролу пристрасности и људски надзор. Организациона евалуација проверава да ли су јасно дефинисане улоге, одговорности, процедуре и дневници употребе. Друштвена евалуација укључује питања транспарентности, јавног поверења, жалби и нежељених ефеката. На тај начин се модел позиционира као контролисан, евалуабилан и институционално одговоран систем, а не као аутономни механизам безбедносне процене.

Овакво позиционирање има двоструку вредност. Прво, оно показује да техничка ефикасност модела није довољан услов за његову примену у полицијском контексту. Друго, оно омогућава да се предложени модел већ у фази прототипа развија у складу са принципима законитости, транспарентности, људске контроле, робусности и одговорности. Због тога се у овој дисертацији инсистира на томе да предиктивна полицијска аналитика мора остати систем подршке одлучивању, док коначна одлука мора припадати овлашћеном службенику у оквиру јасно дефинисаних правних и институционалних процедура.

6.7. Мере ублажавања ризика

Мере ублажавања ризика у предиктивној и AI-native полицијској аналитици морају бити системске, вишеслојне и континуиране. Оне не могу бити сведене само на техничко побољшање алгоритма или повећање предиктивне тачности, јер ризици настају у више различитих делова аналитичког процеса: у подацима, моделима, инфраструктури, организационим процедурама, правном оквиру и начину на који људи користе аналитичке резултате. Због тога мере ублажавања морају истовремено обухватити управљање подацима, контролу модела, сајбер-безбедност, правну усклађеност, људски надзор, институционалну одговорност и редовну евалуацију. Овај интегрисани приступ приказан је на слици 6.7.1.



Слика 6.7.1. Интегрисани приступ ублажавању ризика у предиктивној и AI-native полицијској аналитици

Слика 6.7.1 приказује да мере ублажавања ризика морају бити међусобно повезане и истовремено примењене. Управљање подацима обезбеђује да извори буду познати, проверени и правно оправдани; контрола модела омогућава проверу тачности, стабилности и правичности алгоритамских резултата; сајбер-безбедност штити инфраструктуру и интегритет података; правна усклађеност поставља границе дозвољене употребе; људски надзор спречава некритичко прихватање алгоритамских препорука; институционална одговорност одређује ко одобрава, користи, контролише и ревидира систем; док редовна евалуација омогућава праћење стварних ефеката и корекцију модела током времена. На тај начин ублажавање ризика није једнократна техничка интервенција, већ континуиран управљачки процес.

На нивоу података, први корак је идентификација критичних извора података. То су извори код којих постоји ризик од непотпуности, застарелости, селективног евидентирања, историјске пристрасности или неуједначеног прикупљања. Посебну пажњу треба посветити полицијским евиденцијама насталим у условима различитог интензитета контроле по територијама, групама или типовима догађаја, јер такви подаци могу репродуковати раније обрасце поступања. Због тога је неопходно документовати порекло података, начин њиховог прикупљања, степен поузданости, временску покривеност, просторну резолуцију и ограничења употребе (Richardson et al., 2019; Babuta & Oswald, 2019).

Поред тога, за сваки извор података мора бити јасно дефинисана сврха употребе. Подаци који су технички доступни не смеју се аутоматски сматрати дозвољеним за употребу у предиктивном моделу. Потребно је проверити да ли постоји правни основ за њихову обраду, да ли је употреба сразмерна циљу, да ли је у складу са првобитном сврхом прикупљања и да ли постоје ограничења у погледу приступа, чувања и повезивања са другим изворима. На тај начин се смањује ризик да интероперабилност прерасте у неконтролисано повезивање података и ширење надзора.

На нивоу модела, потребно је спроводити систематску валидацију пре, током и након примене. То подразумева тестирање модела на различитим временским периодима, просторним јединицама и подгрупама, као и анализу расподеле грешака. Није довољно да модел има високу укупну тачност ако истовремено производи систематски веће грешке за поједине групе, територије или типове инцидената. Због тога је потребно пратити не само

предиктивну тачност, већ и правичност, стабилност, робусност, промене перформанси током времена и осетљивост на промену улазних података (Alikhademi et al., 2021; Mohler et al., 2018).

Посебну улогу имају технике објашњиве вештачке интелигенције (XAI). Оне треба да омогуће аналитичарима и доносиоцима одлука да разумеју који фактори су утицали на резултат модела, колико је резултат поуздан, која су ограничења процене и у којим условима препоруку не треба користити. Међутим, објашњивост не сме бити схваћена као формални додатак моделу, већ као предуслов критичке употребе резултата. Објашњење мора бити разумљиво корисницима, повезано са конкретним подацима и довољно јасно да омогући људску проверу, а не само да накнадно оправда алгоритамску препоруку (Adadi & Berrada, 2018; Bennett Moses & Chan, 2018).

На нивоу инфраструктуре, неопходно је обезбедити сајбер-безбедност, интегритет података и отпорност система. Предиктивна полицијска аналитика, нарочито у PIoT и AI-native окружењу, зависи од камера, сензора, IoT уређаја, комуникационих мрежа, edge, fog и cloud нивоа обраде, база података и аналитичких платформи. Компромитација било ког дела овог ланца може довести до погрешних података, погрешних предикција и непримерених одлука. Због тога је потребно обезбедити контролу приступа, аутентификацију, ауторизацију, шифровану комуникацију, евидентирање активности, праћење промена, резервне механизме рада и редовно тестирање рањивости система.

Поред класичних сајбер-безбедносних мера, у AI-native окружењу треба предвидети и заштиту самих модела. То подразумева контролу скупа података за обуку, заштиту од тровања података, праћење неочекиваног понашања модела, проверу да ли се модел временом „помера“ у односу на почетне перформансе и заштиту од злонамерних улазних података. У системима који користе машинско учење, дубоко учење или генеративну вештачку интелигенцију, грешке и манипулације могу бити тешко уочљиве, па је потребно успоставити процедуре за редовну техничку и методолошку ревизију.

На институционалном нивоу, потребно је јасно дефинисати ко одобрава модел, ко га користи, ко има право приступа подацима, ко тумачи резултате, ко доноси оперативну одлуку и ко врши контролу након примене. Одговорност не сме бити распршена између ИТ

службе, аналитичара, руководилаца и оперативних службеника на начин који онемогућава накнадну проверу. Свака фаза аналитичког процеса мора имати јасног носиоца одговорности: од управљања подацима и развоја модела, преко валидације и употребе, до евалуације ефеката и поступања по евентуалним примедбама.

Посебно је важно да људска контрола буде стварна, а не формална. Овлашћени службеник или аналитичар мора имати могућност да резултат модела прихвати, допуни, доведе у питање, одложи или одбаци. Да би то било могуће, мора имати приступ објашњењу резултата, информацију о квалитету података, увид у ограничења модела и институционалну подршку да алгоритамску препоруку не прихвати ако је контекстуално, правно или оперативно спорна. У супротном, постоји ризик да људски надзор постане само формално потврђивање резултата система, што појачава аутоматизациону пристрасност и смањује стварну одговорност.

Мере ублажавања морају обухватити и правну контролу. Пре увођења модела потребно је спровести процену утицаја на права и слободе, укључујући заштиту података, ризик од дискриминације, могућност прекомерног надзора, степен аутоматизације и механизме људског надзора. Ова процена не треба да буде једнократна формалност, већ периодична процедура која се понавља приликом значајних промена у моделу, изворима података, правном оквиру, технологији или начину употребе система (Gstrein et al., 2019; European Parliament and Council of the European Union, 2024).

Примена модела треба да буде постепена. Уместо једнократног увођења сложеног система у пуном обиму, пожељно је започети пилот-пројектом на ограниченој територији, ограниченом типу инцидената или ограниченом скупу података. Пилот-фаза треба да омогући тестирање техничке тачности, правичности, објашњивости, организационе употребљивости, утицаја на поступање и прихватљивости за кориснике. Тек након независне евалуације и корекције уочених слабости модел може бити постепено проширивaн.

Независна евалуација представља један од кључних механизама ублажавања ризика. Она треба да обухвати не само техничке метрике, као што су тачност, прецизност, осетљивост или стопа лажних позитивних резултата, већ и стварне ефекте примене: да ли је модел

допринео превенцији, да ли је поступање било пропорционално, да ли су ресурси распоређени оправдано, да ли је било нежељених последица, да ли су поједине групе или простори били непропорционално погођени и да ли је очувано поверење јавности. У том смислу, евалуација мора бити истовремено техничка, организациона, правна и друштвена.

Коначно, мере ублажавања ризика морају укључити обуку корисника и развој организационе културе критичке употребе аналитичких резултата. Полицијски службеници, аналитичари и руководиоци морају разумети шта модел може да уради, шта не може, која су његова ограничења, како се тумачи процена ризика и у којим ситуацијама резултат треба додатно проверити. Без такве обуке, чак и технички добар модел може бити погрешно употребљен, јер ризик не настаје само у алгоритму, већ и у начину на који људи прихватају, тумаче и примењују његове резултате.

На основу наведеног, мере ублажавања ризика треба разумети као континуиран циклус управљања: идентификација ризика, процена утицаја, техничка и правна контрола, пилот-примена, евалуација, ревизија и корекција модела. Само такав приступ омогућава да предиктивна и AI-native полицијска аналитика буду примењене као контролисан систем подршке одлучивању, а не као аутоматизован механизам за производњу полицијских одлука. Унапређени модел зато мора бити пројектован тако да су мере ублажавања ризика уграђене у његову архитектуру од почетка, а не додате накнадно као корективни механизам.

6.8. Људска контрола и етички оквир

Иако се предиктивна аналитика често представља као средство за објективизацију одлука, алгоритам не сме заменити професионалну процену, правно утемељену одговорност и институционалну контролу. Аналитички модел може указати на повећан ризик, издвојити одређени образац, предложити приоритет или подржати распоређивање ресурса, али не може самостално одлучити да ли је конкретно полицијско поступање законито, пропорционално и оправдано. Због тога резултат модела мора бити схваћен као један од улаза у процес одлучивања, а не као коначна одлука.

Људска контрола подразумева да полицијски службеници, аналитичари и руководиоци не прихватају резултате модела некритички, већ да их тумаче у односу на контекст, квалитет података, ограничења модела, законски основ и могуће последице поступања. Коначна

одлука мора бити заснована на провереним подацима, разумевању конкретне ситуације, принципу пропорционалности и могућности накнадне контроле. У том смислу, људска контрола није само формално присуство човека у процесу, већ стварна способност да се алгоритамска препорука прихвати, допуни, доведе у питање, одложи или одбаци.

Етички оквир мора да обухвати принципе правичности, недискриминације, транспарентности, објашњивости, пропорционалности, одговорности, заштите људског достојанства и људске контроле. Ови принципи нису одвојени од техничког модела, већ морају бити уграђени у начин на који се подаци прикупљају, модели развијају, резултати тумаче и одлуке примењују. Основне компоненте етичког оквира приказане су на слици 6.8.1.

Слика 6.8.1. Људска контрола и етички оквир у предиктивној и AI-native полицијској аналитици

Слика 6.8.1 приказује да етички оквир предиктивне и AI-native полицијске аналитике мора повезати више међусобно зависних принципа. Правичност и недискриминација спречавају

да модел репродукује неједнакости или селективне праксе. Транспарентност и објашњивост омогућавају да се разуме како је аналитички резултат настао и под којим ограничењима се може користити. Пропорционалност обезбеђује да поступање буде у складу са степеном ризика и законитим циљем. Одговорност одређује ко је надлежан за податке, модел, тумачење резултата и коначну одлуку. Заштита људског достојанства поставља границу између легитимне аналитичке подршке и прекомерног или непримереног надзора. Људска контрола повезује све ове принципе у практичном процесу одлучивања.

Управљање ризицима у предиктивној и AI-native полицијској аналитици зато није једнократна техничка корекција, већ континуиран процес. Он подразумева стално праћење података, ревизију модела, евалуацију ефеката, обуку корисника, укључивање релевантних институција и очување поверења јавности. Етички оквир има смисла само ако је операционализован кроз конкретне процедуре: документовање одлука, контролу приступа подацима, проверу резултата, могућност ревизије и јасну поделу одговорности.

На основу наведеног, људска контрола и етички оквир представљају завршни услов одговорне примене унапређеног модела. Предиктивна полицијска аналитика може допринети превенцији и раном откривању илегалних активности само ако се користи као контролисан систем подршке одлучивању. У супротном, постоји ризик да технички ефикасан модел постане извор правно спорних, етички неприхватљивих или друштвено неприхваћених одлука.

6.9. Закључна разматрања поглавља

У овом поглављу показано је да су изазови предиктивне и AI-native полицијске аналитике вишеслојни и међусобно повезани. Пристрасност представља један од централних ризика, али није једини. Поред ње, посебно су значајни непоузданост и халуцинације генеративне вештачке интелигенције, непрозирност сложених модела, аутоматизациона пристрасност, сајбер-безбедносни ризици, проблеми заштите података, правна одговорност, могућност прекомерног надзора и питање очувања поверења јавности. Сви ови ризици показују да унапређени модел не може бити развијен као чисто технички систем, већ као контролисан, објашњив, евалуабилан и правно-етички утемељен систем подршке одлучивању.

Због тога решење није у одбацивању предиктивне полицијске аналитике, већ у њеном одговорном пројектовању, примени и континуираној контроли. Унапређени модел мора бити заснован на квалитетним и проверљивим подацима, објашњивим и евалуираним моделима, јасној PIoT архитектури, заштити података, сајбер-безбедности, људској контроли и институционалној одговорности. Само такав приступ може омогућити да предиктивна полицијска аналитика допринесе превенцији и раном откривању илегалних активности, а да истовремено не угрози права грађана, правну сигурност, пропорционалност поступања и поверење јавности.

Закључци овог поглавља представљају основу за даљи развој унапређеног модела, јер јасно показују које ризике модел мора да предвиди, контролише и ублажи већ у фази пројектовања, а не тек након његове оперативне примене.

7. Развој прототипа модела за превенцију и рано откривање илегалних активности

У претходним поглављима показано је да предиктивна полицијска аналитика не може бити сведена на примену једног алгоритма, једног извора података или једне технике предвиђања. Превенција и рано откривање илегалних активности захтевају системски приступ који повезује податке, аналитичке моделе, технолошку инфраструктуру, организационе процедуре, правни оквир, људску контролу и евалуацију ефеката. Због тога се у овом поглављу развија прототип унапређеног модела који представља главни научни и практични допринос дисертације.

Полазиште прототипа је да предиктивна аналитика у области безбедности има вредност само ако се њени резултати могу претворити у благовремено, пропорционално, проверљиво и људски контролисано поступање. Само предвиђање ризика није довољно. Модел мора омогућити да се ризик уочи, контекстуализује, објасни, провери, претвори у одлуку и након тога евалуира. Зато се прототип не дефинише као изоловани предиктивни алгоритам, већ као хијерархијски систем подршке одлучивању у коме су предикција, подршка одлучивању и евалуација повезане у јединствен циклус.

7.1. Полазна идеја и научни допринос прототипа

Прототип модела заснива се на претпоставци да превенција и рано откривање илегалних активности захтевају интеграцију више аналитичких нивоа: од непосредне детекције сигнала у реалном времену, преко краткорочног предвиђања и тактичког усмеравања ресурса, до стратешке анализе и управљања ризиком у условима неизвесности (Meijer & Wessels, 2019; Perry et al., 2013; Fitzpatrick et al., 2019). На најнижем нивоу систем треба да препозна сигнале, догађаје и аномалије у физичком и дигиталном окружењу; на средњем нивоу треба да обезбеди краткорочну предикцију и тактичку координацију; док на највишем нивоу треба да омогући сложенију анализу, fuzzy подршку одлучивању, евалуацију исхода и стратешко планирање.

У односу на приступни рад, у овом поглављу се предлаже конкретнија и операционализована архитектура унапређеног модела. Она повезује полицијску аналитику са инфраструктуром паметног града, Police Internet of Things (PIoT) концептом, edge–fog–

cloud архитектуром, предиктивним моделима, fuzzy логиком, XAI приступом и институционалним механизмима контроле. У односу на објављене PIoT радове, дисертација иде корак даље: не задржава се само на саобраћајном предвиђању и fuzzy одлучивању као студијама случаја, већ те елементе користи као основу за општи модел који може бити прилагођен различитим типовима илегалних активности.

Научни допринос прототипа огледа се у томе што повезује пет компоненти које се у литератури често анализирају одвојено: хијерархијску PIoT инфраструктуру, вертикални ток података, предиктивне аналитичке моделе, fuzzy/XAI подршку одлучивању и континуирану евалуацију са људском контролом. На тај начин прототип превазилази уске hotspot приступе и поставља модел као контролисани, евалуабилни и објашњиви систем подршке превентивном деловању.

Слика 7.1.1. Предложена вертикална PIoT архитектура унапређеног модела

Слика 7.1.1. приказује основну идеју унапређеног модела: подаци из физичког и сајбер окружења улазе у edge ниво, где се врши локална детекција и прелиминарна обрада; затим се релевантни сигнали прослеђују на fog ниво, где се врши краткорочно предвиђање и тактичка координација; док cloud ниво обезбеђује дугорочну интеграцију података, fuzzy подршку одлучивању, објашњивост, евалуацију и стратешко планирање. Посебно је важно

да на свим нивоима буду приказани контролни механизми: заштита података, сајбер-безбедност, људска контрола, правна усклађеност и евалуација исхода.

7.2. Архитектура унапређеног модела

Архитектура унапређеног модела заснива се на три хијерархијска нивоа: ивичном (edge), магленом (fog) и облачном (cloud) нивоу. Ова подела је погодна за полицијску аналитику зато што различите врсте одлука имају различите временске хоризонте, различите последице и различите захтеве у погледу података. Оперативне одлуке захтевају брзу реакцију и минимално кашњење; тактичке одлуке захтевају краткорочну предикцију и координацију ресурса; док стратешке одлуке захтевају дугорочну интеграцију података, процену ефеката и управљање моделима.

Ивични ниво обухвата уређаје и системе који прикупљају податке близу извора: камере, сензоре, бројаче, паметне саобраћајне системе, мобилне уређаје, патролне системе, GPS податке, дронове, системе видео-надзора и друге елементе паметног града. Његова улога је да омогући локалну обраду, препознавање сигнала, детекцију објеката, аномалија или догађаја и прослеђивање само релевантних података ка вишем нивоу. На тај начин се смањује оптерећење централног система, повећава брзина реакције и ограничава непотребан пренос осетљивих података.

Маглени ниво обухвата локалне командне центре, аналитичке сервере, локалне базе података и системе који имају већу рачунарску снагу од ивичних уређаја, али су ближи оперативном окружењу од централног облака. Овај ниво је погодан за краткорочно предвиђање, обједињавање сигнала из више извора, просторну и временску аналитику, корелацију догађаја, тактичку процену ризика и координацију ресурса. На овом нивоу могу се примењивати модели временских серија, класификациони модели, модели откривања аномалија и просторно-временски модели који подржавају одлуке у временском хоризонту од неколико минута до неколико сати.

Облачни ниво представља приватни полицијски облак или контролисано институционално cloud окружење у коме се чувају дугорочни подаци, врше сложене анализе, управља моделима, процењују сценарији, спроводе евалуације и припремају стратешке одлуке. Овај ниво је погодан за интеграцију података из више извора, анализу дугорочних трендова, fuzzy подршку одлучивању, објашњиву вештачку интелигенцију, управљање правилима одлучивања и ревизију модела. Облачни ниво не треба да служи као место аутоматског доношења полицијских одлука, већ као највиши аналитички и управљачки слој који обезбеђује стратешку подршку, контролу и евалуацију.

Табела 7.1. Мапирање нивоа PIoT архитектуре на аналитичке функције

Ниво архитектуре	**Основна функција**	**Извори и системи**	**Модели и алати**	**Временски хоризонт**	**Тип одлуке**
Ивични ниво (edge)	Прикупљање и брза локална обрада података	Камере, сензори, бројачи, IoT уређаји, патролни системи, CCTV, GPS	Видео аналитика, детекција објеката, аларми, локални филтери, предобрада	Секунде	Оперативна реакција
Маглени ниво (fog)	Тактичка координација и краткорочно предвиђање	Локални командни центар, локални сервери, геопросторни подаци, агрегирани edge сигнали	RNN, LSTM, GRU, класификација, корелациона анализа, просторно-временски модели	Минути / сати	Тактичка одлука
Облачни ниво (cloud)	Стратешка анализа, fuzzy подршка одлучивању и евалуација	Приватни полицијски облак, интегрисане базе, архиве, е-управа, административни извори	Fuzzy логика, анализа ризика, XAI, сценарији, евалуација, управљање моделима	Дани / месеци	Стратешка одлука

Табела 7.1 показује да предложени модел није техничка архитектура без организационог значења, већ хијерархијски модел одлучивања. Сваки ниво има различиту улогу у процесу превенције и раног откривања илегалних активности. Ивични ниво је усмерен на брзину и локалну реакцију, маглени ниво на краткорочну предикцију и тактичку координацију, а облачни ниво на дугорочно учење, сложену анализу, управљање ризиком и институционалну контролу.

7.3. Вертикални ток података

Вертикални ток података представља кичму унапређеног модела. Он почиње прикупљањем сигнала из физичког и сајбер окружења: сензорских података, видео-записа, саобраћајних

података, геопросторних података, полицијских евиденција, службених белешки, отворених извора, јавних регистара и других релевантних извора. Међутим, циљ није да се сви доступни подаци неконтролисано интегришу у један систем, већ да се успостави контролисан ток у коме се подаци прикупљају, валидирају, чисте, означавају, трансформишу и користе у складу са сврхом и правним основом.

На ивичном нивоу задржавају се само подаци неопходни за непосредну реакцију и локалну обраду. То значи да систем не треба да шаље све сирове податке у централни систем, већ да на основу дефинисаних правила издваја релевантне сигнале, аномалије или агрегиране показатеље. На пример, уместо континуираног слања целокупног видео-записа, edge уређај може проследити само информацију о детектованом догађају, времену, локацији и нивоу сигурности детекције. Овакво решење смањује оптерећење инфраструктуре и истовремено доприноси минимизацији података.

На магленом нивоу подаци из више edge извора се повезују и анализирају у кратком временском хоризонту. Овде се врши просторно и временско повезивање сигнала, откривање краткорочних образаца, процена да ли се више слабих сигнала може тумачити као релевантан ризик и припрема тактичке препоруке. Маглени ниво има посебну улогу у ситуацијама када појединачни сигнал није довољан за закључак, али комбинација више сигнала указује на могући развој ризичног догађаја.

На облачном нивоу врши се дугорочна интеграција података и њихово коришћење за стратегију, евалуацију и управљање моделима. Овај ниво омогућава анализу трендова, поређење различитих просторних и временских целина, проверу перформанси модела, анализу исхода интервенција и редовну ревизију правила одлучивања. Управо cloud ниво омогућава да модел не буде само реактиван или краткорочно предиктиван, већ да учи из исхода и постаје боље прилагођен стварном безбедносном окружењу.

Слика 7.3.1. Вертикални ток података у унапређеном моделу

Слика 7.3.1, приказјује ток од прикупљања података на edge нивоу, преко предобраде и краткорочне анализе на fog нивоу, до интеграције, евалуације и управљања моделима на cloud нивоу. Посебно треба приказати да се подаци не крећу само навише, већ да постоји и повратни ток: резултати евалуације, нова правила, ажурирани модели и институционалне одлуке враћају се ка нижим нивоима система.

7.4. Циклус података, предикције, одлуке и учења

Унапређени модел треба да функционише као динамичан циклус, а не као линеарни процес. У класичном линеарном приступу подаци се прикупљају, модел производи предикцију, а одлука се доноси на основу добијеног резултата. Такав приступ је недовољан за полицијску аналитику, јер не обезбеђује систематско учење из исхода и може довести до репродукције постојећих образаца у подацима.

Због тога прототип мора да обухвати повратну спрегу. Након сваке интервенције, али и након ситуација у којима се предвиђени ризик није реализовао, систем треба да забележи исход: да ли је ризик био реалан, да ли је интервенција била оправдана, да ли је поступање било пропорционално, да ли је било нежељених последица и да ли су се појавили нови обрасци. Ови подаци затим улазе у процес евалуације и корекције модела.

Повратна спрега има три функције. Прво, омогућава проверу предиктивне тачности и стабилности модела. Друго, омогућава процену стварних ефеката полицијског поступања,

што је важно јер висок степен предиктивне тачности не значи нужно да је модел допринео превенцији. Треће, омогућава контролу пристрасности, јер се може проверити да ли модел непропорционално усмерава пажњу ка одређеним просторима, групама или типовима догађаја.

Слика 7.4.1. Циклус података, предикције, одлуке и учења у унапређеном моделу

Слика 7.4.1. приказјује циклус који обухвата следеће фазе: подаци, обрада, предикција, објашњење, људска процена, одлука, поступање, исход, евалуација и корекција модела. На тај начин се наглашава да унапређени модел није само модел предвиђања, већ модел управљања ризиком и институционалног учења.

7.5. Аналитички слој прототипа

Аналитички слој прототипа састоји се од више функционалних модула који раде на различитим временским и просторним скалама (слика 7.5.1). Његова улога је да из хетерогених извора података издвоји релевантне обрасце, процени ризик, припреми објашњење и обезбеди улаз у процес људски контролисаног одлучивања.

Слика 7.5.1. Аналитички слој прототипа

Први модул је модул за просторну аналитику. Он идентификује концентрације догађаја, промене у ризичним зонама, појаву нових жаришта и просторне обрасце који могу бити релевантни за превенцију. Овај модул користи hot spot анализу, GIS алате, просторну статистику, анализу густине и визуелизацију ризика. Његова улога није само да покаже где се догађаји јављају, већ и да омогући поређење са контекстуалним факторима као што су саобраћај, инфраструктура, демографија, типови објеката и динамика кретања.

Други модул је модул за временску аналитику. Он анализира сезоналност, дневне и недељне обрасце, краткорочне промене, трендове и изненадна одступања. У зависности од типа података, могу се користити класични модели временских серија, регресиони приступи, RNN, LSTM, GRU и други модели дубоког учења. У објављеном PIoT раду показано је да се RNN, LSTM и GRU модели могу користити за краткорочно предвиђање саобраћајног тока на раскрсницама, што у дисертацији служи као емпиријска основа за ширу примену временских серија у полицијској аналитици.

Трећи модул је модул машинског учења и откривања образаца. Он може обухватити класификацију, кластеризацију, откривање аномалија, ансамбл методе, анализу текста,

видео аналитику и моделе за процену приоритета. Овај модул је посебно значајан када постоји велики број променљивих и када се ризик не може поуздано проценити једноставним статистичким показатељима. Ипак, његова примена мора бити праћена контролом квалитета података, провером пристрасности и објашњивошћу резултата.

Четврти модул је модул за обраду неструктурираних података. Он обухвата обраду службених белешки, наративних извештаја, отворених извора, слика, видео-записа и других формата који нису унапред припремљени за класичну статистичку анализу. У овом делу генеративна вештачка интелигенција може имати помоћну улогу у резимирању, категоризацији, претрази, издвајању тема и припреми аналитичких питања. Међутим, резултат генеративне вештачке интелигенције не сме бити самосталан извор сумње, већ мора бити проверен, документован и повезан са изворним подацима.

Пети модул је модул објашњивости. Он треба да обезбеди да резултат модела не буде приказан само као индекс ризика, већ као проверљива аналитичка информација. То подразумева приказ главних фактора који су допринели резултату, степена поузданости, ограничења модела, коришћених извора података и услова под којима се резултат може користити. На тај начин се повећава могућност људске контроле и смањује ризик од некритичког прихватања алгоритамске препоруке.

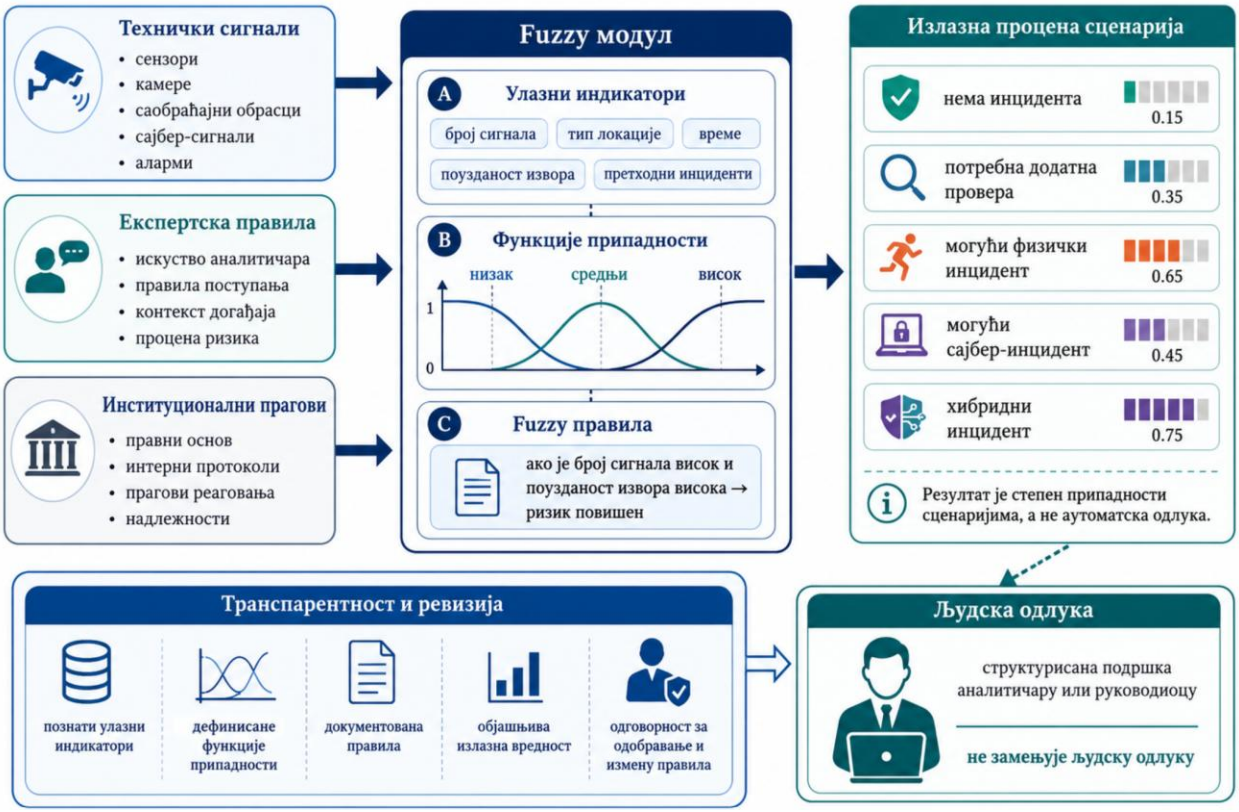
7.6. Fuzzy модул за подршку одлучивању

Fuzzy модул представља једну од кључних компоненти унапређеног модела, јер омогућава подршку одлучивању у ситуацијама у којима су подаци непотпуни, конфликтни, неодређени или различитог квалитета. За разлику од класичне бинарне логике, која ситуацију своди на „да“ или „не“, fuzzy приступ омогућава процену степена припадности одређеним категоријама ризика, као што су низак, средњи или висок ризик, односно различити типови безбедносних сценарија.

У полицијском контексту овај приступ је посебно важан зато што се одлуке често доносе у условима непотпуне информације. На пример, један систем може указати на покрет у заштићеном простору, други на прекид комуникације, трећи на неуобичајен саобраћајни образац, док четврти може указати на могући сајбер-инцидент. Ниједан сигнал сам по себи

не мора бити довољан за закључак, али њихова комбинација може указивати на сценарио који захтева пажњу.

Fuzzy модул може објединити техничке сигнале, експертска правила и институционалне прагове поступања (слика 7.6.1.). Уместо да систем аутоматски донесе одлуку, fuzzy правила могу израчунати степен припадности различитим сценаријима, на пример: „нема инцидента“, „потребна додатна провера“, „могући физички инцидент“, „могући сајбер-инцидент“, „хибридни инцидент“. Такав резултат представља структурирану подршку аналитичару или руководиоцу, али не замењује људску одлуку.



Слика 7.6.1. Fuzzy модул унапређеног модела прототипа

Унапређени модел треба да омогући да fuzzy правила буду транспарентна, документована и подложна ревизији. То значи да мора бити познато који улазни индикатори се користе, како су дефинисане функције припадности, која правила се примењују, како се добија излазна вредност и ко је одговоран за одобравање и измену правила. На тај начин fuzzy

модул постаје не само технички алат, већ и механизам формализације експертског знања и институционалних правила.

Табела 7.2. Пример структуре fuzzy модула за процену ризика

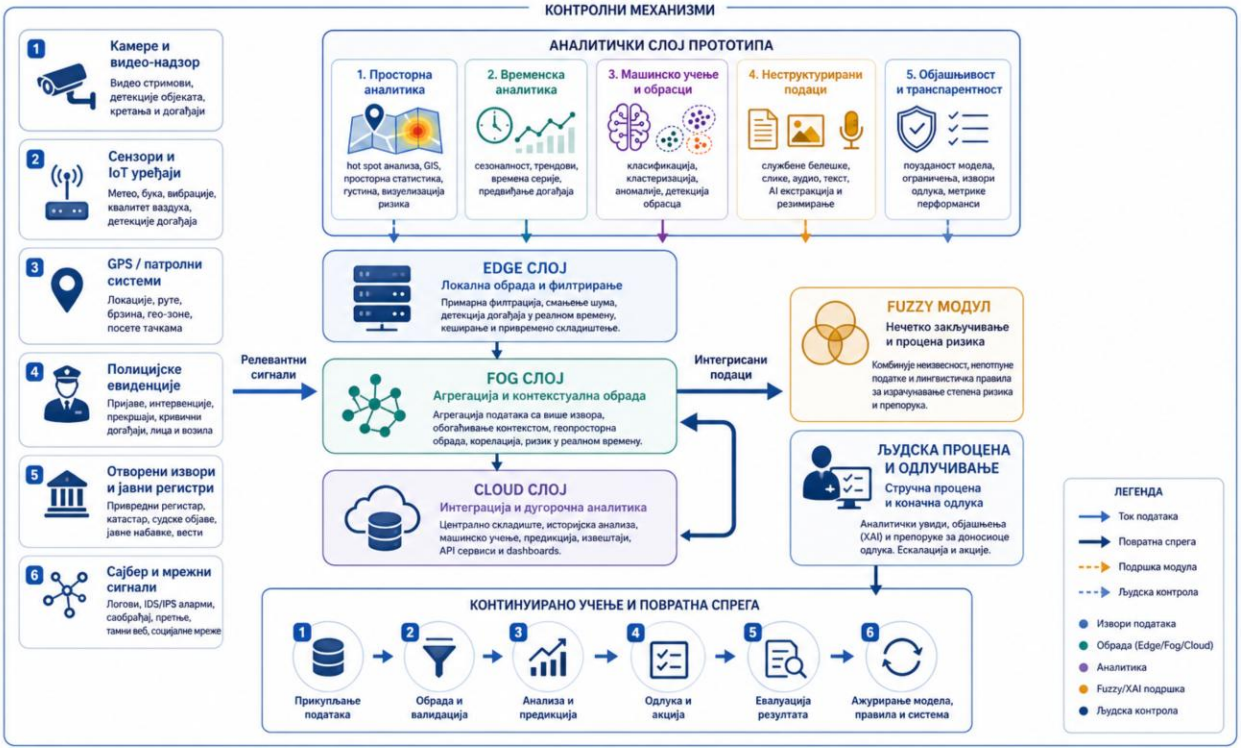
Елемент fuzzy модула	**Пример улаза / правила**	**Улога у моделу**
Улазни индикатори	број сигнала, тип локације, време догађаја, поузданост извора, претходни инциденти, сајбер-сигнали	Описују контекст ризика
Лингвистичке вредности	низак, средњи, висок; слаб, умерен, јак; краткотрајан, понављајући, интензиван	Омогућавају рад са неодређеношћу
Fuzzy правила	ако је број сигнала висок и поузданост извора висока, онда је ризик повишен	Формализују експертско знање
Излазна процена	низак ризик, потребна провера, висок ризик, критичан ризик	Припрема улаз за људску процену
Контролни механизам	људска провера, правни основ, XAI објашњење, ревизија правила	Спречава аутоматизовано поступање

Fuzzy модул је нарочито погодан за cloud ниво PIoT архитектуре, где се могу објединити технички подаци, стратешки индикатори, историјски обрасци, правила поступања и процена несигурности. Међутим, поједини једноставнији fuzzy механизми могу бити корисни и на fog нивоу, посебно када треба брзо проценити да ли комбинација сигнала захтева тактичку реакцију или додатну проверу.

7.7. Интегрисани приказ прототипа модела

Након појединачног разматрања архитектуре, вертикалног тока података, аналитичких модула, fuzzy подршке одлучивању и улоге људске контроле, могуће је сагледати целину предложеног прототипа као јединствен аналитичко-оперативни систем. У том систему различити извори података, нивои PIoT архитектуре, аналитички модули, механизми подршке одлучивању и повратна спрега нису посматрани изоловано, већ као међусобно повезане компоненте унапређеног модела.

На слици 7.7.1 приказан је интегрисани прототип модела за превенцију и рано откривање илегалних активности. Слика синтетизује основне изворе података, вертикални ток обраде кроз edge, fog и cloud ниво, аналитички слој прототипа, fuzzy модул, људску процену и одлучивање, као и механизам континуираног учења и повратне спреге.



Слика 7.7.1. Интегрисани прототип модела за превенцију и рано откривање илегалних активности

Слика 7.7.1 показује да унапређени модел није заснован на једном алгоритму, већ на хијерархијски организованом систему у којем се подаци из више хетерогених извора прикупљају, филтрирају, интегришу и анализирају на различитим нивоима архитектуре. Ивични ниво је задужен за локалну обраду и детекцију релевантних сигнала, маглени ниво за контекстуализацију и краткорочну предикцију, док облачни ниво омогућава дугорочну интеграцију података, сложенију аналитику и стратешко управљање ризиком.

Посебан значај има аналитички слој прототипа, који обједињује просторну и временску аналитику, машинско учење и откривање образаца, обраду неструктурираних података, као и модул објашњивости и транспарентности. На тај начин резултат модела није само

предикција, већ структурисана аналитичка информација која укључује контекст, факторе ризика, ограничења и процену поузданости.

Fuzzy модул је у моделу позициониран као механизам за подршку одлучивању у условима неизвесности, непотпуних или конфликтних сигнала. Његова улога није да аутоматски донесе коначну одлуку, већ да формализује експертска правила и припреми структурирану процену ризика за аналитичара или руководиоца. Коначна одлука зато остаје у домену људске процене и институционалне одговорности.

Доњи део слике наглашава да модел функционише као циклус континуираног учења. Након анализе, одлуке и поступања, резултати се евалуирају, а сазнања се користе за ажурирање модела, правила и прагова одлучивања. Управо та повратна спрега омогућава да прототип не остане статичан систем, већ да се временом прилагођава променама у обрасцима ризика, квалитету података и оперативним потребама.

Овако постављен интегрисани приказ јасно показује да је предложени прототип истовремено технички, аналитички и организациони модел. Његова сврха није само да предвиди ризик, већ да обезбеди проверљиву, објашњиву и људски контролисану подршку одлучивању у процесу превенције и раног откривања илегалних активности.

7.8. Излазни резултати модела прототипа

Излаз унапређеног модела не треба да буде само један број, једна ознака ризика или аутоматски генерисана препорука за поступање. Такав поједностављен излаз повећао би опасност од погрешног тумачења, прекомерног ослањања на алгоритам и некритичког прихватања аналитичког резултата као коначне одлуке. Уместо тога, излаз модела треба да буде структуриран аналитички налаз који омогућава разумевање, проверу, тумачење и одговорну употребу резултата у процесу људски контролисаног одлучивања.

Основна сврха излазног резултата није да замени полицијског службеника, аналитичара или руководиоца, већ да им обезбеди проверљиву и употребљиву управљачку информацију. Та информација треба да покаже на који простор, време, тип догађаја или сценарио се процена односи, који фактори су утицали на резултат, колико је процена поуздана, која су ограничења тумачења и да ли је потребна додатна провера пре било каквог поступања. На

тај начин излаз модела повезује аналитички слој, fuzzy/XAI подршку, људску контролу и накнадну евалуацију.

Препоручује се да излаз модела садржи најмање следеће елементе: индекс ризика, простор и време на које се ризик односи, тип ризика или сценарија, главне факторе који су утицали на процену, степен поузданости, ограничења тумачења, препоручени ниво пажње, могуће мере поступања, статус људске провере и евиденцију донете одлуке. Оваква структура омогућава да резултат буде користан оперативним службеницима, аналитичарима и руководиоцима, али и да касније буде предмет евалуације, ревизије и контроле.

Табела 7.3. Препоручена структура излазног резултата унапређеног модела

Компонента излаза	**Опис**	**Сврха**
Индекс ризика	Нумеричка или категоријална процена ризика, на пример низак, средњи, висок или критичан ризик	Омогућава брз увид у ниво ризика
Просторно-временски обухват	Локација, зона, рута, објекат или временски интервал на који се процена односи	Ограничава важење процене и спречава претерано ширење закључка
Тип ризика / сценарио	Криминални, саобраћајни, сајбер-физички, хибридни, јавни ред или други безбедносно релевантан сценарио	Контекстуализује резултат и повезује га са типом поступања
Главни фактори	Најважнији индикатори који су утицали на процену: број сигнала, тип локације, време, претходни инциденти, поузданост извора и сл.	Омогућава објашњивост и критичко тумачење резултата
Поузданост процене	Степен сигурности модела, квалитет података, број извора, несигурност и могућност грешке	Спречава претерано поверење у резултат
Препоручени ниво пажње	Нема поступања, потребна додатна провера, појачано праћење, тактичка координација или стратешка анализа	Помаже у одређивању интензитета институционалне реакције
Могуће мере поступања	Провера података, додатно прикупљање информација, усмеравање патроле, превентивна мера, координација са другим службама	Претвара аналитички налаз у управљачку информацију
Ограничења тумачења	Недостајући подаци, могућа пристрасност, ограничена валидност, кратак временски хоризонт, непотпун контекст	Подржава људску контролу и спречава некритичку примену

Статус људске провере	Ко је прегледао резултат, да ли је препорука прихваћена, допуњена, одложена или одбачена	Обезбеђује стварну, а не само формалну људску контролу
Евиденција одлуке и исхода	Ко је донео одлуку, шта је одлучено, која мера је предузета и какав је исход забележен	Омогућава накнадну контролу, евалуацију и учење модела

Овакво структурирање излазног резултата важно је јер смањује ризик да алгоритамска процена буде схваћена као коначна одлука. Уместо тога, резултат се третира као аналитичка информација која мора бити протумачена у контексту конкретне ситуације, правног основа, пропорционалности, расположивих ресурса и могућих последица поступања. Посебно је важно да сваки излаз садржи и ограничења тумачења, јер управо тај део спречава да се модел представи као потпуно сигуран или неутралан извор истине.

Излазни резултати могу се разликовати у зависности од нивоа PIoT архитектуре. На ивичном нивоу излаз је најчешће брз сигнал, аларм или иницијална детекција догађаја. На магленом нивоу излаз може бити краткорочна процена ризика, упозорење о промени обрасца или тактичка препорука за додатну проверу. На облачном нивоу излаз је сложенији аналитички налаз који обухвата интеграцију више извора, сценарије, fuzzy процену, XAI објашњење, евалуацију исхода и препоруке за стратешко планирање.

Унапређени модел зато не производи само предикцију, већ проверљиву основу за одлучивање. Његова вредност није у томе да понуди „аутоматски одговор“, већ да омогући да овлашћени корисник разуме шта је модел уочио, на основу којих података, са којим степеном поузданости, уз која ограничења и под којим условима резултат може бити употребљен. Само такав излаз омогућава да предиктивна полицијска аналитика остане систем подршке одлучивању, а не механизам аутоматизованог полицијског поступања.

На крају, структура излазног резултата има значај и за континуирано учење модела. Ако се уз сваку процену бележи шта је модел предложио, како је резултат протумачен, која је одлука донета и какав је исход наступио, тај запис постаје основ за накнадну евалуацију, откривање грешака, проверу пристрасности и корекцију модела. На тај начин излазни резултат није само крај аналитичког процеса, већ и почетак новог циклуса учења и унапређења модела.

7.9. Оквир за евалуацију прототипа

Евалуација представља саставни део развоја прототипа, јер унапређени модел не може бити оцењиван само на основу предиктивне тачности. У полицијској аналитици није довољно утврдити да ли је модел технички успешно предвидео одређени догађај, простор или временски интервал. Потребно је проверити и да ли је резултат био употребљив у оперативном раду, да ли је препорука била разумљива корисницима, да ли је поступање било пропорционално, да ли су подаци коришћени у складу са правним основом и да ли су избегнути нежељени ефекти, као што су пристрасност, прекомерно усмеравање ресурса или смањење поверења јавности.

Због тога се евалуација прототипа мора посматрати као вишедимензионалан процес који обухвата техничке, оперативно-организационе, правно-етичке и друштвене критеријуме. Технички критеријуми односе се на тачност, стабилност, робусност и латенцију модела. Оперативно-организациони критеријуми односе се на употребљивост резултата у реалном раду, време реакције, јасноћу препоруке и утицај на распоред ресурса. Правно-етички критеријуми обухватају законитост, пропорционалност, објашњивост, људску контролу и заштиту података, док друштвени критеријуми укључују недискриминацију, избегавање прекомерног надзора, транспарентност и поверење јавности.

У овом поглављу евалуација се помиње само као неопходна компонента прототипа и као део његовог циклуса континуираног учења. Детаљна методологија евалуације, укључујући фазе тестирања, техничке метрике, оперативну употребљивост, правно-етичку проверу и механизме унапређења модела, разрађује се у наредном поглављу.

7.10. Прототип као истраживачко решење и основ за пилот-примену

Прототип који се развија у овој дисертацији треба посматрати као истраживачко решење које има задатак да покаже изводљивост, логичку утемељеност и применљивост унапређеног модела. То значи да није неопходно да прототип одмах обухвати целокупни национални систем, све институционалне изворе података или све облике илегалних активности. Његова основна сврха је да покаже да је предложена архитектура изводљива, да је методолошки оквир логички повезан, да су одабрани аналитички модули употребљиви

и да се предикција може повезати са подршком одлучивању, људском контролом и евалуацијом исхода.

У том смислу, прототип може бити реализован као контролисано пилот-окружење. Пилот-примена може бити ограничена на одређену територију, одређени тип догађаја, одређени скуп података или ограничен број аналитичких сценарија. Такво ограничење није слабост, већ методолошки оправдан приступ, јер омогућава проверу модела у контролисаним условима, без ризика неконтролисане примене на шири систем. Пилот-окружење треба да има јасно дефинисане улазне податке, сценарије, аналитичке модуле, правила одлучивања, метрике успеха и механизме контроле.

Прототип треба да покаже три врсте изводљивости. Прва је техничка изводљивост: да ли је могуће прикупити, обрадити, интегрисати и анализирати податке кроз edge–fog–cloud архитектуру. Друга је аналитичка изводљивост: да ли модели временских серија, машинског учења, обраде неструктурираних података, објашњивости и fuzzy подршке могу произвести употребљиве и проверљиве резултате. Трећа је институционална изводљивост: да ли се добијени резултати могу уклопити у полицијске процедуре, људску контролу, правне услове, механизме евалуације и организациону одговорност.

Овако схваћен прототип представља прелаз између теоријског модела и оперативне примене. Он омогућава да се унапређени модел тестира у ограниченом и контролисаном окружењу, да се уоче техничка, аналитичка, организациона, правна и етичка ограничења, као и да се на основу резултата евалуације изврше корекције пре шире примене. Због тога прототип има двоструку улогу: научну, јер омогућава проверу предложеног модела, и практичну, јер представља основу за будућу пилот-примену у реалном институционалном окружењу.

7.11. Логика имплементације прототипа

Имплементација прототипа треба да буде фазна, контролисана и евалуабилна, што је приказано на слици 7.11.1.

7.11.1. Фазна имплементација прототипа

Прва фаза подразумева дефинисање обухвата пилота: избор типа илегалних активности, избор територије, дефинисање извора података, правног основа и институционалних актера. У овој фази се утврђује шта је предмет предвиђања, који подаци се могу користити и који су критеријуми успеха.

Друга фаза подразумева припрему података и изградњу аналитичког окружења. Она обухвата чишћење података, стандардизацију, геокодирање, временско означавање, дефинисање индикатора, проверу квалитета и успостављање контролисаног вертикалног тока података. У овој фази је неопходно документовати сваки извор података и ограничења његове употребе.

Трећа фаза подразумева развој и тестирање аналитичких модула. У зависности од доступних података, могу се тестирати статистички модели, модели временских серија, модели машинског учења, fuzzy правила и XAI објашњења. У овој фази је важно поредити сложеније моделе са базним моделима, како би се утврдило да ли сложеност доноси стварну аналитичку вредност.

Четврта фаза подразумева контролисану пилот-примену. У овој фази резултати модела не треба да производе аутоматске одлуке, већ се користе као подршка аналитичарима и руководиоцима. Свака препорука треба да буде документована, објашњена и проверена, а коначна одлука мора остати у надлежности овлашћеног службеника.

Пета фаза подразумева евалуацију и корекцију. Она обухвата анализу техничких перформанси, оперативне употребљивости, правне усклађености, етичких ефеката, корисничког искуства и могућих нежељених последица. На основу евалуације модел се коригује, правила се ревидирају, а обухват примене се може постепено проширивати.

Посебан елемент имплементације прототипа односи се на операционализацију људске контроле. Унапређени модел не може бити примењен као аутономни систем који самостално доноси полицијске одлуке, већ као систем подршке одлучивању у коме су јасно дефинисане улоге, надлежности и тачке контроле. Због тога је у пилот-примени потребно разликовати најмање три групе улога: аналитичара, оперативног руководиоца и правно-етичку контролу.

Аналитичар је задужен за проверу улазних података, тумачење аналитичког резултата, контролу квалитета модела и припрему објашњења препоруке. Он нема овлашћење да самостално наложи оперативно поступање, али има право да означи резултат као непоуздан, да затражи додатну проверу података, да предложи ревизију параметара или fuzzy правила и да документује уочене неправилности у раду модела.

Оперативни руководилац је носилац одлуке о томе да ли ће се препорука модела прихватити, одбити или модификовати у складу са оперативним околностима, расположивим ресурсима и законским овлашћењима. Он је одговоран за превођење аналитичког налаза у конкретну меру поступања, али само након провере контекста, пропорционалности и оправданости интервенције. Одлука оперативног руководиоца мора бити документована, нарочито у случајевима када се значајно одступа од препоруке модела или када се препорука користи као основ за појачано поступање.

Правно-етичка контрола, која може бити организована кроз правног официра, интерни надзорни тим или етичко-ревизиони одбор, има задатак да проверава законитост, пропорционалност, заштиту података, објашњивост и могуће дискриминаторне ефекте примене модела. Овај ниво контроле има право да захтева измену правила, ограничење употребе одређених података, додатну процену утицаја или привремену обуставу примене модела ако се утврди ризик од систематске пристрасности, прекомерног надзора или правно спорне употребе резултата.

У оквиру пилот-примене потребно је предвидети и посебан „emergency stop“ протокол, односно процедуру хитне обуставе употребе модела. Тај протокол се активира ако се уочи систематска грешка, висок број лажно позитивних сигнала, необјашњиво фаворизовање одређених простора или група, повреда правила о заштити података, сајбер-компромитација система или други ризик који може угрозити права грађана или законитост поступања. Активирање овог протокола мора бити документовано, а наставак примене модела могућ је тек након ревизије података, параметара, правила, правног основа и процедура људске контроле.

Овако дефинисана људска контрола омогућава да се предложени модел примењује као контролисан аналитичко-оперативни систем. Његова улога није да замени аналитичара, руководиоца или правну процену, већ да обезбеди проверљиву, објашњиву и документовану подршку одлучивању. Тиме се смањује ризик од аутоматизационе пристрасности и обезбеђује да коначна одговорност остане на овлашћеним људским актерима унутар институционалног оквира.

7.12. Закључна разматрања о прототипу

Предложени прототип представља унапређени модел за превенцију и рано откривање илегалних активности применом предиктивне аналитике. Његова основна вредност није у примени једног напредног алгоритма, већ у интеграцији више аналитичких, технолошких, организационих и контролних елемената у јединствену архитектуру. Та архитектура повезује вертикални PIoT оквир, edge–fog–cloud обраду података, вертикални ток података, просторно-временску аналитику, моделе машинског учења, обраду неструктурираних података, fuzzy подршку одлучивању, објашњивост, људску контролу и континуирану евалуацију.

У односу на постојеће приступе, предложени прототип настоји да превазиђе три кључна ограничења. Прво, предикцију не посматра као коначни циљ, већ као један корак у ширем процесу превенције, одлучивања, поступања и учења. Друго, технологију не третира као самосталан основ за полицијско поступање, већ као подршку људском, институционално одговорном и правно утемељеном одлучивању. Треће, техничку архитектуру повезује са

правним, етичким и организационим предусловима, чиме се повећава могућност одговорне и контролисане примене модела.

Посебан значај прототипа огледа се у томе што омогућава да се различити нивои одлучивања раздвоје, али и међусобно повежу. Ивични ниво обезбеђује брзу локалну обраду и детекцију сигнала; маглени ниво омогућава краткорочну анализу, предикцију и тактичку координацију; док облачни ниво подржава дугорочну интеграцију података, сложенију аналитику, fuzzy/XAI подршку, евалуацију и стратешко управљање ризиком. На тај начин прототип повезује оперативне, тактичке и стратешке потребе у један хијерархијски систем подршке одлучивању.

На тај начин прототип представља централни допринос дисертације: он преводи претходну теоријску, методолошку и критичку анализу у конкретан модел који може бити тестиран, евалуиран и даље развијан. Његова примена не треба да буде схваћена као једнократно увођење сложеног техничког система, већ као постепен, контролисан и проверљив процес развоја предиктивне полицијске аналитике у условима паметних градова и хибридног физичко-сајбер окружења.

Закључно, предложени прототип показује да унапређење модела за превенцију и рано откривање илегалних активности није питање само предиктивне тачности, већ питање изградње целокупног аналитичко-оперативног оквира. Тај оквир мора бити хијерархијски, интероперабилан, објашњив, евалуабилан и контролисан. Управо зато се у наредном поглављу посебно разрађује евалуација модела, односно начин на који се може проверити његова техничка успешност, оперативна употребљивост, правна прихватљивост и етичка одрживост.

8. Евалуација модела

Евалуација модела представља завршну, али истовремено и развојну фазу унапређеног модела за превенцију и рано откривање илегалних активности. У претходном поглављу прототип је дефинисан као хијерархијски, интероперабилан, објашњив, евалуабилан и људски контролисан систем подршке одлучивању. Због тога се његова успешност не може процењивати само на основу техничке тачности предвиђања, већ мора обухватити и питања оперативне употребљивости, организационе применљивости, правне прихватљивости, етичке одрживости и стварног доприноса превенцији.

Основна претпоставка овог поглавља јесте да модел који има добру предиктивну тачност није нужно успешан модел у полицијском контексту. Модел може прецизно указивати на повећан ризик, али ако резултати нису разумљиви корисницима, ако нису правно употребљиви, ако доводе до несразмерног поступања, ако производе пристрасне ефекте или ако се не могу уклопити у организационе процедуре, такав модел не може бити основа одговорне институционалне примене. Зато евалуација мора бити вишедимензионална и мора обухватити целокупан животни циклус прототипа: податке, архитектуру, аналитичке модуле, излазне резултате, људску контролу, поступање и евалуацију исхода.

8.1. Циљ евалуације

Циљ евалуације је да утврди да ли унапређени модел заиста доприноси превенцији и раном откривању илегалних активности, и то на више међусобно повезаних нивоа. У техничком смислу, проверава се тачност предвиђања, стабилност модела, робусност, латенција, квалитет података и способност рада у различитим сценаријима. У оперативном и организационом смислу, процењује се да ли резултати модела помажу аналитичарима, руководиоцима и овлашћеним службеницима да донесу брже, боље, пропорционалније и документоване одлуке. У правно-етичком смислу, проверава се да ли су испоштовани принципи законитости, заштите података, транспарентности, недискриминације, људске контроле и одговорности (Meijer & Wessels, 2019; Bennett Moses & Chan, 2018; Gstrein et al., 2019; Oswald et al., 2018).

Тако постављена евалуација одговара савременом схватању предиктивне полицијске аналитике као система подршке одлучивању, а не само као алгоритма за прогнозу. Због тога

предмет евалуације није само модел у ужем смислу, већ читав прототип: архитектура, вертикални ток података, аналитички модули, fuzzy/XAI подршка, начин приказа резултата, људска контрола, организациони контекст употребе и механизам повратне спреге (Perry et al., 2013; Casey et al., 2014; Meijer et al., 2021; Oatley, 2021).

Евалуација има три основне функције. Прва је валидациона: да се утврди да ли модел ради у складу са постављеним циљевима и да ли производи употребљиве резултате. Друга је контролна: да се провери да ли модел производи нежељене ефекте, пристрасност, прекомерно ослањање на алгоритам или правно спорне резултате. Трећа је развојна: да се резултати евалуације искористе за корекцију података, параметара, правила, модела, визуелизација и процедура.

Слика 8.1. Мултидимензионални оквир валидације прототипа унапређеног модела

Слика 8.1 приказује да евалуација прототипа треба да обухвати четири међусобно повезане димензије: техничку, оперативно-организациону, правно-етичку и друштвену. Техничка димензија одговара на питање да ли модел добро предвиђа и стабилно функционише. Оперативно-организациона димензија проверава да ли је модел употребљив у реалном раду. Правно-етичка димензија процењује да ли је модел законит, пропорционалан, објашњив и контролисан. Друштвена димензија процењује да ли модел доприноси превенцији без

нарушавања поверења јавности и без репродукције дискриминаторних или непропорционалних ефеката.

8.2. Методологија тестирања

Евалуација прототипа треба да буде фазна, како би се постепено прешло од лабораторијске провере ка ограниченој оперативној примени. Такав приступ је методолошки оправдан јер смањује ризик да се сложен систем примени у реалном окружењу без претходне провере података, модела, процедура, правног основа и људске контроле.

Први корак је тестирање на историјским подацима. У овој фази проверава се да ли модел може да предвиди догађаје који су се већ десили, али који нису били доступни у тренутку тренирања. Ово представља основни облик backtesting приступа у предиктивној аналитици. Посебно је важно да се подаци деле хронолошки, а не случајно, како би се избегла ситуација да модел индиректно „види“ будућност кроз неправилно формиране скупове за тренирање и тестирање (Joshi et al., 2021; Perry et al., 2013).

Други корак је тестирање у симулираном оперативном окружењу. У овој фази проверава се како систем реагује на сценарије са непотпуним, конфликтним, шумовитим или закашњелим подацима. Ово је посебно важно за хибридне физичко-сајбер ситуације, за модуле детекције аномалија и за fuzzy модул, који треба да подржи одлучивање у условима неизвесности и неодређености (Shalaginov, 2018; Khalid et al., 2021).

Трећи корак је контролисани пилот, уколико правни, организациони и технички услови то дозвољавају. Пилот-примена треба да буде ограничена на одређену територију, тип догађаја или скуп података, уз јасно дефинисане критеријуме успеха и механизме контроле. У овој фази резултати модела не смеју бити основ за аутоматско поступање, већ само подршка аналитичарима, руководиоцима и овлашћеним службеницима.

Четврти корак подразумева ревизију резултата и унапређење прототипа. На основу резултата тестирања и пилот-примене врши се анализа грешака, корекција модела, ревизија fuzzy правила, провера објашњивости, процена пристрасности, ажурирање процедура и поновно тестирање. Овај приступ је у складу са искуствима из евалуација пилот-пројеката

у предиктивној полицији, као што су RAND студије и квазиекспериментalне анализе полицијских пилота (Hunt et al., 2014; Saunders et al., 2016; Mohler et al., 2015).

Оваква методологија је важна зато што спречава да се модел оцењује искључиво на основу једне метрике или једног скупа података. Уместо тога, евалуација се заснива на више нивоа провере: статистичком, сценаријском, оперативном, организационом, правном и етичком (Fitzpatrick et al., 2019; Ferguson, 2020).

8.3. Метрике техничке успешности

Техничка евалуација има задатак да утврди да ли аналитички модули прототипа дају тачне, стабилне и употребљиве резултате. Пошто прототип обухвата различите модуле, не постоји једна универзална метрика која би била довољна за његову процену. Метрике морају бити прилагођене типу модела, врсти података, временском хоризонту и последицама грешке.

За моделе предвиђања временских серија користе се метрике као што су MAE, MSE, RMSE, MAPE и коефицијент детерминације. Оне омогућавају да се измери просечна грешка, осетљивост на већа одступања и стабилност модела кроз време (Vinodhini et al., 2020; Joshi et al., 2021). Код полицијске аналитике посебно је важно да се метрике не тумаче изоловано, јер мала просечна грешка не мора значити да је модел користан у ситуацијама ретких, али важних инцидената.

За класификационе моделе користе се тачност, прецизност, одзив, F1 мера, AUC и матрица конфузије. Ове метрике су посебно важне у ситуацијама у којима су класе неравномерно распоређене и где лажно позитивни и лажно негативни налази имају различите оперативне последице. Лажно позитиван резултат може довести до непотребног ангажовања ресурса и прекомерног надзора, док лажно негативан резултат може значити пропуштање стварног ризика (Berk, 2021; Alikhademi et al., 2021).

За моделе детекције аномалија кључни су стопа лажних позитивних и лажних негативних сигнала, време детекције, стабилност у условима шумовитих података и способност раног откривања неуобичајених образаца. Ове метрике су важне јер обе врсте грешке могу имати озбиљне последице: или преоптерећење ресурса, или пропуштање стварног инцидента (Pramanik et al., 2017; King et al., 2020).

За fuzzy модул користе се стабилност правила, осетљивост на промене улазних параметара, усаглашеност са експертском проценом и разумљивост излазне препоруке. Пошто fuzzy модул има улогу подршке одлучивању у условима неодређености, његова успешност не мери се само нумеричком тачношћу, већ и тиме да ли производи објашњиву, контролисану и институционално употребљиву препоруку (Shalaginov, 2018; Khalid et al., 2021).

Табела 8.1. Метрике евалуације према типу аналитичког модула

Тип модула	**Метрике**	**Пример примене**	**Критеријум успеха**
Временске серије	MAE, MSE, RMSE, MAPE, R^2	Краткорочно предвиђање саобраћаја, инцидената или позива	Најмања грешка уз стабилност кроз време
Класификација	Тачност, прецизност, одзив, F1, AUC, матрица конфузије	Разврставање пријава или догађаја по приоритету	Равнотежа између пропуштених и лажних аларма
Детекција аномалија	Лажно позитивни/негативни сигнали, време детекције, стабилност у шумовитим подацима	Неуобичајени обрасци у физичком или сајбер простору	Брза детекција без преоптерећења ресурса
Fuzzy одлучивање	Осетљивост правила, експертска усаглашеност, стабилност излаза, разумљивост препоруке	Конфликтни сигнали и неодређени сценарији	Разумљива, стабилна и контролисана препорука

Поред класичних метрика, корисно је применити и метрике које су прилагођене ретким и просторно неравномерно распоређеним догађајима, јер традиционални индикатори понекад не одражавају реалну вредност модела у безбедносном окружењу (Adepeju et al., 2016; Kounadi et al., 2020). Због тога техничка евалуација мора бити повезана са оперативном и правно-етичком проценом, а не посматрана као самосталан доказ успешности.

8.4. Оперативна и организациона евалуација

Техничка тачност није довољна ако модел не доводи до бољих оперативних одлука. Зато се евалуација мора проширити на питања оперативне употребљивости: да ли је препорука стигла на време, да ли је разумљива службеницима, да ли је помогла у расподели ресурса, да ли је смањила време реакције, да ли је довела до мањег броја непотребних интервенција и да ли је омогућила боље планирање патрола, контрола или превентивних активности (Camacho-Collados & Liberatore, 2015; Casey et al., 2014; College of Policing, 2021).

Оперативна евалуација треба да прати цео пут од аналитичке препоруке до стварног поступања. То подразумева да се евидентира када је препорука генерисана, коме је достављена, како је протумачена, да ли је прихваћена, допуњена, одложена или одбачена, која је одлука донета и какав је исход наступио. На тај начин се може утврдити да ли модел заиста подржава превентивно деловање или само производи додатне информације које нису употребљиве у реалном раду.

Организациона евалуација треба да укључи интервјуе и упитнике са корисницима система, анализу дневника употребе, праћење одступања између препоруке и коначне одлуке и анализу разлога због којих су службеници прихватили или одбили препоруку (Meijer et al., 2021; Ilijazi et al., 2019). Ово је важно зато што модел не сме постати ни формална процедура која се игнорише, нити неформална обавеза која се слепо прати, већ контролисан алат подршке одлучивању у коме човек задржава кључну улогу (Joh, 2020; Bennett Moses & Chan, 2018).

У овој димензији евалуације посебно је важно пратити однос између препоруке и исхода. Уколико службеници систематски одбијају препоруке модела, потребно је испитати да ли је проблем у слабом поверењу, неразумљивости интерфејса, лошем времену испоруке информације или стварној недовољној употребљивости модела у оперативном раду. Са друге стране, ако се препоруке модела прихватају без критичке провере, то може указивати на ризик од аутоматизационе пристрасности и формалне, а не стварне људске контроле (Fitzpatrick et al., 2019; Meijer & Wessels, 2019).

8.5. Правно-етичка евалуација

Правно-етичка евалуација обухвата проверу законског основа обраде података, примену принципа минимизације података, процену ризика по приватност, ревизију приступа, проверу објашњивости и анализу могуће дискриминације (Albrecht, 2020; Gstrein et al., 2019; Vogiatzoglou, 2019). У полицијском контексту ова димензија евалуације има посебан значај, јер аналитички резултати могу утицати на распоређивање ресурса, интензитет надзора, приоритет поступања и процену ризика по лица, просторе или догађаје.

Правно-етичка евалуација треба да провери да ли се подаци користе у складу са сврхом за коју су прикупљени, да ли постоји правни основ за њихову обраду, да ли су приступи евидентирани, да ли су подаци заштићени, да ли је омогућена људска контрола и да ли су резултати модела објашњиви. Подаци који су технички доступни нису самим тим и правно оправдани за употребу у предиктивном моделу.

Резултати модела треба да буду упоредиви по подручјима и групама догађаја, али без незаконите обраде осетљивих карактеристика. То захтева пажљив дизајн улазних променљивих, контролу proxy променљивих, анализу расподеле грешака и јасно документовање ограничења модела (Oswald et al., 2018; Favaretto et al., 2019). Ако се утврди да модел систематски производи штетне разлике, потребно је кориговати податке, променљиве, правила или начин употребе резултата, а не само констатовати постојање пристрасности (Richardson et al., 2019; Alikhademi et al., 2021).

У том смислу правно-етичка евалуација није споредна провера, већ равноправан елемент процене успешности модела. Систем који је технички добар, али правно или етички неприхватљив, не може бити основа институционалне примене (Asaro, 2019; Ferguson, 2017).

Посебан значај има и питање објашњивости. Ако корисник система, надзорни орган или суд не може разумети основну логику препоруке, способност правне контроле и институционалне одговорности је озбиљно умањена (Adadi & Berrada, 2018; Grace, 2019). Зато правно-етичка евалуација мора обухватити и проверу да ли су резултати модела приказани на начин који омогућава разумевање, оспоравање, ревизију и накнадну контролу.

8.6. Друштвена евалуација и поверење јавности

Поред техничке, оперативне и правно-етичке евалуације, унапређени модел треба процењивати и са становишта његовог друштвеног утицаја. Предиктивна полицијска аналитика се примењује у области која директно утиче на безбедност, слободу, приватност и поверење грађана у институције. Због тога модел може бити технички успешан и организационо употребљив, али друштвено неприхватљив ако се доживљава као инструмент непрозирног, пристрасног или прекомерног надзора.

Друштвена евалуација треба да обухвати питања поверења јавности, транспарентности примене, пропорционалности поступања, недискриминације и јавне комуникације. Она не подразумева откривање осетљивих оперативних метода, али подразумева да институција може објаснити зашто се систем користи, у које сврхе, под којим ограничењима, ко га контролише и како се спречавају злоупотребе. На тај начин се смањује ризик да се модел доживи као непрозирна технологија која замењује људску процену.

Посебно је важно пратити да ли примена модела доводи до непропорционалног усмеравања полицијских ресурса ка одређеним просторима или групама, јер то може угрозити поверење јавности чак и када модел формално користи неосетљиве променљиве. Због тога друштвена евалуација мора бити повезана са анализом пристрасности, правно-етичком провером и евалуацијом стварних исхода.

8.7. Интегрисани евалуациони оквир

На основу наведеног, евалуација унапређеног модела треба да буде организована као интегрисани оквир који обједињује више група критеријума. Такав приступ омогућава да се избегне уско техничко тумачење успешности и да се модел процењује као целина: као аналитички, технолошки, организациони, правни и друштвени систем подршке одлучивању.

Табела 8.2. Интегрисани оквир евалуације унапређеног модела

Димензија евалуације	**Кључна питања**	**Примери показатеља**
Техничка евалуација	Да ли модел тачно, стабилно и благовремено предвиђа?	Тачност, RMSE, F1, AUC, латенција, стабилност, робусност
Оперативна евалуација	Да ли модел помаже у реалном поступању?	Време реакције, јаснoћа препоруке, употребљивост у раду, однос препоруке и одлуке
Организациона евалуација	Да ли се модел уклапа у процедуре и улоге?	Прихватање од корисника, обука, дневници употребе, јасна подела одговорности
Правно-етичка евалуација	Да ли је примена законита, пропорционална и контролисана?	Правни основ, заштита података, објашњивост, људска контрола, недискриминација
Друштвена евалуација	Да ли модел чува поверење јавности и избегава прекомерни надзор?	Транспарентност, прихватљивост, жалбе, јавна комуникација, анализа нежељених ефеката
Развојна евалуација	Да ли се модел унапређује на основу исхода?	Документоване корекције, ревизија правила, анализа грешака, ажурирање модела

Да би евалуациони оквир био применљив у будућој пилот-примени, потребно је да свака евалуациона димензија буде повезана са примерима мерљивих индикатора. Ови индикатори не морају бити коначни, јер њихов избор зависи од врсте пилот-пројекта, доступних података, правног основа и институционалних процедура. Ипак, њихово дефинисање је важно зато што омогућава да се модел не процењује само описно, већ и кроз проверљиве показатеље успешности, ризика и прихватљивости.

Табела 8.3. Примери операционализације евалуационих критеријума у будућој пилот-примени

Димензија евалуације	Пример мерљивог индикатора	Начин мерења / извор података	Сврха индикатора
Техничка евалуација	RMSE, MAE, F1, AUC, стопа лажно позитивних и лажно негативних сигнала	Резултати тестирања модела на означеним подацима или пилот-скупу	Провера тачности, стабилности и предиктивне вредности модела
Техничка евалуација	Просечна латенција обраде	Време од пријема сигнала до аналитичког излаза	Провера да ли модел може да подржи рад у реалном или скоро реалном времену
Оперативна евалуација	Време од аналитичког сигнала до оперативне реакције	Дневници система, евиденције поступања, оперативни извештаји	Процена да ли модел убрзава или рационализује поступање
Оперативна евалуација	Удео препорука које су прихваћене, одбијене или модификоване	Евиденција одлука и образложења корисника система	Процена односа између алгоритамске препоруке и људске одлуке
Организациона евалуација	Ниво прихватања модела од стране корисника	Анкете, интервјуи, фокус групе, дневници употребе	Процена употребљивости, разумљивости и организационе прихваћености
Организациона евалуација	Број потребних обука и учесталост грешака у употреби система	Евиденције обука, интерни извештаји, корисничка подршка	Процена кадровске спремности и потребе за додатним процедурама
Правно-етичка евалуација	Број случајева у којима је потребна додатна правна провера пре употребе резултата	Правне процене, записници о одобрењу, DPIA/процене утицаја	Провера законитости, пропорционалности и сврсисходности примене
Правно-етичка евалуација	Број лажно позитивних интервенција са потенцијалним утицајем на права грађана	Евиденције поступања, жалбе, накнадне провере исхода	Процена ризика од неоправданог поступања или прекомерног надзора
Друштвена евалуација	Број жалби грађана или приговора у вези са применом модела	Жалбени механизми, интерне контроле, извештаји омбудсмана или надзорних тела	Процена јавне прихватљивости и друштвеног ризика
Друштвена евалуација	Перципирана правичност и разумљивост примене модела	Анкете грађана, интервјуи, јавне консултације	Процена поверења јавности и легитимности примене
Развојна евалуација	Број документованих корекција модела након евалуације	Верзионисање модела, ревизиони извештаји, логови измена	Провера да ли модел учи из грешака и исхода
Развојна евалуација	Учесталост ревизије правила, параметара и fuzzy модула	Документација модела и записници евалуационог тима	Процена адаптивности и одрживости модела

Оваква операционализација показује да се евалуација модела не завршава мерењем предиктивне тачности. Технички успешан модел може бити неприхватљив ако производи велики број лажно позитивних сигнала, ако није разумљив корисницима, ако не постоји јасан правни основ за употребу резултата или ако изазива пад поверења јавности. Због тога се у будућој пилот-примени мора истовремено пратити технички учинак, оперативна употребљивост, правна пропорционалност, етичка прихватљивост и друштвени ефекти.

Поред појединачних индикатора, евалуација модела треба да обухвати и процену односа између техничког добитка и правно-етичког ризика. У полицијском контексту није довољно да модел буде брз или статистички тачан; потребно је проценити да ли добитак у брзини, тачности или ефикасности оправдава потенцијалне ризике по права грађана, пропорционалност поступања и поверење јавности.

Табела 8.4. Матрица односа техничког добитка и правно-етичког ризика

Технички добитак	**Правно-етички ризик**	**Евалуациона оцена**	**Препоручено поступање**
Висока тачност и ниска латенција	Низак ризик по права грађана, јасан правни основ и висока објашњивост	Повољан однос користи и ризика	Могућа контролисана пилот-примена уз редовну ревизију
Висока тачност и брза обрада	Средњи ризик због ограничене објашњивости или осетљивих података	Условно прихватљиво	Додати XAI механизме, правну проверу и људску контролу пре шире примене
Средња техничка тачност	Висок ризик од лажно позитивних интервенција или непропорционалног поступања	Неповољан однос користи и ризика	Ограничити примену на аналитичку подршку, без оперативног поступања
Висока техничка тачност	Висок ризик по приватност, недовољан правни основ или могућа дискриминација	Неприхватљиво без додатних мера	Забрана оперативне примене док се не отклоне правни и етички ризици
Ниска техничка тачност	Низак или средњи правно-етички ризик	Недовољна аналитичка вредност	Наставити развој модела, али без примене у оперативном одлучивању
Ниска техничка тачност	Висок правно-етички ризик	Неприхватљиво	Обуставити примену и редизајнирати модел

Ова матрица указује на то да технички добитак сам по себи не може бити довољан услов за примену модела. Уколико је правно-етички ризик висок, чак и технички успешан модел мора бити ограничен, редизајниран или искључен из оперативне примене. Насупрот томе, модел са умереним техничким резултатима може имати вредност у аналитичкој подршци, али не и као основ за непосредно полицијско поступање. Због тога се предложени модел у овој дисертацији посматра као систем подршке одлучивању, а не као механизам аутоматизованог одлучивања.

Интегрисани евалуациони оквир омогућава да се резултати прототипа тумаче у ширем институционалном и друштвеном контексту. Модел који има високу техничку тачност, али ниску објашњивост, слаб ниво прихватања од корисника или нејасан правни основ, не може се сматрати потпуно успешним. Слично томе, модел који је оперативно користан, али производи висок број лажно позитивних сигнала или изазива пад поверења јавности, не може бити препоручен за широку примену. Због тога одговорна примена предиктивне полицијске аналитике захтева да се технички учинак модела стално доводи у везу са оперативном употребљивошћу, правном пропорционалношћу, етичком прихватљивошћу и друштвеним ефектима.

8.8. Провера истраживачких хипотеза кроз евалуациони оквир

У оквиру интегрисаног евалуационог оквира потребно је посебно назначити да истраживачке хипотезе немају исту методолошку природу, нити исти ниво емпиријске потврђености. X1 и X2 имају превасходно архитектонско-аналитички карактер и делимично се поткрепљују кроз студију случаја засновану на PIoT приступу. X3 и X4 имају евалуационо-нормативни и институционални карактер, због чега се не могу проверити искључиво квантитативним тестирањем, већ се разматрају кроз анализу литературе, правно-етичке принципе, критеријуме људске контроле и услове институционалне примене. Табела 8.5 приказује начин на који су хипотезе повезане са методом провере и нивоом поткрепљености у оквиру ове дисертације.

Табела 8.5. Начин провере истраживачких хипотеза и ниво поткрепљености

Хипотеза	Тип хипотезе	Метод провере у дисертацији	Ниво поткрепљености
X1: хијерархијски организована вертикална PIoT архитектура представља погодан оквир за превенцију, рано откривање и подршку одлучивању у интелигентном граду.	Архитектонска и концептуално-моделска хипотеза	Концептуално моделирање, анализа edge–fog–cloud архитектуре, приказ вертикалног тока података и студија случаја заснована на PIoT приступу.	Делимично емпиријски поткрепљена кроз доказ концепта (proof of concept) студију случаја; захтева даљу проверу у реалном полицијском пилот-окружењу.
X2: интеграција модела машинског учења и fuzzy логике у оквиру PIoT архитектуре може унапредити краткорочну предикцију и подршку одлучивању у сложеним безбедносним сценаријима.	Аналитичка и техничко-евалуациона хипотеза	Анализа примене RNN, LSTM и GRU модела за краткорочно предвиђање, као и fuzzy модула за подршку одлучивању у условима неизвесности.	Делимично емпиријски поткрепљена на ограниченом сценарију; потребна је провера на већем броју безбедносно релевантних случајева.
X3: успешност предиктивне аналитике у безбедносном систему не може се процењивати само на основу предиктивне тачности, већ мора обухватити и квалитет података, организациону употребљивост, објашњивост, правну пропорционалност и контролу пристрасности.	Евалуационо-нормативна хипотеза	Анализа литературе, анализа ризика, правно-етичка евалуација, разматрање критеријума квалитета података, објашњивости, пристрасности и организационе применљивости.	Теоријски и нормативно оправдана; захтева будућу институционалну проверу кроз пилот-примену и вишекритеријумску евалуацију.
X4: унапређени модел може бити институционално одржив само ако је развијен као систем подршке одлучивању са јасно дефинисаном људском контролом.	Институционална, правно-етичка и нормативна хипотеза	Анализа принципа људске контроле, одговорности, забране потпуно аутоматизованог полицијског одлучивања, правне пропорционалности и етичке прихватљивости.	Нормативно и институционално оправдана; није потпуно емпиријски проверена без реалног полицијског пилота.

Овако постављена провера хипотеза показује да дисертација не тврди да је предложени модел у потпуности емпиријски валидиран у реалном полицијском систему. Њен допринос је у развоју концептуално, архитектонски и методолошки утемељеног модела, као и у потврди појединих архитектонских и аналитичких елемената кроз доказ концепта. Потпуна

провера применљивости модела захтева даљу пилот-примену у контролисаном институционалном окружењу.

8.9. Унапређење прототипа

Евалуација није завршни корак, већ механизам учења и унапређења. Након сваког циклуса тестирања прототип се дорађује: чисте се подаци, мењају параметри, додају или уклањају променљиве, ревидирају fuzzy правила, прилагођавају визуелизације, ажурирају процедуре и унапређују механизми људске контроле. Ово је у складу са итеративним приступом развоју аналитичких система и design science логиком истраживачких решења (Hevner et al., 2004; Meijer et al., 2021).

Посебно је важно документовати све промене, јер само документован модел може бити предмет научне провере, репликације и институционалне одговорности (Bennett Moses & Chan, 2018; Oswald et al., 2018). Документација треба да обухвати изворе података, промене у параметрима, измене правила, резултате тестирања, разлоге за корекције и ефекте након измена.

На тај начин евалуација постаје интегрални део животног циклуса модела, а не једнократна фаза након развоја. То је нарочито важно у домену полицијске аналитике, где се окружење, обрасци ризика, извори података, технолошки услови и нормативни захтеви временом мењају (Mugari & Obioha, 2021; Ferguson, 2020).

8.10. Закључна разматрања поглавља

У овом поглављу дефинисан је оквир за евалуацију унапређеног модела за превенцију и рано откривање илегалних активности. Полазиште је да успешност модела не може бити сведена само на предиктивну тачност, већ мора бити процењена кроз више повезаних димензија: техничку, оперативну, организациону, правно-етичку, друштвену и развојну.

Техничка евалуација омогућава проверу тачности, стабилности и робусности аналитичких модула. Оперативна и организациона евалуација показују да ли модел заиста помаже у реалном раду и да ли се уклапа у институционалне процедуре. Правно-етичка евалуација обезбеђује да модел буде законит, објашњив, пропорционалан и контролисан. Друштвена евалуација указује на значај поверења јавности, недискриминације и избегавања

прекомерног надзора. Развојна евалуација омогућава да се модел континуирано унапређује на основу исхода, грешака и промена у окружењу.

Овако постављена евалуација директно је повезана са главним доприносом дисертације. Унапређени модел није само технички систем за предвиђање, већ контролисан, објашњив, евалуабилан и правно-етички утемељен систем подршке одлучивању. Само ако се његова успешност проверава на овај начин, могуће је проценити да ли модел заиста доприноси превенцији и раном откривању илегалних активности, уз очување законитости, пропорционалности и поверења јавности.

9. Студија случаја: примена PIoT модела у паметном граду

9.1. Улога студије случаја у валидацији унапређеног модела

У претходним поглављима развијен је унапређени модел за превенцију и рано откривање илегалних активности применом предиктивне аналитике. Модел је постављен као хијерархијски, интероперабилан, објашњив, евалуабилан и људски контролисан систем подршке одлучивању. Да би се показало да такав модел није само теоријски конструкт, у овом поглављу као студија случаја користи се објављени рад *Data-Driven Police IoT in Smart Cities: A Sustainable Hierarchical Framework for Traffic Prediction and Policing Decisions*, објављен 2026. године у часопису *Sustainability* (Dragović et al., 2026).

Овај рад је посебно значајан за дисертацију јер у конкретном истраживачком контексту операционализује више кључних елемената унапређеног модела: *Police Internet of Things* (PIoT) архитектуру, edge–fog–cloud хијерархију, вертикални ток података, краткорочно предвиђање применом модела временских серија и fuzzy подршку одлучивању у условима неизвесности. На тај начин овај рад не представља само пратећи научни резултат, већ и емпиријску и визуелну потврду централне логике дисертације.

Студија случаја у овом поглављу има статус доказа концепта, односно proof of concept, за поједине архитектонске и аналитичке елементе унапређеног модела. Она не представља потпуну емпиријску валидацију целог хијерархијског система за превенцију и рано откривање свих облика илегалних активности. Из објављеног рада преузимају се и у дисертацији адаптирају елементи који се односе на PIoT архитектуру, вертикални ток података, предвиђање саобраћајног тока и fuzzy подршку одлучивању. Дисертација те елементе поставља у шири модел предиктивне полицијске аналитике, повезује их са претходно разматраним предусловима, ризицима, правно-етичким ограничењима, људском контролом и евалуационим критеријумима, и тиме проширује њихову улогу са техничке демонстрације на део интегрисаног аналитичко-оперативног оквира.

Из перспективе ове дисертације, наведени рад потврђује две кључне тезе:

- Прва је архитектонска теза: вертикална PIoT архитектура омогућава јасно раздвајање оперативних, тактичких и стратешких функција кроз edge, fog и cloud нивое.
- Друга је аналитичка теза: различити аналитички модели могу бити распоређени на различите нивое хијерархије у складу са временским захтевима, расположивим подацима, капацитетима обраде и врстом одлуке коју треба подржати.

У том смислу, објављени рад представља студију случаја која показује како се општи модел предложен у дисертацији може технички, аналитички и организационо операционализовати.

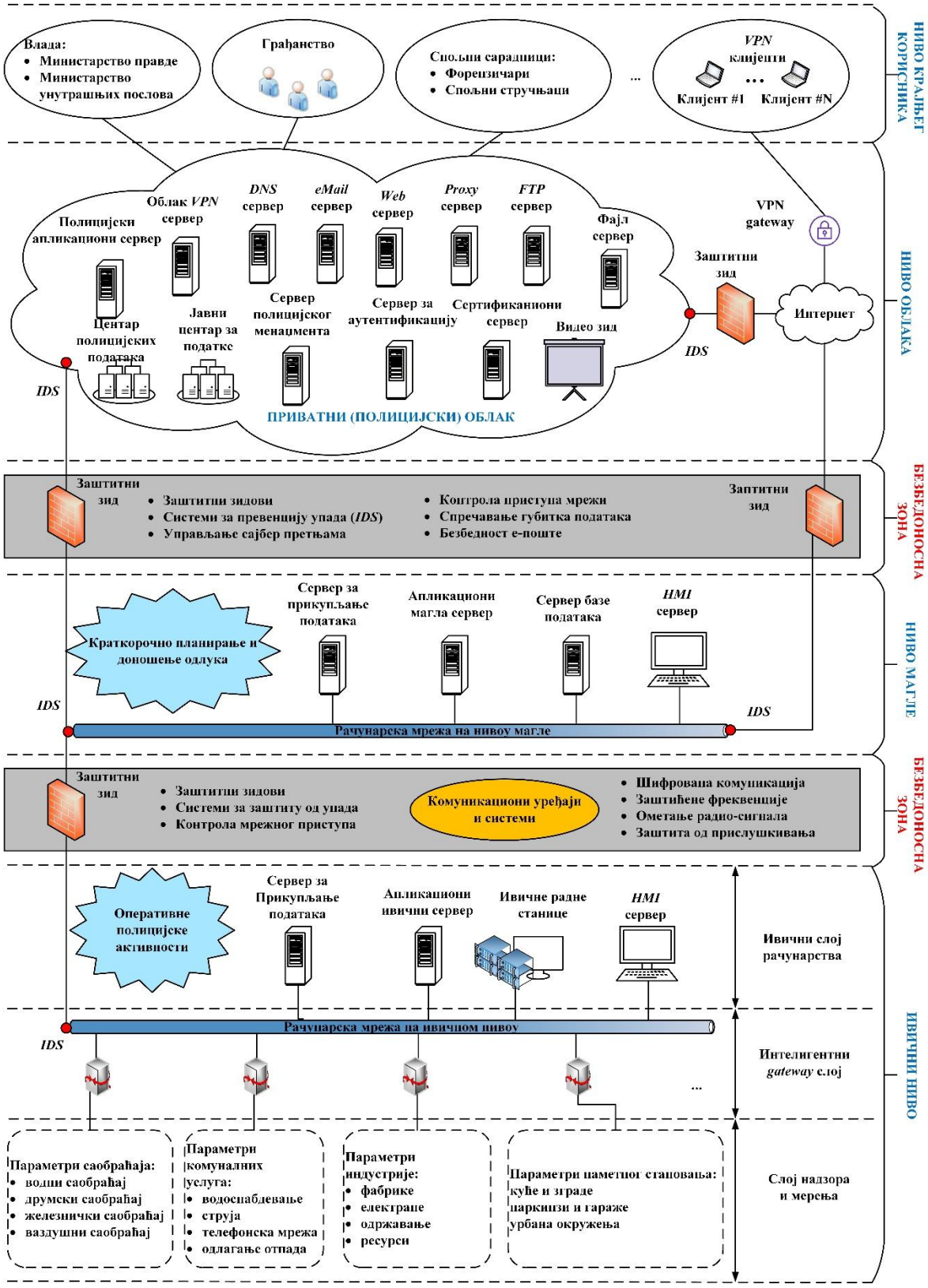
Важно је нагласити да предвиђање саобраћајног тока у овој студији случаја не представља директну предикцију криминалитета, нити доказ да се само на основу саобраћајних података могу предвиђати илегалне активности. Саобраћајни ток се у овом раду посматра као један од урбаних динамичких сигнала који у PIoT окружењу може имати индиректну аналитичку вредност. Његова вредност постаје безбедносно релевантна тек када се повеже са другим подацима, као што су локације јавних догађаја, позиви грађана, полицијске евиденције, сензорски подаци, геопросторни обрасци, подаци о критичној инфраструктури и оперативна сазнања. У том смислу, студија случаја не доказује директну везу између саобраћајног тока и криминалитета, већ показује како PIoT архитектура може да подржи прикупљање, обраду, предикцију и коришћење урбаних података у ширем систему процене безбедносног ризика.

9.2. Архитектонска основа студије случаја: вертикални PIoT модел

Полазиште студије случаја јесте да се полицијски рад у паметном граду више не може посматрати искључиво кроз класичне, реактивне и централистичке обрасце поступања. Паметни градови производе велике количине података из сензора, камера, саобраћајних система, комуникационих мрежа, паметне инфраструктуре, јавних сервиса и дигиталног окружења. Такво окружење истовремено отвара нове могућности за превенцију и рано откривање ризика, али и нове безбедносне изазове на граници физичког и сајбер простора.

Због тога објављени рад предлаже вертикални PIoT концепт, заснован на три хијерархијска нивоа: edge, fog и cloud (слика 9.2.1). Edge ниво је најближи изворима података и омогућава локалну обраду, брзу детекцију и иницијалну реакцију. Fog ниво омогућава агрегацију података, локалну аналитику, краткорочно предвиђање и тактичку координацију. Cloud ниво омогућава дугорочну интеграцију података, сложенију аналитику, fuzzy одлучивање, стратешко планирање и управљање ризиком.

У односу на равне IoT концепте, вертикални PIoT модел има посебну предност јер омогућава функционално раздвајање различитих врста обраде и одлучивања. Брзе, временски осетљиве активности остају ближе извору података, док се сложеније анализе, процена ризика и институционално осетљиве одлуке смештају на више нивое система. Ово је у складу са логиком унапређеног модела у овој дисертацији, у коме се оперативно, тактичко и стратешко одлучивање не смеју мешати, већ морају бити повезани кроз контролисан вертикални ток података.



Слика 9.2.1. Вертикални PIoT концепт са edge, fog и cloud нивоима (Dragović et al., 2026).

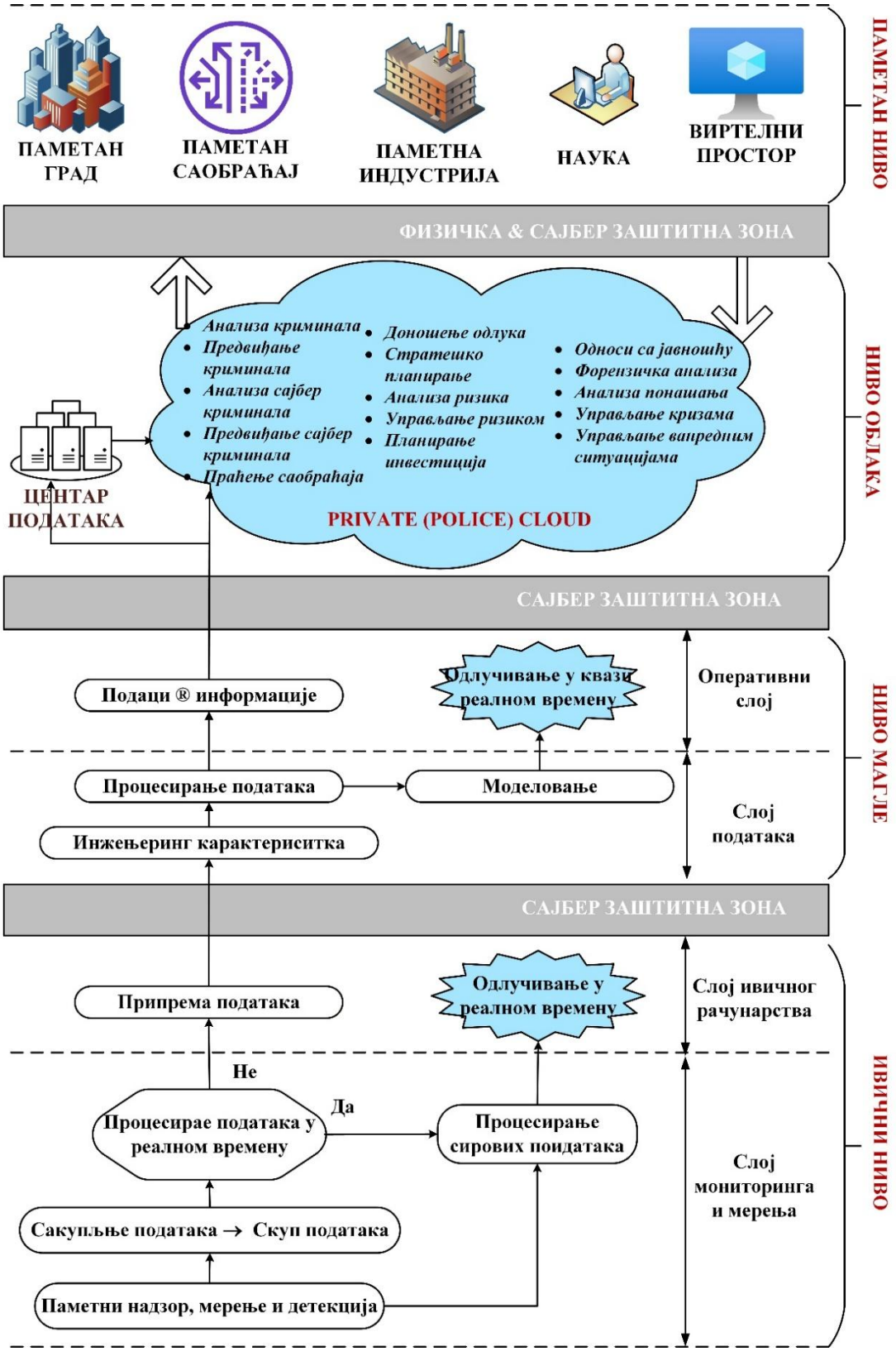
9.3. Вертикални ток података и мапирање функција по нивоима

Поред саме архитектуре, објављени рад посебно приказује вертикални ток података кроз PIoT систем. Тај ток не представља само техничку комуникацију између уређаја, већ процес постепеног претварања сирових података у информације, предикције, препоруке и одлуке. На тај начин вертикални ток података представља методолошку везу између инфраструктуре и аналитичког модела.

У студији случаја подаци се крећу од monitoring и sensing слоја, преко edge обраде, припреме података, *feature engineering*-а и моделирања, до cloud нивоа на коме се врше сложене анализе, стратешко планирање, процена ризика и подршка одлучивању. Тај ток омогућава да се подаци из различитих извора не посматрају изоловано, већ као делови јединственог хијерархијског система који повезује физички и сајбер простор паметног града.

Док слика 9.2.1 приказује општу архитектонску структуру PIoT модела, слика 9.3.1 детаљније приказује вертикални ток података и функционално мапирање процеса по нивоима. На доњем нивоу налазе се активности паметног праћења, сензорског регистровања и мерења, затим следе обрада сирових података, припрема података, *feature engineering* и моделирање. На fog нивоу подаци се трансформишу у информације погодне за квази-реално одлучивање, док cloud ниво омогућава стратешку анализу, анализу ризика, управљање кризама, односе с јавношћу, форензичку анализу и друге сложеније функције.

Овај приказ је важан из два разлога. Прво, он показује да се унапређени модел не заснива на неконтролисаном прикупљању свих доступних података, већ на структурисаном току у коме сваки ниво има јасно дефинисану функцију. Друго, он потврђује да су предикција и одлучивање део истог управљачког процеса: подаци се прикупљају на нижим нивоима, али се њихова вредност у потпуности остварује тек кроз обраду, моделирање, тумачење и примену у процесу одлучивања.

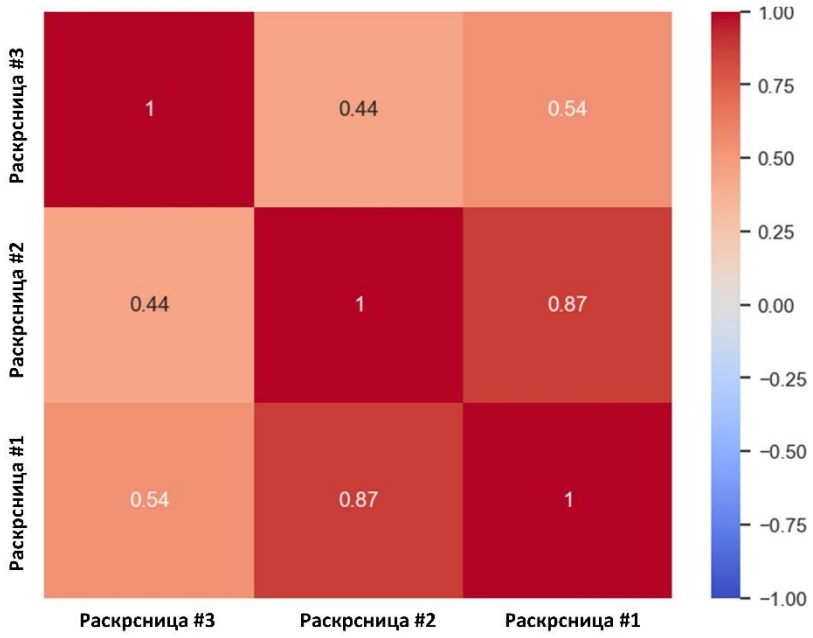


Слика 9.3.1. Вертикални ток података у PIoT окружењу (Dragović et al., 2026).

9.4. Студија случаја 1: предвиђање саобраћајног тока на fog нивоу

Прва студија случаја у објављеном раду односи се на краткорочно предвиђање саобраћајног тока на три блиске раскрснице. Подаци су прикупљани током четири године помоћу детектора возила и саобраћајних камера на edge нивоу. Ови подаци су затим обрађени на fog нивоу, где су спроведени exploratory data analysis, формирање универијантних временских серија, нормализација, подела на тренинг и тест скупове и креирање sliding window структура погодних за рекурентне моделе.

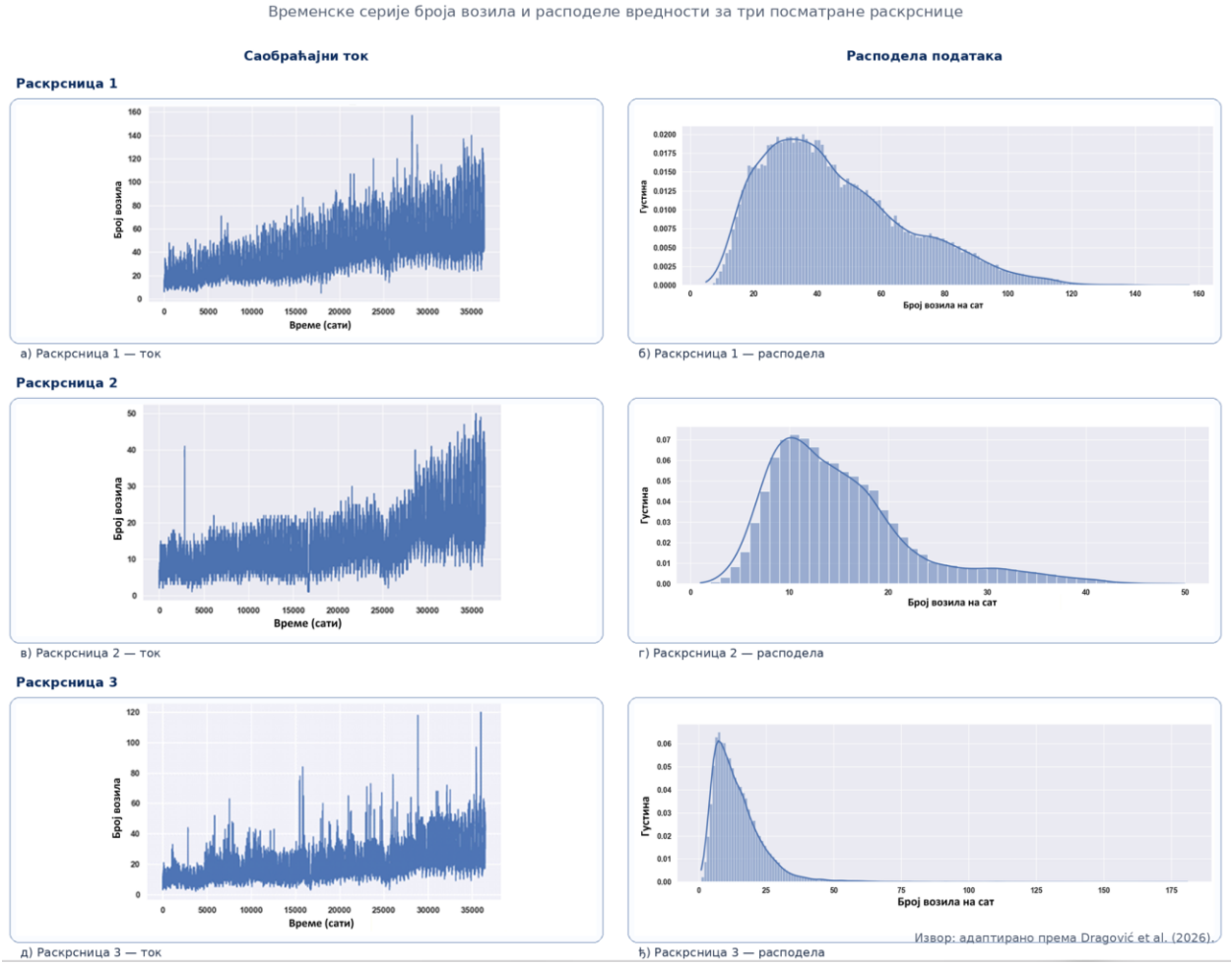
Иако је предмет ове студије случаја саобраћајни ток, њен значај за дисертацију је шири. Саобраћај у паметном граду није само инфраструктурно питање, већ и безбедносно релевантан индикатор. Нагле промене у саобраћајном току могу указивати на инциденте, блокаде, масовна окупљања, кризне ситуације, промену урбане динамике или потребу за другачијим распоређивањем полицијских ресурса. Због тога је предвиђање саобраћајног тока погодан пример за демонстрацију како PIoT систем може да подржи рано уочавање ризика и тактичко планирање.



Слика 9.4.1. Корелациона структура саобраћајних токова на посматраним раскрсницама.

Поред појединачних серија, илустрованих на слици 9.4.2. рад користи и корелациону матрицу, односно heatmap приказ односа између временских серија (Слика 9.4.1). Овај

приказ је важан јер показује да раскрснице нису потпуно изоловане јединице, већ делови локалне саобраћајне мреже. Управо то оправдава PIoT приступ: уместо да се свака камера или свака раскрсница посматра као засебан уређај, систем их третира као повезане изворе података унутар ширег smart city окружења.



Слика 9.4.2. Саобраћајни токови и расподеле по раскрсницама у студији случаја (Dragović et al., 2026).

Слика 9.4.2 приказује временске серије саобраћајног тока и расподеле броја возила за три посматране раскрснице у студији случаја. Временске серије омогућавају увид у динамику, трендове, варијабилност и екстремне вредности у саобраћајним подацима, док расподеле показују структуру и учесталост појединих вредности броја возила. Ови прикази су значајни јер показују да свака раскрсница има специфичну динамику, па избор предиктивног модела мора бити емпиријски проверен, а не унапред претпостављен.

9.5. Резултати предиктивних модела RNN, LSTM и GRU

У аналитичком делу прве студије случаја коришћени су RNN, LSTM и GRU модели, имплементирани у TensorFlow/Keras окружењу. Сви модели су тестирани у упоредивом експерименталном оквиру, са циљем да се провери који модел даје најбоље резултате за сваку од посматраних раскрсница. Овај приступ је важан јер показује да се избор модела не сме заснивати на претпоставци да је један алгоритам увек најбољи, већ на емпиријској провери у конкретном контексту.

RNN, LSTM и GRU припадају породици рекурентних неуронских мрежа погодних за анализу временских серија. RNN омогућава основно моделирање секвенцијалних зависности, али има ограничења у учењу дугорочних зависности. LSTM уводи меморијске механизме и додатне капије, што повећава способност учења сложенијих образаца, али и број параметара. GRU представља компромисно решење, са мањом сложеношћу од LSTM модела и често повољнијим односом између тачности и рачунарске ефикасности.

Табела 9.1. Структура и сложеност RNN, LSTM и GRU модела у студији случаја Извор: адаптирано према Dragović et al. (2026).

Модел	**Улога у студији случаја**	**Карактеристике**	**Значај за PIoT примену**
RNN	Основни рекурентни модел	Једноставнија структура, мањи број параметара	Погодан као базни модел за поређење
LSTM	Модел са меморијским механизмом	Већа способност учења сложених временских зависности, већи број параметара	Погодан када серија има израженије временске зависности
GRU	Компромис између једноставности и меморије	Мање параметара од LSTM, често бржи тренинг	Погодан за fog примену када су важни тачност и рачунарска ефикасност

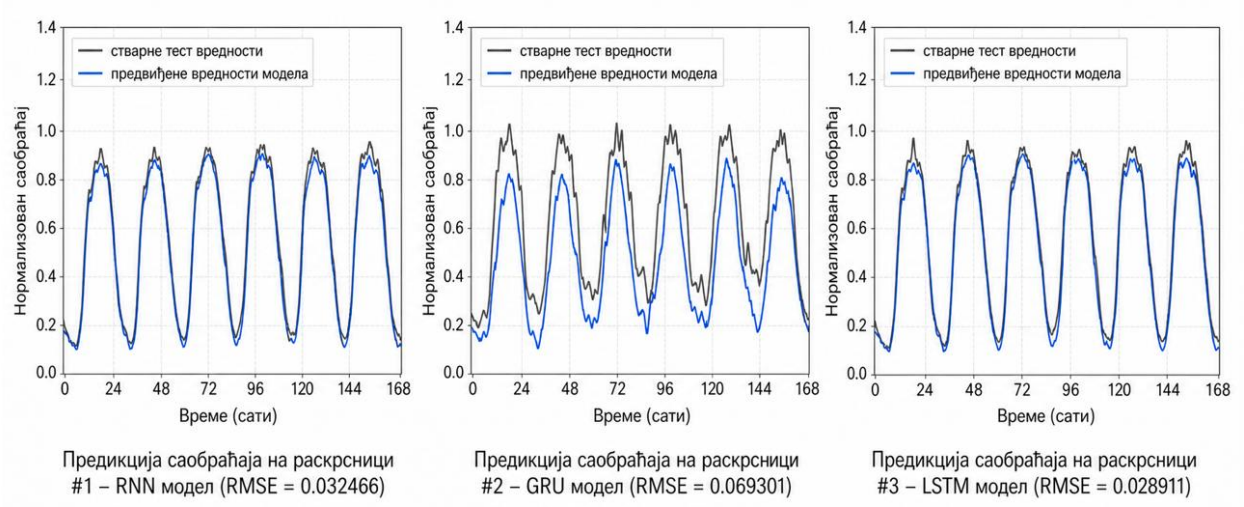
Резултати показују да се најбољи модел не појављује нужно у истом облику за све раскрснице. То је методолошки важан налаз, јер потврђује да унапређени модел не треба да прописује један универзални алгоритам, већ да омогући тестирање, поређење и избор модела у складу са карактеристикама конкретног скупа података.

Табела 9.2. Најбољи резултати модела временских серија по раскрсници

Посматрана раскрсница	Најбољи модел	MAE	MSE	RMSE	R^2	MAPE (%)	Интерпретација
Раскрсница 1	RNN	0.024589	0.001054	0.032466	0.964056	6.198616	На овој раскрсници најбољи резултат даје једноставнији RNN модел, што указује да структура серије не захтева сложенију меморијску архитектуру.
Раскрсница 2	GRU	0.054249	0.004803	0.069301	0.859426	10.089411	GRU даје најбољи резултат за ову раскрсницу и представља повољан однос између тачности и сложености модела.
Раскрсница 3	LSTM	0.021822	0.000836	0.028911	0.925654	8.825509	LSTM даје најбољи резултат за ову раскрсницу, што указује да меморијска структура модела боље хвата временске зависности у овој серији.

Табела 9.2 приказује најбоље моделе за сваку од три посматране раскрснице, на основу најниже RMSE вредности. Резултати показују да не постоји један универзално најбољи модел за све временске серије. За Раскрсницу 1 најбољи резултат даје RNN модел, за Раскрсницу 2 GRU модел, док за Раскрсницу 3 најбољи резултат даје LSTM модел. Овај налаз је важан јер потврђује да избор предиктивног модела мора зависити од структуре конкретних података, а не од унапред претпостављене супериорности одређене архитектуре.

Посматрано по свим моделима и раскрсницама, најнижу RMSE вредност има LSTM модел за Раскрсницу 3 (RMSE = 0.028911), док највећи R^2 има RNN модел за Раскрсницу 1 (R^2 = 0.964056). То показује да избор „најбољег“ модела може зависити од метрике која се узима као примарна, због чега је у раду оправдано приказати више комплементарних метрика.



Слика 9.5.1. Поређење стварних и предвиђених вредности саобраћајног тока (Dragović et al., 2026).

Слика 9.5.1. приказује поређење стварних и предвиђених вредности саобраћајног тока за три посматране раскрснице. За сваку раскрсницу приказан је модел који је у датој серији остварио најнижу RMSE вредност: RNN за раскрсницу 1, GRU за раскрсницу 2 и LSTM за раскрсницу 3. За дисертацију овај приказ има двоструку вредност. Прво, показује да се модели временских серија могу оперативно применити на fog нивоу PIoT архитектуре. Друго, показује да евалуација модела мора бити и визуелна и статистичка: није довољно приказати само RMSE или другу нумеричку метрику, већ је потребно проверити како се предвиђене вредности понашају у односу на стварне вредности кроз време.

На основу ових резултата може се закључити да fog ниво има значајну улогу у краткорочној предиктивној аналитици. Он није само комуникациони посредник између edge и cloud нивоа, већ активан аналитички слој који може да извршава моделе временских серија, процењује краткорочне ризике и обезбеди улаз за тактичко одлучивање.

9.6. Студија случаја 2: fuzzy подршка одлучивању на cloud нивоу

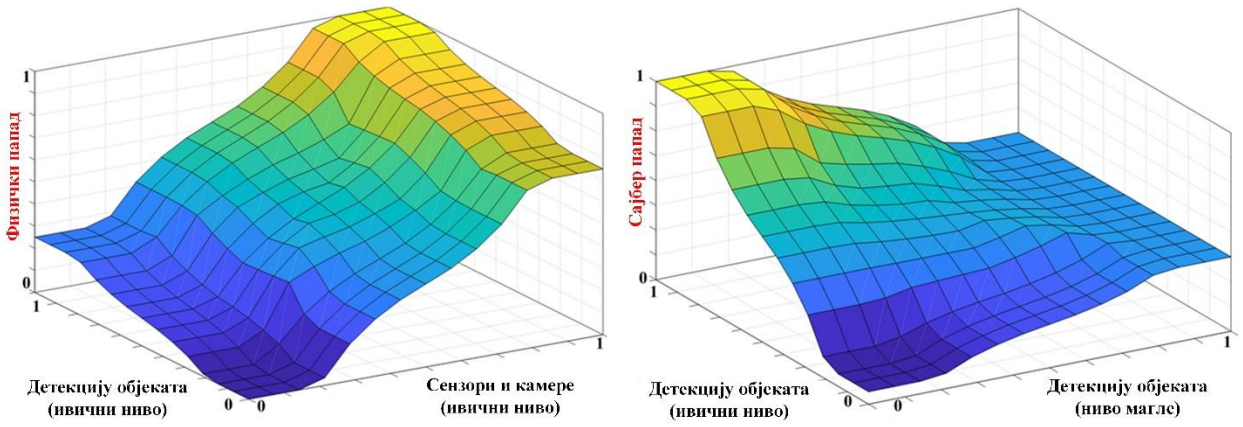
Друга студија случаја има другачију функцију од прве. Док прва показује како се на fog нивоу може вршити краткорочно предвиђање, друга показује како се на cloud нивоу може организовати подршка одлучивању у условима неизвесности. Полазни сценарио односи се на заштићени објекат чији су сензори, камере и системи надзора повезани са PIoT архитектуром. Потребно је проценити да ли је у питању стварни физички упад, непозната ситуација или лажни сигнал изазван сајбер-нападом.

За ту сврху у раду је примењен Sugeno type-1 fuzzy inference system. Улазне променљиве одражавају сигнале са различитих нивоа архитектуре: сензоре и камере на edge нивоу, објектну детекцију, праћење на fog нивоу и излазне категорије које се односе на тип напада. На тај начин fuzzy модел повезује више извора података и омогућава да се неизвесност не сведе на бинарну одлуку.

Табела 9.3. Променљиве и лингвистичке вредности fuzzy модела у студији случаја Извор: адаптирано према Dragović et al. (2026).

Елемент система	**Ниво PIoT архитектуре**	**Пример улазне или излазне вредности**	**Улога у одлучивању**
Сензори и камере	Edge	no / motion	Региструју иницијални сигнал у физичком простору
Object detection алгоритам	Edge	no / detection	Проверава постојање објекта или кретања
Object tracking алгоритам	Fog	no / tracking	Утврђује да ли се сигнал наставља и прати кроз време
Тип напада	Cloud	no attack / unknown / physical / cyber	Даје структурирану процену сценарија

Оваква структура показује да fuzzy модул не доноси коначну одлуку уместо човека, већ формализује степен припадности различитим сценаријима. То је у складу са логиком унапређеног модела у овој дисертацији: систем може помоћи у структурирању ризика, али коначна одлука мора остати у домену људске процене, правне одговорности и институционалне контроле.



Слика 9.6.1. Fuzzy подршка одлучивању у разликовању физичког и сајбер-инцидента (Dragović et al., 2026).

Слика 9.6.1. приказује 3D површине fuzzy одлучивања које показују однос између параметара са edge и fog нивоа и процене типа инцидента. Лева површина односи се на процену физичког напада, док десна површина приказује процену сајбер-инцидента. Приказ је значајан јер показује да fuzzy модел може да структурира одлучивање у условима неизвесности и конфликтних сигнала, али да резултат остаје подршка људској процени, а не аутоматска одлука.

Ова студија случаја директно подржава тврдњу да унапређени модел треба да комбинује предиктивну аналитику и подршку одлучивању. У реалним безбедносним ситуацијама проблем није увек у томе да се предвиди број догађаја, већ да се у условима непотпуних и конфликтних сигнала донесе пропорционална и проверљива одлука. Fuzzy приступ омогућава да се тај процес структурира, али без замене људске контроле.

9.7. Веза студије случаја са прототипом

Вредност студије случаја огледа се у томе што она није изоловани експеримент, већ емпиријска потврда више компоненти прототипа развијеног у поглављу 7. У дисертацији је прототип постављен као интегрисани систем који обухвата изворе података, вертикалну PIoT архитектуру, аналитичке модуле, fuzzy/XAI подршку, људску контролу и

континуирано учење. Објављени рад показује како се ови елементи могу практично повезати.

Табела 9.4. Мапирање елемената студије случаја на компоненте прототипа дисертације

Компонента прототипа из дисертације	**Потврда у студији случаја**	**Значај за модел**
Вертикална PIoT архитектура	Приказ edge, fog и cloud нивоа	Потврђује хијерархијску организацију модела
Вертикални ток података	Collecting → processing → computing → decision-making	Показује како се подаци трансформишу у одлуке
Edge ниво	Камере, сензори, vehicle detectors, object detection	Потврђује локалну детекцију и брзу обраду
Fog ниво	EDA, временске серије, RNN/LSTM/GRU модели	Потврђује тактичку предиктивну аналитику
Cloud ниво	Sugeno fuzzy inference system	Потврђује сложенију подршку одлучивању
Објашњивост и контрола	Fuzzy правила и 3D површине одлучивања	Показује могућност тумачења резултата
Евалуација	Метрике предвиђања и поређење модела	Потврђује потребу за емпиријском провером
Ограничења примене	Саобраћајни и моделовани безбедносни сценарио	Показује границе, али и преносивост модела

Ова табела показује да студија случаја не потврђује само један део дисертације, већ практично целокупну логику унапређеног модела. Она показује да се подаци могу прикупљати на edge нивоу, обрађивати и предвиђати на fog нивоу, а користити за сложенију подршку одлучивању на cloud нивоу. Истовремено, студија показује да модел мора бити евалуиран, упоредив, визуелно проверљив и прилагођен конкретном контексту.

9.8. Ограничења студије случаја и могућности проширења

Иако објављени рад има значајну вредност као студија **случаја**, потребно је јасно назначити његова ограничења. Прва студија случаја односи се на саобраћајни ток, а не директно на класични криминалитет. Њена вредност за дисертацију зато није у доказивању да се сви облици илегалних активности могу предвиђати на исти начин, већ у потврди да вертикална

PIoT архитектура и аналитика на fog нивоу могу подржати краткорочно предвиђање у окружењу паметног града.

Друго ограничење односи се на fuzzy студију случаја. Она је ближа безбедносној проблематици, јер разматра физички упад и сајбер-инцидент, али је ипак реч о моделованом сценарију. Због тога је потребна даља емпиријска провера на већем броју реалних или реалистично симулираних безбедносних сценарија. Ипак, њена вредност је у томе што показује како се fuzzy правила могу користити за структурирање одлучивања у условима неизвесности, што је једна од кључних функција унапређеног модела.

Треће, резултати студије случаја не доказују универзалну супериорност једног модела, нити апсолутну предност вертикалног PIoT приступа у свим условима. Они пре показују да овај приступ има јасну методолошку и практичну вредност: омогућава расподелу функција по нивоима, смањује кашњење, подржава краткорочну предикцију и омогућава структурирано одлучивање у сложеним сценаријима.

Четврто, саобраћајни подаци представљају индиректан урбани сигнал, а не директан индикатор илегалних активности. Због тога би наредна фаза истраживања морала да укључи интеграцију са полицијским евиденцијама, подацима о инцидентима, подацима о јавним догађајима и другим безбедносно релевантним изворима, како би се испитала стварна вредност саобраћајних и сензорских параметара у процени ризика од илегалних активности.

Посебно треба нагласити да студија случаја не мери директне криминално-безбедносне исходе, као што су смањење броја одређених врста инцидената, спречавање конкретних илегалних активности, повећање стопе откривања или побољшање ефикасности полицијских интервенција у реалном окружењу. Ти исходи у овој фази остају у домену потенцијалних ефеката предложеног модела, а не емпиријски измерених резултата. Да би се они проверили, потребна је будућа пилот-примена у реалном или контролисано симулираном полицијском окружењу, са унапред дефинисаним индикаторима исхода, контролним периодом и јасним критеријумима евалуације.

Посебан правац будуће провере односи се на доменску трансферабилност модела, односно на питање у којој мери се логика краткорочног предвиђања, развијена на примеру

саобраћајног тока, може применити на конкретне криминално-безбедносне појаве. У будућим пилот-истраживањима то би могло да обухвати, на пример, предвиђање просторних и временских жаришта џепних крађа у зонама јавног превоза и масовних окупљања, процену ризика од вандализма у деловима града са високом ноћном фреквенцијом кретања, или рано откривање образаца нарушавања јавног реда у близини критичне инфраструктуре, школа, спортских објеката или великих јавних догађаја. У таквим применама саобраћајни и сензорски подаци не би били самостални предиктори криминалитета, већ део ширег скупа података који укључује полицијске евиденције, позиве грађана, геопросторне карактеристике, временске услове, календар јавних догађаја и оперативна сазнања.

Ограничења студије случаја истовремено отварају простор за даљи развој. У будућим истраживањима PIoT оквир може бити проширен од саобраћајних података ка другим облицима безбедносног ризика, уз интеграцију полицијских евиденција, позива грађана, података о јавним догађајима, геопросторних карактеристика, сензорских података и оперативних сазнања. Такође, fuzzy модул може бити проширен са једноставнијих type-1 fuzzy модела на сложеније приступе, уколико постоје подаци, експертска правила и институционални разлози за такву сложеност.

9.9. Закључна разматрања поглавља

Представљени рад Dragović et al. (2026) може се оправдано третирати као студија случаја у овој дисертацији, јер повезује концептуални модел, архитектуру система, вертикални ток података, алгоритамску примену и емпиријску евалуацију. Његов највећи допринос није само у томе што показује да су RNN, LSTM, GRU и fuzzy модели применљиви у PIoT окружењу, већ у томе што показује како се различите аналитичке функције могу распоредити по хијерархијским нивоима у складу са временским захтевима, капацитетима обраде и управљачком логиком паметног полицијског рада.

Из угла дисертације, ова студија случаја има улогу моста између теоријски развијеног прототипа и његове практичне примене. Она показује да предложени приступ није само нормативно и концептуално замишљен, већ и технички операционализован на начин који омогућава даљу научну проверу, проширење и институционалну примену.

Најважнији закључак овог поглавља јесте да PIoT модел има вредност онда када повезује три функције: прикупљање и обраду података, предиктивну аналитику и подршку одлучивању. У том смислу, студија случаја потврђује основну тезу дисертације: унапређење модела за превенцију и рано откривање илегалних активности не постиже се само избором бољег алгоритма, већ изградњом интегрисаног, хијерархијског, евалуабилног и људски контролисаног аналитичко-оперативног система.

10. ЗАКЉУЧАК

10.1. Синтеза резултата

Полазна идеја овог истраживања била је да предиктивна полицијска аналитика не треба да буде сведена на изолован алгоритам за означавање ризичних места, лица или догађаја, већ да је треба разумети као интегрисани систем који повезује податке, аналитичке методе, технолошку инфраструктуру, институционалне процедуре и контролисано доношење одлука (Perry et al., 2013; Meijer & Wessels, 2019; Bennett Moses & Chan, 2018). У том смислу, унапређење предложеног модела огледа се у померању тежишта са једноставног предвиђања ка целокупном циклусу деловања: прикупљању и интеграцији података, њиховој припреми, предикцији, подршци одлучивању, интервенцији, евалуацији исхода и организационом учењу (Meijer et al., 2021; Oatley, 2021).

Кључни резултат рада јесте постављање вертикалне архитектуре Police Internet of Things (PIoT) као носећег инфраструктурног оквира за превенцију и рано откривање илегалних активности у интелигентном граду. Та архитектура омогућава функционално раздвајање оперативних, тактичких и стратешких нивоа обраде, тако да edge ниво обезбеђује брзу локалну детекцију и иницијалну обраду података, fog ниво краткорочно предвиђање, координацију и анализу временски осетљивих сигнала, а cloud ниво сложенију аналитику, fuzzy подршку одлучивању и дугорочно планирање (Dragović et al., 2026; Mohamed et al., 2021; Songhorabadi et al., 2023).

Истраживање је показало да суштина унапређења није у аутоматизацији полицијске процене, већ у изградњи система који омогућава бољу ситуациону свест, бржу аналитичку обраду, доследније институционално поступање и проверљивију подршку одлучивању (Oswald et al., 2018; Joh, 2020; Asaro, 2019). На тај начин предложени модел треба разумети као систем подршке одлучивању у коме подаци и аналитички модели унапређују квалитет процене ризика, али не преузимају улогу човека као носиоца коначне одговорности.

10.2. Разматрање истраживачких хипотеза

Подршка истраживачким хипотезама у овом раду заснива се на теоријској анализи литературе, концептуалном развоју унапређеног модела и анализи објављене PIoT студије случаја, у којој су тестирани кључни архитектонски и аналитички елементи предложеног приступа. Добијени налази не представљају коначну и универзалну потврду модела у свим доменима безбедности, али представљају значајну основу за процену његове функционалне изводљивости, методолошке оправданости и применљивости у окружењу паметног града.

При разматрању истраживачких хипотеза важно је имати у виду да оне немају исти методолошки статус. X1 и X2 односе се на архитектонску и аналитичку изводљивост предложеног модела и делимично су поткрепљене кроз студију случаја засновану на PIoT приступу. Насупрот томе, X3 и X4 имају евалуационо-нормативни и институционални карактер, јер се односе на услове под којима би модел могао бити одговоран, објашњив, правно прихватљив и људски контролисан. Због тога се оне не могу третирати као класичне статистички проверљиве хипотезе, већ као претпоставке које су теоријски, правно-етички и институционално оправдане, али захтевају даљу проверу у реалном полицијском пилот-окружењу.

Прва хипотеза, према којој хијерархијски организована вертикална PIoT архитектура представља погодан оквир за превенцију, рано откривање и подршку одлучивању у интелигентном граду, добија снажну концептуалну и функционалну подршку. У објављеном раду показано је да се функције прикупљања сигнала, предобраде, краткорочне предикције и подршке одлучивању могу логично и оперативно распоредити по edge, fog и cloud нивоима, чиме се постиже јасно раздвајање оперативних, тактичких и стратешких улога (Dragović et al., 2026). Ипак, ова хипотеза је потврђена пре свега на нивоу функционалне изводљивости, а не кроз директно експериментално поређење са више конкурентних архитектура. Због тога је научно коректније говорити о снажној индикацији предности вертикалног PIoT приступа, а не о коначно доказаној супериорности у свим условима примене.

Друга хипотеза, према којој интеграција модела машинског учења и fuzzy логике у оквиру PIoT архитектуре може унапредити краткорочну предикцију и подршку одлучивању у

сложеним безбедносним сценаријима, добија јасну емпиријску подршку. У првој студији случаја показано је да RNN, LSTM и GRU модели дају практично употребљиве краткорочне прогнозе саобраћајног тока на fog нивоу, при чему су за различите раскрснице најбоље резултате давали различити модели. Најбољи пријављени резултат укупно је остварио LSTM модел за трећу раскрсницу, са RMSE = 0.028911 и R^2 = 0.925654 (Dragović et al., 2026). Овај налаз показује да предложени оквир није везан за један алгоритам, већ омогућава адаптиван избор модела у зависности од карактеристика конкретних података, што је у складу са широм литературом о моделима временских серија и предиктивној полицијској аналитици (Hall & Rasheed, 2025; Yamak et al., 2019; Meijer & Wessels, 2019).

Додатну потврду друге хипотезе даје fuzzy студија случаја, у којој је показано да се у условима неизвесности и непотпуних сигнала може формализовати подршка одлучивању у сценаријима у којима је потребно разликовати физички упад од сајбер-инцидента. Сигнали са edge и fog нивоа у том моделу преводе се у структурирани излаз на cloud нивоу кроз Sugeno fuzzy inference system (Dragović et al., 2026). Вредност овог приступа је у томе што модел пружа следљиву и интерпретабилну логику одлучивања, али ограничење остаје у чињеници да је реч о моделованом сценарију који треба даље тестирати у ширим оперативним условима (Zadeh, 1965; Wang & Chen, 2014; Khalid et al., 2021).

Трећа хипотеза, према којој се успешност предиктивне аналитике у безбедносном систему не може процењивати само на основу предиктивне тачности, већ мора обухватити и квалитет података, организациону употребљивост, објашњивост модела, правну пропорционалност и контролу алгоритамске пристрасности, добија снажну теоријску и методолошку подршку. Анализа литературе показује да технички прецизан модел може бити недовољно употребљив или чак проблематичан ако се заснива на непоузданим подацима, ако није објашњив, ако производи пристрасне ефекте или ако није уклопљен у правни и институционални оквир (Bennett Moses & Chan, 2018; Richardson et al., 2019; Gstrein et al., 2019). Због тога је у дисертацији предложен шири евалуациони оквир, који поред статистичких метрика укључује оперативне, организационе, правне, етичке и друштвене критеријуме.

Четврта хипотеза, према којој унапређени модел може бити институционално одржив само ако је развијен као систем подршке одлучивању са јасно дефинисаном људском

контролом, а не као потпуно аутоматизован механизам безбедносне процене, подржана је концептуалном, нормативном и практичном аргументацијом. Литература о примени алгоритамских система у полицијском раду доследно указује да аутоматизација без људске контроле може довести до аутоматизационе пристрасности, смањења одговорности и прекомерног ослањања на алгоритамске излазе (Joh, 2020; Asaro, 2019; Oswald et al., 2018). У предложеном моделу зато је задржана логика да аналитички систем може да структурира информације, процени ризик и предложи сценарије поступања, али да коначна одлука мора остати у домену овлашћеног човека, уз правну, етичку и институционалну одговорност.

Сагледано у целини, подршка истраживачким хипотезама може се оценити као довољно снажна да оправда предложени правац развоја модела, али не и као завршна потврда свих његових претпоставки. Управо у томе лежи истраживачка вредност дисертације: она не затвара питање примене предиктивне аналитике у безбедности, већ поставља систематизован, емпиријски ослоњен и методолошки брањив оквир за наредну фазу развоја и провере модела у сложенијим безбедносним сценаријима.

10.3. Научни доприноси

Први научни допринос дисертације огледа се у систематизацији постојећих приступа полицијској аналитици према њиховој методолошкој основи, типовима података, домену примене, оперативној употребљивости и ризицима које производе у пракси (Meijer & Wessels, 2019; Kounadi et al., 2020; Oatley, 2021). На тај начин је формиран аналитички преглед који превазилази техничко набрајање модела и поставља их у шири контекст институционалне примене, квалитета података, алгоритамске пристрасности и правне пропорционалности (Richardson et al., 2019; Babuta & Oswald, 2019; Gstrein et al., 2019).

Други значајан допринос односи се на дефинисање унапређеног хијерархијског модела који повезује науку о подацима, предиктивну аналитику, PIoT инфраструктуру и подршку одлучивању у јединствен концептуални оквир. За разлику од модела усмерених искључиво на hotspot прогнозу или једну аналитичку технику, овде је предложена архитектура у којој су прикупљање сигнала, предобрада, предвиђање, подршка одлучивању у условима неизвесности и евалуација повезани у вертикални ток података и одлука (Dragović et al., 2026; Perry et al., 2013).

Трећи допринос је постављање оквира за евалуацију који укључује техничке, организационе и правно-етичке критеријуме, чиме се превазилази ограничење приступа који успешност система мере само предиктивном тачношћу (Bennett Moses & Chan, 2018; Joshi et al., 2021; Oswald et al., 2018). На тај начин је показано да модел може бити статистички прецизан, а истовремено организационо непрактичан, правно споран или друштвено неприхватљив, што представља једно од централних питања савремене критичке литературе о предиктивном полицијском раду (Ferguson, 2017; Couchman, 2019; Strikwerda, 2020).

Посебан научни допринос огледа се у проширењу логике објављеног PIoT рада са појединачних студија случаја на општи модел превенције и раног откривања илегалних активности. Док објављени рад потврђује изводљивост архитектуре кроз прогнозирање саобраћајног тока и fuzzy подршку одлучивању, дисертација ту логику подиже на виши ниво апстракције и развија је у генерализовани оквир за различите безбедносне сценарије у паметним градовима (Dragović et al., 2026; Joh, 2019; Mugari & Obioha, 2021).

10.4. Стручни и друштвени доприноси

Стручни допринос предложеног модела огледа се у томе што он може послужити као основа за пилот-пројекте полиције, градских служби, служби физичке и сајбер безбедности, ватрогасно-спасилачких структура и других организација које делују у области безбедности у сложеним урбаним срединама (Dragović et al., 2026; Joh, 2019; Yamin et al., 2020). Модел не нуди само општу идеју дигиталне трансформације, већ дефинише улоге актера, типове података, хијерархију аналитичке обраде, технолошке услове, евалуационе метрике и процедуре контроле, што га чини погодним за постепену и институционално контролисану примену (Perry et al., 2013; Casey et al., 2014).

Практични значај предложеног приступа огледа се и у могућности стандардизације примене предиктивне аналитике у домену безбедности. Уместо фрагментарног и ad hoc увођења појединачних алгоритамских алата, модел омогућава да се дигитална трансформација безбедносних служби заснива на претходно дефинисаном архитектонском, организационом и етичком оквиру, чиме се смањује ризик технолошког импровизовања и

неусклађености између техничких могућности и институционалних правила (Meijer et al., 2021; Gstrein et al., 2019).

Друштвени допринос рада огледа се у могућности да се безбедносни ресурси усмеравају правовременије, пропорционалније и информисаније, тако да се ризици и проблеми идентификују пре ескалације, а интервенције планирају на основу релевантних образаца, а не искључиво реактивно (Perry et al., 2013; Braga et al., 2019; Meijer & Wessels, 2019). Истовремено, истраживање полази од јасног становишта да технолошки напредак сам по себи не гарантује друштвену корист: без заштите приватности, објашњивости модела, контроле пристрасности и јасне институционалне одговорности, аналитички системи могу постати извор нових облика дискриминације, прекомерног надзора и губитка јавног поверења (Richardson et al., 2019; Asaro, 2019; Zuiderveen Borgesius, 2020).

10.5. Ограничења и будућа истраживања

Иако је у дисертацији развијен заокружен концептуални, архитектонски и евалуациони оквир унапређеног модела, потребно је нагласити да његова пуна верификација захтева даљи емпиријски рад. Посебно је важно да се предложени модел у наредним фазама провери у контролисаном пилот-окружењу, са јасно дефинисаним изворима података, оперативним процедурама, правним основом, евалуационим метрикама и механизмима људске контроле.

Ограничење овог истраживања јесте и то што су емпиријске потврде најјасније развијене кроз један објављени PIoT рад и његове две студије случаја, што представља снажан, али још увек не и довољан основ за потпуну генерализацију на све облике илегалних активности и све институционалне контексте. Студија случаја, заснована на објављеном PIoT раду, зато се у овој дисертацији третира као доказ концепта за поједине елементе предложеног модела, а не као потпуна валидација целог хијерархијског система. Предвиђање саобраћајног тока показује могућност краткорочне предикције у окружењу паметног града, док fuzzy сценарио показује могућност структуриране подршке одлучивању у условима неизвесности. Међутим, за потпуну проверу применљивости модела у превенцији и раном откривању илегалних активности потребна су даља истраживања, уз повезивање са

полицијским евиденцијама, подацима о инцидентима, јавним догађајима, сензорским подацима и другим безбедносно релевантним изворима.

Најзначајније ограничење дисертације односи се на одсуство реалног пилот-тестирања у полицијско-институционалном окружењу. Предложени модел је концептуално развијен, архитектонски разрађен и делимично поткрепљен кроз доказ концепта, али није тестиран у реалним условима полицијског поступања, са стварним оперативним токовима, институционалним ограничењима, правним процедурама и одговорношћу службеника који користе аналитичке резултате. Ово ограничење је разумљиво имајући у виду осетљивост полицијских података, правне услове обраде података о личности, организационе баријере, безбедносне ризике и потребу за формалним одобрењима надлежних институција. Управо зато се у дисертацији предложени модел не представља као коначно валидиран оперативни систем, већ као научно утемељен и евалуабилан оквир који треба да буде предмет будуће пилот-примене.

Криминално-безбедносни исходи, као што су смањење броја инцидената, спречавање конкретних илегалних активности или повећање ефикасности интервенција, у овој дисертацији нису емпиријски измерени, већ су постављени као потенцијални ефекти будуће примене модела. Њихова провера захтева посебно дизајнирану пилот-студију са јасним индикаторима исхода и контролисаним условима евалуације.

У складу са тим, будућа истраживања треба усмерити ка проширењу броја студија случаја, укључивању изразитије сајбер-безбедносних сценарија, поређењу већег броја алгоритамских породица, развоју explainable AI решења и емпиријској провери модела у реалним или реалистично симулираним полицијским окружењима (Adadi & Berrada, 2018; Hall & Rasheed, 2025; Dragović et al., 2026).

Посебно важан правац будућег рада односи се на испитивање равнотеже између аналитичке ефикасности и нормативне прихватљивости. Савремена литература јасно указује да ће одрживост предиктивних полицијских система зависити не само од њихове тачности, већ и од начина на који се решавају питања правичности, објашњивости, законитости и одговорности (Hobson et al., 2021; Alikhademi et al., 2021; Gstrein et al., 2019). Управо зато

даљи развој модела мора истовремено обухватити техничко унапређење, организациону примену и нормативну верификацију.

10.6. Завршна разматрања

Унапређење модела за превенцију и рано откривање илегалних активности применом предиктивне аналитике има научни и практични смисао само ако води ка проактивном, законитом и одговорном деловању институција безбедности (Meijer & Wessels, 2019; Oswald et al., 2018; Ferguson, 2020). Зато предложени модел не тежи аутоматизацији полицијске процене, већ њеном унапређењу кроз структурирано коришћење података, аналитичких модела и хијерархијске дигиталне инфраструктуре.

Његова суштина је у томе да подаци помогну да се ризици боље разумеју, да се ресурси распоређују рационалније, да се одлуке доносе брже и информисаније, али увек уз људску контролу, правну заснованост, етичка ограничења и сталну проверу стварних ефеката у пракси (Asaro, 2019; Bennett Moses & Chan, 2018; Dragović et al., 2026).

На крају се може закључити да предложени модел представља методолошки, технолошки и организациони основ за даљи развој савременог, хијерархијски организованог и институционално одговорног приступа превенцији и раном откривању илегалних активности у условима интелигентног града. Његов главни допринос није у замени постојећих полицијских процедура алгоритмом, већ у унапређењу аналитичко-оперативног циклуса кроз повезивање података, предикције, fuzzy/XAI подршке, људске контроле, евалуације и организационог учења.

Литература

1. Adadi, A., & Berrada, M. (2018). Peeking inside the black-box: A survey on explainable artificial intelligence (XAI). IEEE Access, 6, 52138–52160. https://doi.org/10.1109/ACCESS.2018.2870052
2. Adepeju, M., Rosser, G., & Cheng, T. (2016). Novel evaluation metrics for sparse spatio-temporal point process hotspot predictions: A crime case study. International Journal of Geographical Information Science, 30(11), 2133–2154. https://doi.org/10.1080/13658816.2016.1159684
3. Albrecht, H.-J. (2020). Data, data banks and security. European Journal for Security Research, 5, 305–316. https://doi.org/10.1007/s41125-019-00062-9
4. Alikhademi, K., Drobina, E., Prioleau, D., Richardson, B., Purves, D., & Gilbert, J. E. (2021). A review of predictive policing from the perspective of fairness. Artificial Intelligence and Law, 30, 1–17. https://doi.org/10.1007/s10506-021-09286-4
5. Alon-Barkat, S., & Busuioc, M. (2023). Human–AI interactions in public sector decision-making: “Automation bias” and “selective adherence” to algorithmic advice. Journal of Public Administration Research and Theory, 33(1), 153–169. https://doi.org/10.1093/jopart/muac007
6. Andresen, M. A., Linning, S. J., & Malleson, N. (2017). Crime at places and spatial concentrations: Exploring the spatial stability of property crime in Vancouver, BC, 2003–2013. Journal of Quantitative Criminology, 33(2), 255–275. https://doi.org/10.1007/s10940-016-9295-8
7. Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). Machine bias. ProPublica. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing
8. Asaro, P. M. (2019). AI ethics in predictive policing: From models of threat to an ethics of care. IEEE Technology and Society Magazine, 38(2), 40–53. https://doi.org/10.1109/MTS.2019.2915154
9. Ashby, D. I., & Longley, P. A. (2005). Geocomputation, geodemographics and resource allocation for local policing. Transactions in GIS, 9(1), 53–72. https://doi.org/10.1111/j.1467-9671.2005.00202.x
10. Babuta, A., & Oswald, M. (2019). Data analytics and algorithmic bias in policing. Royal United Services Institute.
11. Bachner, J. (2013). Predictive policing: Preventing crime with data and analytics. IBM Center for The Business of Government.
12. Bakke, E. (2018). Predictive policing: The argument for public transparency. Annual Survey of American Law, 74(1), 131–171.
13. Beaverton Police Department. (2010). Crime analysis and tactical analysis in policing. Beaverton Police Department.

14. Bennett Moses, L., & Chan, J. (2018). Algorithmic prediction in policing: Assumptions, evaluation, and accountability. Policing and Society, 28(7), 806–822. https://doi.org/10.1080/10439463.2016.1253695
15. Berk, R. A. (2021). Artificial intelligence, predictive policing, and risk assessment for law enforcement. Annual Review of Criminology, 4, 209–237. https://doi.org/10.1146/annurev-criminol-051520-012342
16. Berman, E. (2019). Individualized suspicion in the age of big data. Iowa Law Review, 105, 463–509. https://ssrn.com/abstract=3414467
17. Biliri, E., et al. (2017). Big data analytics in public safety and personal security: Challenges and potential. In 2017 International Conference on Engineering, Technology and Innovation (ICE/ITMC) (pp. 1382–1386). https://doi.org/10.1109/ICE.2017.8280043
18. Boba, R. (2001). Introductory guide to crime analysis and mapping. Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services.
19. Bommasani, R., Hudson, D. A., Adeli, E., Altman, R., Arora, S., von Arx, S., Bernstein, M. S., Bohg, J., Bosselut, A., Brunskill, E., Brynjolfsson, E., Buch, S., Card, D., Castellon, R., Chatterji, N., Chen, A., Creel, K., Davis, J. Q., Demszky, D., Donahue, C., Doumbouya, M., Durmus, E., Ermon, S., Etchemendy, J., Ethayarajh, K., Fei-Fei, L., Finn, C., Gale, T., Gillespie, L., Goel, K., Goodman, N., Gross, S., Guha, N., Hashimoto, T., Ho, D. E., Hong, J., Hsu, K., Huang, J., Icard, T., Jain, S., Jurafsky, D., Kalluri, P., Karamcheti, S., Keeling, G., Khani, F., Khattab, O., Koh, P. W., Krass, M., Krishna, R., Kuditipudi, R., Kumar, A., Ladhak, F., Lee, M., Lee, T., Leskovec, J., Levent, I., Li, X. L., Li, X., Li, T., Ma, T., Malik, A., Manning, C. D., Mirchandani, S., Mitchell, E., Munyikwa, Z., Nair, S., Narayan, A., Narayanan, D., Newman, B., Nie, A., Niebles, J. C., Ogut, G., Orr, L., Papadimitriou, I., Park, J. S., Piech, C., Portelance, E., Potts, C., Raghunathan, A., Reich, R., Ren, H., Rong, F., Roohani, Y., Ruiz, C., Ryan, J., Ré, C., Sadigh, D., Sagawa, S., Santhanam, K., Shih, A., Srinivasan, K., Tamkin, A., Taori, R., Thomas, A. W., Tramèr, F., Wang, R. E., Wang, W., Wu, B., Wu, J., Wu, Y., Xie, S. M., Yasunaga, M., You, J., Zaharia, M., Zhang, M., Zhang, T., Zhang, X., Zhang, Y., Zheng, L., Zhou, K., & Liang, P. (2021). On the opportunities and risks of foundation models. arXiv preprint. https://arxiv.org/abs/2108.07258
20. Braga, A. A., Turchan, B., Papachristos, A. V., & Hureau, D. M. (2019). Hot spots policing of small geographic areas: Effects on crime. Campbell Systematic Reviews, 15(3), e1046. https://doi.org/10.1002/cl2.1046
21. Brantingham, P. J., Valasik, M., & Mohler, G. O. (2018). Does predictive policing lead to biased arrests? Results from a randomized controlled trial. Statistics and Public Policy, 5(1), 1–6. https://doi.org/10.1080/2330443X.2018.1438940
22. Brayne, S. (2017). Big data surveillance: The case of policing. American Sociological Review, 82(5), 977–1008. https://doi.org/10.1177/0003122417725865
23. Brayne, S., Rosenblat, A., & Boyd, d. (2015). Predictive policing, data, and civil rights: A new era of policing and justice. Data & Civil Rights.

24. Camacho-Collados, M., & Liberatore, F. (2015). A decision support system for predictive police patrolling. Decision Support Systems, 75, 25–37. https://doi.org/10.1016/j.dss.2015.04.012
25. Casey, D., Burrell, P., & Sumner, N. (2014). Decision support systems in policing. European Law Enforcement Research Bulletin, Special Conference Edition, 59–65.
26. College of Policing. (2021). The effectiveness of visible police patrol. College of Policing. https://www.college.police.uk/research/what-works-policing-reduce-crime/visible-police-patrol
27. Čomić, T. (2019). Unapređenje zvanične statistike primenom Big Data koncepta. Doktorska disertacija, Univerzitet u Beogradu, Fakultet organizacionih nauka, Beograd.
28. Couchman, H. (2019). Policing by machine: Predictive policing and the threats to our rights. Liberty.
29. Council of Europe. (2024). Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. Council of Europe. https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence
30. Das, M., Saraswathi, S., Panda, R., Mishra, A. K., & Tripathy, A. K. (2021). Exquisite analysis of popular machine learning-based phishing detection techniques for cyber systems. Journal of Applied Security Research, 16(4), 538–562.
31. Demchenko, Y., Grosso, P., de Laat, C., & Membrey, P. (2013). Addressing big data issues in scientific data infrastructure. In 2013 International Conference on Collaboration Technologies and Systems (CTS) (pp. 48–55). https://doi.org/10.1109/CTS.2013.6567203
32. Doan, L., Ray, R., Powelson, C., Fuentes, G., Shankman, R., Genter, S., & Bailey, J. (2021). Evaluation of a virtual reality simulation tool for studying bias in police-civilian interactions. In Augmented Cognition. HCI 2021 (pp. 388–399).
33. Dragović, N., Milić, S. D., Vukmirović, D., & Ćomić, T. (2026). Data-driven Police IoT in smart cities: A sustainable hierarchical framework for traffic prediction and policing decisions. Sustainability, 18(10), 4867. https://doi.org/10.3390/su18104867
34. Dumbill, E. (2013). Making sense of big data. Big Data, 1(1), 1–2. https://doi.org/10.1089/big.2012.1503
35. E&Y. (2018). Predictive policing and the way forward. Ernst & Young LLP.
36. European Parliament and Council of the European Union. (2016). Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. Official Journal of the European Union, L 119, 89–131. https://eur-lex.europa.eu/eli/dir/2016/680/oj

37. European Parliament and 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. https://eur-lex.europa.eu/eli/reg/2024/1689/oj
38. Europol Innovation Lab. (2023). ChatGPT: The impact of large language models on law enforcement. Europol. https://www.europol.europa.eu/publications-events/publications/chatgpt-impact-of-large-language-models-law-enforcement
39. Falade, A., Azeta, A. A., Oni, A. A., & Odun-Ayo, I. (2019). Systematic literature review of crime prediction and data mining. Review of Computer Engineering Studies, 6(3), 56–65. https://doi.org/10.18280/rces.060302
40. Favaretto, M., De Clercq, E., & Elger, B. S. (2019). Big data and discrimination: Perils, promises and solutions. A systematic review. Journal of Big Data, 6, 12. https://doi.org/10.1186/s40537-019-0177-4
41. Feng, M., Zheng, J., Ren, J., Hussain, A., Li, X., Xi, Y., & Liu, Q. (2019). Big data analytics and mining for effective visualization and trends forecasting of crime data. IEEE Access, 7, 106111–106123. https://doi.org/10.1109/ACCESS.2019.2930410
42. Fennelly, L. J. (2020). What is crime prevention in 2020? In L. J. Fennelly (Ed.), Handbook of loss prevention and crime prevention (6th ed., pp. 99–103). Butterworth-Heinemann. https://doi.org/10.1016/B978-0-12-817273-5.00010-7
43. Ferguson, A. G. (2017). Policing predictive policing. Washington University Law Review, 94, 1109–1189.
44. Ferguson, A. G. (2018). Illuminating black data policing. Ohio State Journal of Criminal Law, 15(2), 503–525.
45. Ferguson, A. G. (2020). Predictive policing theory. Washington College of Law Research Paper.
46. Ferreira, J. (2012). GIS for crime analysis: Geography for predictive models. Electronic Journal of Information Systems Evaluation, 15.
47. Fitzpatrick, D. J., Gorr, W. L., & Neill, D. B. (2019). Keeping score: Predictive analytics in policing. Annual Review of Criminology, 2, 473–491. https://doi.org/10.1146/annurev-criminol-011518-024534
48. Grace, J. (2019). Algorithmic impropriety in UK policing? Journal of Information Rights, Policy and Practice. https://doi.org/10.21039/irpandp.v3i1.57
49. Gstrein, O. J., Bunnik, A., & Zwitter, A. (2019). Ethical, legal and social challenges of predictive policing. Católica Law Review, 3(3), 77–98.
50. Hall, T., & Rasheed, K. (2025). A survey of machine learning methods for time series prediction. Applied Sciences, 15(11), 5957. https://doi.org/10.3390/app15115957
51. Hassani, H., Huang, X., Silva, E. S., & Ghodsi, M. (2021). A review of data mining applications in crime. Statistical Analysis and Data Mining. https://doi.org/10.1002/sam.11312

52. Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75–105.
53. Hobson, Z., Yesberg, J. A., Bradford, B., & Jackson, J. (2021). Artificial fairness? Trust in algorithmic police decision-making. Journal of Experimental Criminology, 19, 165–189. https://doi.org/10.1007/s11292-021-09484-9
54. Huang, L., Yu, W., Ma, W., Zhong, W., Feng, Z., Wang, H., Chen, Q., Peng, W., Feng, X., Qin, B., & Liu, T. (2025). A survey on hallucination in large language models: Principles, taxonomy, challenges, and open questions. ACM Transactions on Information Systems. https://doi.org/10.1145/3703155
55. Hunt, P., Saunders, J., & Hollywood, J. S. (2014). Evaluation of the Shreveport predictive policing experiment. RAND Corporation.
56. Ilijazi, V., Milic, N., Milidragovic, D., & Popovic, B. (2019). An assessment of police officers' perception of hotspots: What can be done to improve officers' situational awareness? ISPRS International Journal of Geo-Information, 8(6), 260. https://doi.org/10.3390/ijgi8060260
57. Innefu Lab. (2025). Policing software in the age of AI: From reactive reports to proactive crime prevention. https://innefu.com/policing-software-in-the-age-of-ai-from-reactive-reports-to-proactive-crime-prevention/
58. International Association of Crime Analysts. (2024). Crime analysis defined. International Association of Crime Analysts.
59. Joh, E. E. (2019). Policing the smart city. International Journal of Law in Context, 15(2), 177–182. https://doi.org/10.1017/S1744552319000107
60. Joh, E. E. (2020). Increasing automation in policing. Communications of the ACM, 63(1), 20–22. https://doi.org/10.1145/3372912
61. Jones, D., & Gwinn, S. L. (2017). Strategic crime analysis. In R. Wortley, A. Sidebottom, N. Tilley, & G. Laycock (Eds.), Routledge handbook of crime science. Routledge.
62. Joshi, C., Curtis-Ham, S., D'Ath, C., & Searle, D. (2021). Considerations for developing predictive spatial models of crime and new methods for measuring their accuracy. ISPRS International Journal of Geo-Information, 10(9), 597. https://doi.org/10.3390/ijgi10090597
63. Khalid, S., Khan, S. A., & Ifzal, S. Q. (2021). A fuzzy logic-based framework for mapping crime data on established sociological hypothesis for societal disorder identification and prevention. IEEE Access, 9, 80197–80207. https://doi.org/10.1109/ACCESS.2021.3083542
64. Khatun, M. R., Ayon, S. I., Hossain, M. R., & Alam, M. J. (2021). Data mining technique to analyse and predict crime using crime categories and arrest records. Indonesian Journal of Electrical Engineering and Computer Science, 22, 1052–1060. https://doi.org/10.11591/IJEECS.V22.I2.PP1052-1060

65. King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. Science and Engineering Ethics, 26, 89–120. https://doi.org/10.1007/s11948-018-00081-0
66. Kounadi, O., Ristea, A., Araujo, A., & Leitner, M. (2020). A systematic review on spatial crime forecasting. Crime Science, 9, 7. https://doi.org/10.1186/s40163-020-00116-7
67. Lam, D. (2014). A survey of predictive analytics in data mining with big data. Athabasca University.
68. Lamnisos, D., Lambrianou, A., & Kontoyiannis, D. (2019). Using geodemographic data to model crime patterns. ISPRS International Journal of Geo-Information, 8(5), 213. https://doi.org/10.3390/ijgi8050213
69. LISC/BCJI. (2014). Crime analysis for non-criminal justice researchers. Local Initiatives Support Corporation / Byrne Criminal Justice Innovation.
70. London Strategic Crime Analysis. (2022). Strategic crime analysis: Analytical framework and applications. London Strategic Crime Analysis.
71. Lum, C., & Koper, C. S. (2017). Evidence-based policing: Translating research into practice. Oxford University Press.
72. Malleson, N., & Andresen, M. A. (2015). The impact of using social media data in crime rate calculations: Shifting hot spots and changing spatial patterns. Cartography and Geographic Information Science, 42(2), 112–121. https://doi.org/10.1080/15230406.2014.905756
73. Meijer, A., & Wessels, M. (2019). Predictive policing: Review of benefits and drawbacks. International Journal of Public Administration, 42(12), 1031–1039. https://doi.org/10.1080/01900692.2019.1575664
74. Meijer, A., Lorenz, L., & Wessels, M. (2021). Algorithmization of bureaucratic organizations: Using a practice lens to study how context shapes predictive policing systems. Public Administration Review, 81(5), 837–846. https://doi.org/10.1111/puar.13391
75. Mitchell, I., Hara, S., Ibarra Jimenez, J., Jahankhani, H., & Montasari, R. (2020). IoT and cloud forensic investigation guidelines. In H. Jahankhani, B. Akhgar, P. Cochrane, & M. Dastbaz (Eds.), Policing in the era of AI and smart societies (pp. 69–88). Springer.
76. Mittal, P. (2020). Big data and analytics: A data management perspective in public administration. International Journal of Big Data Management, 1(2), 152–165. https://doi.org/10.1504/IJBDM.2020.10032871
77. Mohamed, N., Al-Jaroodi, J., Lazarova-Molnar, S., & Jawhar, I. (2021). Applications of integrated IoT-fog-cloud systems to smart cities: A survey. Electronics, 10(23), 2918. https://doi.org/10.3390/electronics10232918
78. Mohler, G. O., Short, M. B., Malinowski, S., Johnson, M., Tita, G. E., Bertozzi, A. L., & Brantingham, P. J. (2015). Randomized controlled field trials of predictive policing. Journal of the American Statistical Association, 110(512), 1399–1411. https://doi.org/10.1080/01621459.2015.1077710

79. Mohler, G., Raje, R., Carter, J., Valasik, M., & Brantingham, J. (2018). A penalized likelihood method for balancing accuracy and fairness in predictive policing. In 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC) (pp. 2454–2459).
80. Morley, A. (2020). Digital policing: Disruptive technologies enhancing the policing experience. Deloitte.
81. Mugari, I., & Obioha, E. E. (2021). Predictive policing and crime control in the United States of America and Europe: Trends in a decade of research and the future of predictive policing. Social Sciences, 10(6), 234. https://doi.org/10.3390/socsci10060234
82. National Policing Institute. (2026). AI in policing beyond the early adopters: What your agency can and should do. https://www.policinginstitute.org/infocus/ai-in-policing/
83. NIJ. (2014). Predictive policing. National Institute of Justice. https://nij.ojp.gov/topics/articles/predictive-policing
84. Norton, A. A. (2013). Predictive policing: The future of law enforcement in the Trinidad and Tobago Police Service (TTPS). International Journal of Computer Applications, 62(4), 32–36. https://doi.org/10.5120/10070-4680
85. Oatley, G. C. (2021). Themes in data mining, big data, and crime analytics. WIREs Data Mining and Knowledge Discovery, 12(2), e1432. https://doi.org/10.1002/widm.1432
86. Oatley, G., & Ewart, B. (2011). Data mining and crime analysis. WIREs Data Mining and Knowledge Discovery. https://doi.org/10.1002/widm.6
87. OSCE. (2017). OSCE guidebook: Intelligence-led policing. Organization for Security and Co-operation in Europe. https://www.osce.org/chairmanship/327476
88. Oswald, M., Grace, J., Urwin, S., & Barnes, G. C. (2018). Algorithmic risk assessment policing models: Lessons from the Durham HART model and experimental proportionality. Information & Communications Technology Law, 27(2), 223–250. https://doi.org/10.1080/13600834.2018.1458455
89. Perera, C., Qin, Y., Estrella, J. C., Reiff-Marganiec, S., & Vasilakos, A. V. (2017). Fog computing for sustainable smart cities: A survey. ACM Computing Surveys, 50(3), Article 32. https://doi.org/10.1145/3057266
90. Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Hollywood, J. S. (2013). Predictive policing: The role of crime forecasting in law enforcement operations. RAND Corporation. https://doi.org/10.7249/RR233
91. Pramanik, M. I., Lau, R. Y. K., Yue, W. T., Ye, Y., & Li, C. (2017). Big data analytics for security and criminal investigations. WIREs Data Mining and Knowledge Discovery. https://doi.org/10.1002/widm.1208
92. Prislan, K., & Slak, B. (2018). Analysis of the relationship between smart cities, policing and criminal investigation. Journal of Criminal Justice and Security, 389–413.
93. Public Safety Data Portal. (2022). Toronto Police Service public safety data portal. Toronto Police Service.

94. Radenković, B., & Kočović, P. (2017). Emerging trends and applications of the Internet of Things. IGI Global.
95. Ratcliffe, J. H. (2004). The hotspot matrix: A framework for the spatio-temporal targeting of crime reduction. Police Practice and Research, 5(1), 5–23. https://doi.org/10.1080/1561426042000191305
96. Ratcliffe, J. H. (2007). Integrated intelligence and crime analysis: Enhanced information management for law enforcement leaders. Police Foundation.
97. Richardson, R., Schultz, J. M., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. New York University Law Review Online, 94, 15–55.
98. Saunders, J., Hunt, P., & Hollywood, J. S. (2016). Predictions put into practice: A quasi-experimental evaluation of Chicago's predictive policing pilot. Journal of Experimental Criminology, 12(3), 347–371. https://doi.org/10.1007/s11292-016-9272-0
99. Schatsky, D., Muraskin, C., & Gurumurthy, R. (2015). Cognitive technologies: The real opportunities for business. Deloitte Review, 16, 77–91.
100. Sekulović, A. (2018). Procena rizika u urbanom bezbednosnom okruženju. Beograd: Kriminalističko-policijski univerzitet.
101. Selbst, A. D. (2017). Disparate impact in big data policing. Georgia Law Review, 52, 109–195.
102. Shalaginov, A. (2018). Advancing neuro-fuzzy algorithm for automated classification in large-scale forensic and cybercrime investigations (Doctoral dissertation). Norwegian University of Science and Technology.
103. Sneader, K., & Singhal, S. (2021). The next normal arrives: Trends that will define 2021 and beyond. McKinsey & Company.
104. Songhorabadi, M., Rahimi, M., Moghadam Farid, A., & Haghi Kashani, M. (2023). Fog computing approaches in IoT-enabled smart cities. Journal of Network and Computer Applications, 211, 103557. https://doi.org/10.1016/j.jnca.2022.103557
105. Strikwerda, L. (2020). Predictive policing: The risks associated with risk assessment. The Police Journal: Theory, Practice and Principles, 1–15. https://doi.org/10.1177/0032258X20947749
106. Stupar, D. (2021). Kriminalističко-obavještajna djelatnost kao preduslov kvalitetne kriminalističke prognostike kriminaliteta. Žurnal za bezbjednost i kriminalistiku, 3(1), 57–74. https://doi.org/10.5937/zurbezkrim2101057S
107. Sun, J., et al. (2021). CrimeForecaster: Crime prediction by exploiting the geographical neighborhoods' spatiotemporal dependencies. In Y. Dong et al. (Eds.), Machine learning and knowledge discovery in databases. Applied data science and demo track (pp. 180–196). Springer. https://doi.org/10.1007/978-3-030-67670-4_14
108. Tian, Z., Luo, C, Lu, H., Su, S., Sun, Y., & Zhang, M. (2020). User and entity behavior analysis under urban big data. ACM Transactions on Data Science, 1(3), 1–19.

109. Tonkin, M., Santtila, P., & Bull, R. (2012). The linking of burglary crimes using offender behaviour: Testing research cross-nationally and exploring methodology. Legal and Criminological Psychology, 17(2), 276–293. https://doi.org/10.1111/j.2044-8333.2010.02007.x
110. Tonmoy, S. M. T. I., Zaman, S. M. M., Jain, V., Rani, A., Rawte, V., Chadha, A., & Das, A. (2024). A comprehensive survey of hallucination mitigation techniques in large language models. arXiv. https://arxiv.org/abs/2401.01313
111. Turvey, B. E. (1999). Criminal profiling: An introduction to behavioral evidence analysis. Academic Press.
112. UNICRI. (2019). Artificial intelligence and robotics for law enforcement. United Nations Interregional Crime and Justice Research Institute; INTERPOL.
113. Van Brakel, R., & De Hert, P. (2011). Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology-based strategies. Cahiers Politiestudies, 20(20), 163–192.
114. Vinodhini, M., Srivastava, D., Hirani, S., & Arora, S. (2020). An end-to-end novel forecasting model for crime prediction based on big data. International Journal of Recent Technology and Engineering, 8(6). https://doi.org/10.35940/ijrte.F9153.038620
115. Vogiatzoglou, P. (2019). Mass surveillance, predictive policing and the implementation of the CJEU and ECtHR requirement of objectivity. European Journal of Law and Technology, 10(1), 1–18.
116. Vukmirović, D. V., Bolbotinović, Ž. Z., Čomić, T. Z., & Stanojević, N. D. (2022). HR analytics: Serbian perspective. In Proceedings of the 1st Serbian International Conference on Applied Artificial Intelligence (SICAAI). http://www.aai2022.kg.ac.rs/aai-2022-papers/
117. Vukmirović, D., & Jovanović-Milenković, M. (2025). Generativna veštačka inteligencija: Principi i primena u savremenom poslovanju. Univerzitet u Beogradu – Fakultet organizacionih nauka.
118. Vukmirović, D. (2026). From Big Data to AI-native: 7V, synthetic data, and the new role of data science in industry, Data Fest 2026. https://doi.org/10.13140/RG.2.2.33467.94245
119. Vuković, I., Čisar, P., Kuk, K., & Popović, B. (2021). Challenges of contemporary predictive policing. Thematic Conference Proceedings of International Significance, International Scientific Conference "Archibald Reiss Days", Belgrade, 513–526.
120. Vuković, N., Vukmirović, D., & Radojičić, Z. (1998). SPSS tutorijal. Fakultet organizacionih nauka.
121. Wang, B., Zhang, D., Zhang, D., Brantingham, P. J., & Bertozzi, A. L. (2017). Deep learning for real time crime forecasting. arXiv preprint. https://arxiv.org/abs/1707.03340
122. Wang, Y., & Chen, Y. (2014). A comparison of Mamdani and Sugeno fuzzy inference systems for traffic flow prediction. Journal of Computers, 9(1), 12–21. https://doi.org/10.4304/jcp.9.1.12-21

123. Wawrzyniak, Z. M., et al. (2018). Relationships between crime and everyday factors. In 2018 IEEE 22nd International Conference on Intelligent Engineering Systems (INES) (pp. 000039–000044). https://doi.org/10.1109/INES.2018.8523999
124. Webber, R., & Burrows, R. (2018). The predictive postcode: The geodemographic classification of British society. London, UK: Zed Books.
125. Weisburd, D., & McEwen, J. T. (Eds.). (1997). Crime mapping and crime prevention. Monsey, NY: Criminal Justice Press.
126. Wilson, D. (2019). Platform policing and the real-time cop. Surveillance & Society, 17(1/2), 69–75.
127. Woodhams, J., & Labuschagne, G. (2002). A test of case linkage principles with serial rapists. Journal of Investigative Psychology and Offender Profiling, 9(1), 28–42.
128. Yamak, P. T., Yujian, L., & Gadosey, P. K. (2019). A comparison between ARIMA, LSTM, and GRU for time series forecasting. In Proceedings of the 2nd International Conference on Algorithms, Computing and Artificial Intelligence. Association for Computing Machinery. https://doi.org/10.1145/3377713.3377722
129. Yamin, M. M., Shalaginov, A., & Katt, B. (2020). Smart policing for a smart world: Opportunities, challenges and way forward. In Advances in Future of Information and Communication Conference (FICC 2020). Springer. https://doi.org/10.1007/978-3-030-39445-5_39
130. Zadeh, L. A. (1965). Fuzzy sets. Information and Control, 8(3), 338–353. https://doi.org/10.1016/S0019-9958(65)90241-X
131. Zuiderveen Borgesius, F. (2020). Discrimination, artificial intelligence, and algorithmic decision-making. Council of Europe Study DGI(2018)12.

Биографија

Небојша Драговић рођен је 1974. године у Лебану, Република Србија. Школске 1996/1997. године уписао је студије на Полицијској академији у Београду, које је завршио 2000. године. Године 2009. уписао је специјалистичке академске студије на Криминалистичко-полицијској академији, студијски програм „Супротстављање савременим облицима криминалитета“, које је завршио са просечном оценом 9 (девет). Године 2012. одбранио је завршни рад на тему „Прикривени иследник као посебна доказна радња – законски и криминалистички аспекти примене“.

Докторске академске студије, студијски програм Информациони системи и квантитативни менаџмент, изборно подручје Квантитативни менаџмент, уписао је 2018. године на Факултету организационих наука Универзитета у Београду. Положио је све испите и одбранио приступни рад на докторским студијама са просечном оценом 10 (десет).

Небојша Драговић има више од 26 године радног искуства на више различитих руководећих радних места у Министарству унутрашњих послова, на пословима унапређења превенције, спречавања и сузбијања различитих облика илегалних активности и инкриминисаних деликата (кривичних дела и прекршаја).

Списак објављених публикација

Радови у међународним часописима

Dragović, N., Milić, S. D., Vukmirović, D., & Čomić, T. (2026). Data-driven police IoT in smart cities: A sustainable hierarchical framework for traffic prediction and policing decisions. *Sustainability, 18*(10), 4867. https://doi.org/10.3390/su18104867 (M23)

Cvetković, N., Dobrota, M., Đoković, A., & Dragović, N. (2019). Field stress detection using remote sensing in agriculture. *INFO M, 69*. Fakultet organizacionih nauka, Beograd. ISSN 1451-4397. (M52)

Milidragović, D. N., Milić, S. D., & Dragović, N. (2020). Community policing implementation in Republic of Serbia: A view from the managers' perspective. *NBP – Journal of Criminalistics and Law, 25*(1). https://doi.org/10.5937/nabepo25-25323 (M24, oblast pravo i politikologija)

Радови на међународним конференцијама

Cvetković, N., Dragović, N., & Đoković, A. (2018). Field stress detection algorithm using remote sensing. In *XVI International Symposium SymOrg 2018: Doing Business in the Digital Age: Challenges, Approaches and Solutions* (pp. 229–235). Zlatibor, Serbia. ISBN 978-86-7680-361-3. (M33)

Radojičić, S., Kresović, D., Bolbotinović, Ž., Dragović, N., Krstić, A., & Vukmirović, D. (2023). E-government divide – Case study Serbia. *E-Business Technologies Conference Proceedings, 3*(1), 44–49. Preuzeto sa https://ebt.rs/journals/index.php/conf-proc/article/view/177 (M33)

Vukmirović, D., Radojičić, S., Stanojević, N., Dragović, N., & Čomić, T. (2026). Enhancing critical infrastructure resilience: An integrated framework for hazardous material management of electric vehicle batteries. In Z. Keković, S. Kentera, M. Dabetić, & S. Grbović (Eds.), *Critical Infrastructure: Risk and Crisis Management in the New Reality* (pp. 81–109). Cham: Springer. https://doi.org/10.1007/978-3-032-20948-1_5 (M14)

Радови на конференцијама националног значаја

Bolbotinović, Ž., Radojičić, S., Dragović, N., & Vukmirović, D. (2022). Izazovi digitalne transformacije malih i srednjih preduzeća u uslovima „nove normalnosti". U: *Zbornik radova 28. IKT konferencije „YU INFO 2022"* (YU INFO 2022). ISBN 978-86-85525-27-8. (M63)

Radojičić, S., Bolbotinović, Ž., Dragović, N., & Vukmirović, D. (2022). Digitalno pismena populacija kao osnova društvenog i ekonomskog razvoja – primer Republike Srbije. U: *Zbornik radova 28. IKT konferencije „YU INFO 2022"* (pp. 312–315). ISBN 978-86-85525-27-8. (M63)

Изјава о ауторству

Име и презиме аутора: **Небојше Драговић**

Број индекса 2018/5038

Изјављујем да је докторска дисертација под насловом

Унапређење модела за превенцију и рано откривање илегалних активности применом предиктивне аналитике

резултат сопственог истраживачког рада;

- да дисертација у целини ни у деловима није била предложена за стицање друге дипломе према студијским програмима других високошколских установа;
- да су резултати коректно наведени и
- да нисам кршио/ла ауторска права и користио/ла интелектуалну својину других лица.

У Београду, **Потпис аутора**

_____ _____

Изјава о истоветности штампане и електронске верзије докторског рада

Име и презиме аутора **Небојше Драговића**

Број индекса 2018/5038

Студијски програм **Информациони системи и квантитативни менаџмент, изборно подручје Квантитативни менаџмент**

Наслов рада **Унапређење модела за превенцију и рано откривање илегалних активности применом предиктивне аналитике**

Ментор **проф. др Драган Вукмировић**

Изјављујем да је штампана верзија мог докторског рада истоветна електронској верзији коју сам предао/ла ради похрањења у **Дигиталном репозиторијуму Универзитета у Београду.**

Дозвољавам да се објаве моји лични подаци везани за добијање академског назива доктора наука, као што су име и презиме, година и место рођења и датум одбране рада.

Ови лични подаци могу се објавити на мрежним страницама дигиталне библиотеке, у електронском каталогу и у публикацијама Универзитета у Београду.

У Београду, **Потпис аутора**

_____ _____

Изјава о коришћењу

Овлашћујем Универзитетску библиотеку „Светозар Марковић“ да у Дигитални репозиторијум Универзитета у Београду унесе моју докторску дисертацију под насловом:

Унапређење модела за превенцију и рано откривање илегалних активности применом предиктивне аналитике која је моје ауторско дело.

Дисертацију са свим прилозима предао/ла сам у електронском формату погодном за трајно архивирање.

Моју докторску дисертацију похрањену у Дигиталном репозиторијуму Универзитета у Београду и доступну у отвореном приступу могу да користе сви који поштују одредбе садржане у одабраном типу лиценце Креативне заједнице (Creative Commons) за коју сам се одлучио/ла.

1. Ауторство (CC BY)

2. Ауторство – некомерцијално (CC BY-NC)

3. Ауторство – некомерцијално – без прерада (CC BY-NC-ND)

4. Ауторство – некомерцијално – делити под истим условима (CC BY-NC-SA)

5. Ауторство – без прерада (CC BY-ND)

6. Ауторство – делити под истим условима (CC BY-SA)