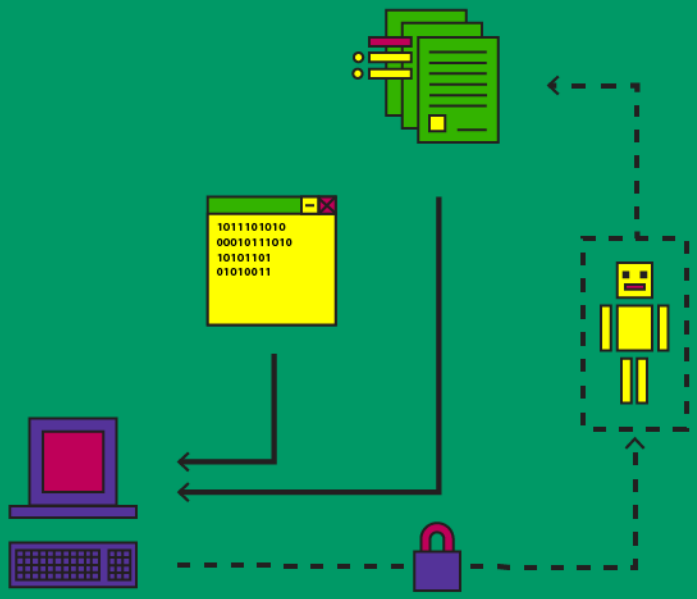


ОДНОС ПРИМЕНЕ ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ У ОБЛАСТИ РАДА И ЗАПОШЉАВАЊА И ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ У РЕПУБЛИЦИ СРБИЈИ

Златко Петровић

Уредници
Бранка Анђелковић
Тања Јакоби

ОДНОС ПРИМЕНЕ ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ У ОБЛАСТИ РАДА И ЗАПОШЉАВАЊА И ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ У РЕПУБЛИЦИ СРБИЈИ

Златко Петровић,
Стручњак у области заштите података о личности, са дугогодишњим искуством у Служби Повереника за информације од јавног значаја и заштиту података о личности

Издавач
Центар за истраживање јавних политика

Уредници
Бранка Анђелковић
Тања Јакоби

Децембар 2022

Напомена
Објављивање овог приказа подржао је Олаф Палме Центар у Србији. Ставови изнети у овом приказу припадају искључиво ЦЕНТРУ и не представљају нужно став Олаф Палме Центра у Србији.

ОДНОС ПРИМЕНЕ ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ У ОБЛАСТИ РАДА И ЗАПОШЉАВАЊА И ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ У РЕПУБЛИЦИ СРБИЈИ

Златко Петровић

„Вештачка интелигенција (ВИ) односи се на системе који показују разумно, интелигентно, понашање на основу анализе свог окружења и доносе одлуке – са одређеним степеном аутономије – да остваре конкретне циљеве. Системи засновани на вештачкој интелигенцији могу бити базирани искључиво на софтверу и деловати у виртуелном свету (на пример, виртуелни асистенти, софтвери за анализу фотографија, интернет претраживачи, системи за препознавање говора и лица) или могу бити уграђени у уређаје – хардвер (на пример, напредни роботи, аутономна возила, дронови и слично).”[1]

I
ПЛАНСКИ ОКВИР ПРИМЕНЕ ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ НА МЕЂУНАРОДНОМ НИВОУ

Феномен вештачке интелигенције и иновације које су засноване на оваквој технологији све више добијају на значају у савременом свету. Потенцијали које вештачка интелигенција има су неслућених размера, управо због широког поља примене, укрштања различитих сфера људског деловања, утицаја на свакодневни живот и стварања нових, додатих вредности које омогућују ефективнију употребу ресурса, бржу обраду информација и стицање нових знања, те рационалнији утрошак времена и квалитетније услуге. Технологија заснована на употреби вештачке интелигенције утиче на информације на које корисници наилазе приликом употребе интернета, тако што предвиђа који садржај их занима, омогућује тренутно превођење текста на стране језике, прикупља и анализира податке да би персонализовала рекламне садржаје, користи се у управљању људским ресурсима, за предикцију и лечење болести. Вештачка интелигенција утиче на многе сегменте савременог друштва и живота појединаца, често и без нашег знања и разумевања овог сложеног процеса. Све облике употребе вештачке интелигенције и њене домете тешко је сагледати, а ова врста технологије ће тек долазити до изражаја у годинама које следе.

Употреба вештачке интелигенције, међутим, производи и низ проблема и изазова у осмишљавању и примени иновативних решења, а који се заснивају на упитној спремности појединца и друштва да у пуној мери разумеју и прихвате иновације и последице примене оваквих решења, те питањима етичке и правне природе. Из овог разлога, неопходно је са више аспеката размотрити примену вештачке интелигенције, како са становишта образовања и научног развоја, економских бенефита, доступности и ефикасности услуга и производа заснованих на вештачкој интелигенцији, тако и из перспективе људских права,

[1] A definition of AI: Main capabilities and scientific disciplines, Independent High-Level Expert Group on Artificial Intelligence set up by the European Commission, 2018. https://digital-strategy.ec.europa.eu/en/library/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines

етичности примене ових решења и њихове безбедности. Развој нових технолошких решења стога мора бити пропраћен осмишљеним планским деловањем и одговарајућим нормативним регулисањем употребе вештачке интелигенције.

Један од најзначајнијих изазова у овој области представља заштита података о личности, као фундаментално људско право, које свој пуни значај добија у 21. веку, захваљујући неслућеном развоју интернетских технологија и пословних модела који се заснивају на обради података. У том смислу, третман обраде података о личности мора се сагледавати како у односу на податке које вештачка интелигенција користи за учење, тако и у односу на податке које обрађује као формиран софтверски или хардверски производ у употреби. Суштински, вештачка интелигенција учи из велике количине података, од којих се неки односе управо на људске карактеристике или деловање, из којих препознаје обрасце. Перформансе оваквих производа се побољшавају са све већом количином података који су на располагању, па су у питању огромни скупови података, који омогућавају све боље извршавање задатака, све савршеније превођење текстова на друге језике, све тачније анализирање и предвиђање понашања физичког лица, све безбеднију вожњу у возилима без возача и слично. Вештачка интелигенција је различите облике примене нашла у савременој медицини, али и у управљању људским ресурсима, индустрији забаве, банкарству, трговини. У том смислу, обрада велике количине података о личности, од којих поједини могу бити веома деликатни, стварање нових вредности укрштањем ових података и употреба истих у различите сврхе, ствара извесне сумње и забринутост у погледу приватности лица на која се исти ти подаци односе, могућих облика дискриминације, па чак и угрожавања слободе воље човека.

Почевши од 2017. године, више од 60 држава широм света донело је документе стратешке природе који се односе на развој вештачке интелигенције, а покренуто је и више иницијатива на међународном плану, у које су укључене државе и међународне организације и донето неколико битних планских докумената. Европска комисија објавила је 2018. године стратешки документ под називом „*Вештачка интелигенција за Европу*“ (Artificial Intelligence for Europe) [2], на основу којег је експертска група исте године донела *Етичке смернице за вештачку интелигенцију достојну поверења*[3]. Током 2019. године, усвојене су и објављене Препоруке OECD-а о вештачкој интелигенцији[4], Принципи о вештачкој интелигенцији организације G20[5], док је Светски економски форум издао десет „*Смерница за јавне набавке за вештачку интелигенцију*“[6]. У 2020. години покренута је међународна иницијатива под називом Глобално партнерство за вештачку интелигенцију (The Global Partnership on Artificial Intelligence - GPAI)[7], а у друге иницијативе су укључене и организације попут UNESCO[8], Интерпола и Центра УН за вештачку интелигенцију и роботику (UNICRI)[9].

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0237&from=EN
[3] https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html
[4] https://www.oecd.org/science/forty-two-countries-adopt-new-oecd-principles-on-artificial-intelligence.htm
[5] https://oecd.ai/en/wonk/documents/g20-ai-principles
[6] https://www3.weforum.org/docs/WEF_Guidelines_for_AI_Procurement.pdf
[7] https://gpai.ai/
[8] https://en.unesco.org/artificial-intelligence
[9] https://unicri.it/artificial-intelligence-and-robotics-law-enforcement

На неопходност нормативног регулисања обраде података о личности, у контексту развоја вештачке интелигенције, годинама уназад указује Савет Европе, која међународна организација има кључну историјску улогу у препознавању заштите података о личности као фундаменталног људског права на међународном нивоу. Савет Европе је још 1981. године отворио за потписивање први мултилатерални споразум о заштити података о личности – Конвенцију о заштити лица у односу на аутоматизовану обраду података о личности (108), који међународни документ представља камен темељац у овој области.

У Препоруци 2102 (2017)[10], која се бави односима технолошке конвергенције, вештачке интелигенције и људских права, Парламентарна скупштина Савета Европе са забринутошћу примећује да постаје све теже прилагодити законодавство брзини којом се наука и технологија развијају и наглашава да очување људског достојанства у 21. веку изискује нове облике управљања, отворених и иформисаних јавних расправа, нових законодавних механизама, те успостављања међународне сарадње, како би се на ефективан начин одговорило на изазове новог доба. Овај документ је нагласио неопходност модернизације Конвенције 108, потребе јачања транспарентности и одговорности у обради података о личности, заједничког оквира за стандарде који се примењују када судови користе вештачку интелигенцију, задржавања контроле над радом машина, те признавања нових права у области заштите података о личности, међу којима се истиче право лица да се успротиви аутоматизованим обрадама података, попут профилисања и праћења. Додатни протокол уз Конвенцију 108 (тзв. Конвенција 108+) накнадно је и отворен за потписивање 2018. године, чиме је овај међународни споразум модернизован.

Комитет министара Савета Европе у Декларацији о манипулативним могућностима алгоритамских процеса[11] из 2019. године указује на потенцијале обраде података у виртуелном окружењу, који се користе за машинско учење, као што су предвиђање или обликовање личних избора, измена токова информација и бихејвиорално експериментисање, што даље води у категоризацију лица, која може довести до различитих форми дискриминације. Доносиоци овог документа недвосмислено указују да овакве обраде података о личности поткопавају демократско уређење и воде угрожавању темељних вредности Савета Европе и Конвенције за заштиту људских права и основних слобода. На овом месту указује се и на савремена сазнања о могућностима употребе оваквих технологија за манипулисање не само економским, већ и политичким и социјалним изборима грађана, очигледно указујући на рецентни случај британске компаније Cambridge Analytica и њихове улоге у изборним кампањама. Овај документ садржи низ мера које би државе чланице требале да предузму, у циљу обуздавања неконтролисаних алгоритамских манипулација, као што су подизање свести у јавности, развој истраживања у овој области, јачање регулаторног оквира, спровођење јавних расправа, укључивање средстава јавног информисања у дебату итд.

[10] https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=23726&lang=en
[11] https://search.coe.int/cm/pages/result_details.aspx?ObjectId=090000168092dd4b

Такође, Комитет министара Савета Европе објавио је 2020. године и детаљне Препоруке државама чланицама о утицајима алгоритамских система на људска права[12], у којима се наглашава да примена вештачке интелигенције мора подразумевати и основна начела владавине права, попут законитости, транспарентности, предвидљивости и одговорности у примени оваквих система.

II
НОРМАТИВНИ ОКВИР ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ И ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ НА МЕЂУНАРОДНОМ НИВОУ

Развој интернетских технологија и вештачке интелигенције у првој и другој деценији 21. века, учинио је аутоматизовану обраду података о личности неизбежном у практично сваком аспекту људског деловања, што је иницирало и потребу за доношењем нове нормативе у овој области у Европској унији. Директива 95/46/ЕЗ о заштити лица у вези са обрадом података о личности из 1995. године показала се неефикасним правним инструментом у растућем интернетском окружењу, што је захтевало доношење прописа који би имао непосредну и директну примену у државама чланицама Европске уније, те могао да одговори на изазове новог времена.

Процес доношења уредбе која би заменила ову директиву трајао је од 2012. до 2016. године, са рекордним бројем амандмана, што све указује да се ради о пропису о којем се највише расправљало у европским институцијама, од њиховог оснивања до данас. Општа уредба о заштити података, позната као GDPR, подигла је на веома висок ниво обавезе руковалаца и обрађивача података о личности, истовремено обезбеђујући палету нових права лицима на која се подаци односе, од којих поједина управо долазе до изражаја у интернетском окружењу, а чији је основни смисао да се физичким лицима врати контрола над сопственим подацима. Поред права на приступ подацима, права на исправку и брисање, призната су права попут права на преносивост података, права на заборав и права на ограничавање обраде. Између осталих права, посебно долази до изражаја могућност дата физичком лицу да се успротиви аутоматизованом доношењу појединачних одлука, што укључује и профилисање, као специфичан облик аутоматизоване обраде података о личности који се користи да би се оценило одређено својство личности, посебно у циљу анализе или предвиђања радног учинка физичког лица, његовог економског положаја, здравственог стања, личних склоности, интереса, поузданости, понашања, локације или кретања.

Радна група 29 (саветодавно тело ЕУ, формирано на основу Директиве 95/46), у својим Смерницама WP251rev.01[13], донетим поводом почетка примене GDPR, управо је нагласила везу између растућег утицаја вештачке интелигенције и аутоматизованог доношења појединачних одлука и профилисања. У овом документу наводи се да је напредак у технологији и могућности анализе великих података (Big data), вештачке интелигенције и машинског учења олакшао креирање профила и доношење

[12] https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154
[13] https://ec.europa.eu/newsroom/article29/items/612053

аутоматизованих одлука, са потенцијалом за значајан утицај на права и слободе појединца, као и да широка доступност личних података на интернету и са уређаја Интернета ствари (Internet of Things), и способност проналажења корелација и стварања веза, може омогућити утврђивање, анализирање и предвиђање аспеката личности појединца или његовог понашања, интересовања и навика. Ове детаљне Смернице потврђене су и од стране актуелног Европског одбора за заштиту података (EDPB).

Један од најважнијих аспеката GDPR јесте афирмисање начела уграђене и подразумеване приватности (privacy by design & privacy by default), као што су свођење обраде података о личности на најмању могућу меру, псеудонимизација података о личности у најкраћем року по остварењу сврхе обраде, транспарентност у вези са функцијама и обрадом података о личности, омогућавање лицу на које се подаци односе да прати обраду података, омогућавање руковаоцу да ствара и унапређује безбедносне карактеристике обраде. GDPR наглашава да, приликом развијања, осмишљавања, бирања и коришћења апликација, услуга и производа који су засновани на обради података о личности или обрађују податке о личности како би испунили свој задатак, произвођаче производа, услуга и апликација треба подстицати да узму у обзир право на заштиту података приликом развијања и осмишљавања таквих производа, услуга и апликација и да, узимајући у обзир најновији технолошки развој, обезбеде да руковаоци и обрађивачи буду у могућности да испуне своје обавезе у вези са заштитом података. Такође, посебно се напомиње да ова начела треба узети у обзир и у контексту јавних позива за достављање понуда. Обавезе руковалаца поводом поштовања начела уграђене и подразумеване приватности су да, узимајући у обзир најновији технолошки развој, трошкове спровођења и природу, обим, контекст и сврхе обраде, као и ризике за права и слободе физичких лица који произилазе из обраде података, примењују одговарајуће техничке и организационе мере, попут псеудонимизације. Руковалац треба да примењује мере којима се обезбеђује да се подразумевана обрада врши само над подацима о личности који су неопходни за конкретну сврху обраде. Као елемент за доказивање усклађености са захтевима уграђене и подразумеване приватности, може да служи одобрени механизам сертификације, у складу са GDPR.

Обраду у области рада GDPR сврстава у посебне врсте обрада података о личности. У складу са GDPR, државе чланице могу законом или колективним уговорима предвидети прецизнија правила са циљем обезбеђивања заштите права и слобода у вези с обрадом података о личности у контексту запослења, посебно за потребе запошљавања, извршења уговора о раду, укључујући и извршавање обавеза прописаних законом или колективним уговорима, за потребе управљања, планирања и организације рада, једнакости и различитости на радном месту, здравља и безбедности на раду, заштите имовине послодавца или клијента и за потребе индивидуалног или колективног остваривања и уживања права и погодности из радног односа, као и за потребе престанка радног односа. Та правила укључују прикладне и посебне мере за заштиту људског достојанства лица на које се подаци односе и његових легитимних интереса и основних права, посебно у вези са транспарентношћу обраде, пренос података о личности унутар групе повезаних друштава или групе предузећа која обављају заједничку привредну делатност, као и система праћења на радном месту.

Међутим, најважнији нормативни акт у области вештачке интелигенције у Европској унији тек треба да буде донет у будућности. Предлог уредбе Европског парламента и Савета којом се регулише вештачка интелигенција (Artificial Intelligence Act)[14] објављен је априла 2021. године. Овај пропис ће несумњиво представљати следећу велику ствар у ЕУ, како са становишта развоја технологије, тако и са становишта заштите људских права.

Предлог овог документа, након детаљне Преамбуле, садржи бројне референце на област заштите података о личности, било да се ради о улози европских и националних институција у овој области, усклађености са начелима GDPR или конкретним обавезама корисника високоризичних система вештачке интелигенције да израђују процене утицаја на заштиту података о личности, у складу са истим прописом. Овај пропис најпре прописује забрану употребе система вештачке интелигенције на начин који сублиминалним порукама утиче на људску свест, искоришћава рањивост појединих група због њихових година, физичких или менталних недостатака, категорише појединце или групе у циљу предвиђања њихове поузданости и других особина или врши масовни биометријски надзор од стране полиције у реалном времену. Предлог уредбе даље дефинише услове употребе високоризичних система вештачке интелигенције, те обавезе добављача и корисника оваквих система, стандарде, сертификацију, регистрацију и низ других мера.

У складу са овим документом, системи вештачке интелигенције који се користе у запошљавању, управљању радницима и приступу самозапошљавању, посебно за регрутацију и селекцију лица, за доношење одлука о унапређењу и престанку рада и за расподелу задатака, праћење или оцењивање особа у уговорним односима у вези са послом, такође требају бити класификовани као високоризични, јер ови системи могу значајно утицати на будуће изгледе за каријеру и средства за живот особа чије податке обрађују. Предлог уредбе дефинише да се високоризичним системима вештачке интелигенције сматрају системи у области запошљавања, управљања радницима и приступа самозапошљавању: (а) Системи вештачке интелигенције који су намењени да се користе за регрутовање или селекцију физичких лица, посебно за оглашавање слободних радних места, скрининг или филтрирање пријава на конкурсима за запослење, оцењивање кандидата током интервјуа или тестирања; (б) Системи намењени за доношење одлука о унапређењу и раскиду уговорног односа у вези са послом, за расподелу задатака и за праћење и процену учинка и понашања особа у таквим односима.

Занимљиво је да су највише запрећене казне у предлогу овог прописа за 50% више у односу на пословично високе казне прописане у GDPR, па се крећу чак до 30 милиона евра или до 6% глобалног годишњег прихода компаније. Попут GDPR, овај правни документ би у будућности могао постати светски релевантан, како због своје територијалне надлежности, која се протеже и на добављаче и кориснике производа вештачке интелигенције лоциране ван територије ЕУ, уколико се исти производи користе у ЕУ, тако и због свог напредног садржаја, који би у будућности могао да прерасте у глобални стандард.

[14] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

У домену радних односа, значајан документ представља и Предлог директиве о побољшању услова за рад на платформама[15], који су децембра 2021. године објавили Европска комисија и Савет. Овај документ, између осталог, разматра и могућности запослених да се служе својим правом на поштену и транспарентну обраду, те да се успротиве аутоматизованом доношењу појединачних одлука, реферишући се на решења GDPR и Предлога уредбе којом се регулише вештачка интелигенција. Овим документом се констатује да нова права у вези са алгоритамским управљањем у раду платформе могу довести до побољшања услова рада за преко 28 милиона људи (и радника и самозапослених) и веће транспарентности у коришћењу вештачке интелигенције на радном месту.

III
ПЛАНСКИ ОКВИР ПРИМЕНЕ ВЕШТАЧКЕ ИНТЕЛИГЕНЦИЈЕ У РЕПУБЛИЦИ СРБИЈИ

Препознајући све важнији утицај вештачке интелигенције на развој информационих технологија, економију и опште друштвене односе, те пратећи светске трендове, Влада Републике Србије донела је крајем 2019. године Стратегију развоја вештачке интелигенције за период 2020-2025. („Сл. гласник РС“, број 96/19). Овај плански документ представља потврду политичких приоритета у области дигитализације и наглашава усклађеност са Европском иницијативом о вештачкој интелигенцији („*Вештачка интелигенција за Европу*“) из 2018. године. Стратегија афирмише управо вредности које су изнете у овој иницијативи, кроз обезбеђивање поверења и одговорности у вези са развојем и употребом вештачке интелигенције. У том смислу, на истоветан начин се препознају потенцијали вештачке интелигенције, њен значај за развој науке и привреде, али и потребе за одговарајућим етичким и правним оквиром, посебно из перспективе заштите података о личности, те посебно права лица у односу на овакве облике аутоматизоване обраде података.

Овај документ је донет благовремено и веома је важан за третман вештачке интелигенције у нашој земљи, посебно имајући у виду спремност за њену употребу. Према Индексу спремности за вештачку интелигенцију, Република Србија је 2019. године била на 58. месту од 194. државе[16], да би већ у Извештају за 2021. годину[17] заузела 52. место. Посебно треба напоменути да је крајем новембра 2022. године Република Србија приступила Глобалном партнерству за вештачку интелигенцију (The Global Partnership on Artificial Intelligence (GPAI).

Из Стратегије се може закључити да су вршена прелиминарна истраживања примене вештачке интелигенције у Републици Србији, која је, због експанзије ИТ сектора, присутна у области образовања и науке, као и у привреди, али је донет закључак да није забележена њена употреба у јавном сектору. У контексту њене будуће употребе у јавном

[15] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A0762%3AFIN
[16] https://www.oxfordinsights.com/ai-readiness2019
[17] https://www.oxfordinsights.com/government-ai-readiness-index2021

сектору, наглашава се да примењена решења морају бити поуздана и пружити заштиту података корисника, као и вишеканални приступ, односно могућност интеракције са службеником приликом пружања услуге. Посебно се истичу могућности које вештачка интелигенција отвара у области здравства и саобраћајне инфраструктуре.

Након указивања на разлоге доношења, те потенцијале за економски развој и унапређење ефикасности, Стратегија наглашава и пратеће изазове и ризике које развој вештачке интелигенције носи, а то су, пре свега, заштита података о личности, ризик дискриминације која може проистећи из података који се обрађују, као и недостатак транспарентности. Као кључни ресурс у развијању вештачке интелигенције, у Стратегији се наводе огромне количине података, те повећане рачунарске могућности обраде, чија комбинација омогућује развој машинског учења, у циљу предвиђања будућег понашања на основу обраде великих скупова података.

У домену рада, Стратегија разматра унапређење продуктивности рада употребом вештачке интелигенције, повећање продуктивности радне снаге у Републици Србији на основу унапређивања наставних садржаја у овој области, могућности брзог повећања запослености стручно оспособљеног кадра, раст извоза ИТ софтвера и услуга и економски положај ИТ радне снаге, отварање нових радних места. Међутим, Стратегија не разматра посебно ризике примене вештачке интелигенције у области запошљавања и радних односа.

Стратегија апострофира Закон о заштити података о личности („Сл. гласник РС“, број 87/18) као кључни пропис повезан са облашћу вештачке интелигенције, за који се наводи да је усклађен са GDPR. За исти закон наведено је да његова практична примена у Републици Србији носи изазове, те да би било корисно сачинити прецизнија упутства за његову примену, што би допринело смањењу ризика произвољног тумачења овог прописа и охрабрило приватни сектор у развоју вештачке интелигенције.

У циљу обезбеђења етичке и безбедне примене вештачке интелигенције, овај плански документ предвиђа увођење превентивних механизама, који ће омогућити одговоран развој вештачке интелигенције и начине верификације да су ови системи у складу са стандардима. У том смислу, Стратегија утврђује Посебан циљ 5: Етична и безбедна примена вештачке интелигенције, у саставу којег је Мера 5.1: Заштита *личних података* [sic][18] у области вештачке интелигенције. У овој Мери се наглашава да је потребно осигурати заштиту података о личности током развоја решења заснованих на вештачкој интелигенцији (података који се користе за „тренирање”) и података који се накнадно обрађују путем већ истренираног система који користи нове податке.

Како би се омогућила сигурност и осигурало поверење јавности да су развијена решења у складу са прописима који регулишу заштиту података о личности фокус се ставља на две активности: 1) развој плана активности и имплементација успостављања практичног дијаграма неопходних корака које је потребно спровести везано за заштиту личних података у развоју решења заснованих на вештачкој интелигенцији; 2)

[18] Устав Републике Србије не познаје заштиту *личних података*, већ заштиту *података о личности* – прим.аут.

сертификација производа и решења заснованих на вештачкој интелигенцији, како би се осигурала заштита података о личности и усклађеност са интернационалним етичким стандардима.

Као институције одговорне за праћење и контролу реализације Мере 5.1, Стратегија опредељује Министарство правде, *Повереника за заштиту података о личности* [sic][19] и Канцеларију за информационе технологије и електронску управу.

Стратегија опредељује као индикаторе за ову меру:

1) Број компанија које примењују *по корак шему приликом развоја вештачке интелигенције како би се обезбедила заштита података о личности* [sic] (почетна вредност: 0; циљна вредност за крај 2022. године: 25; циљна вредност за крај 2025. године: 50);
2) Број *сертификованих решења заснованим на машинском учењу за која се потврђује да су у складу са прописима у области заштите података о личности и интернационално прихваћеним етичким стандардима* (почетна вредност: 0; циљна вредност за крај 2022. године: 25; циљна вредност за крај 2025. године: 50).

Приликом оваквог дефинисања индикатора изостала су ближа објашњења шта тачно представљају (корак) *по корак шема приликом развоја вештачке интелигенције како би се обезбедила заштита података о личности* и *сертификована решења заснована на машинском учењу за која се потврђује да су у складу са прописима у области заштите података о личности и интернационално прихваћеним етичким стандардима*. У том смислу корисно је било прецизирати ове изразе, како би се избегла произвољна тумачења.

Као анализу ефеката на друштво, Стратегија наводи да ће наведена Мера омогућити грађанима заштиту њихових података о личности, те да ће се поступком сертификације у друштву изградити поверење да су одређена решења заснована на вештачкој интелигенцији у складу са законом и интернационалним стандардима.

Стратегија у Мери 5.2 (Заштита од дискриминације код примене вештачке интелигенције) разматра аутоматизацију одлучивања у контексту дискриминаторних критеријума према мањинским групама, те права на транспарентност приликом примене алгоритма, а посебно у односу на карактеристике лица, од којих понеке спадају у категорију посебних врста података о личности (национална припадност, етничко порекло, језик, пол, родни идентитет, инвалидитет, старосна доб, сексуална оријентација, брачни статус или друга лична својства). У том смислу, предвиђа се успостављање етичких смерница, измене закона који регулише забрану дискриминације тако да буде препозната дискриминација до које долази услед примене вештачке интелигенције и одржавање обука за превенцију дискриминације у машинском учењу.

[19] Назив ове институције је погрешно наведен у Стратегији, јер је прави назив Повереник за информације од јавног значаја и заштиту података о личности – прим.аут.

У Мери 5.3 (Обезбеђивање одговорног развоја вештачке интелигенције у складу са међународним етичким стандардима), као индикатор за крај 2022. године опредељују се усвојене етичке смернице за развој и употребу вештачке интелигенције, по угледу на Етичке смернице за вештачку интелигенцију достојну поверења, спроведена анализа усаглашености постојеће регулативе са међународном праксом и препоруке за даље усаглашавање и доношење нове на основу етичких смерница, те успостављен јавни дијалог за изградњу поверења у вештачку интелигенцију и идентификовање нових прилика за развој појединца и целог друштва.

Стратегија прописује доношење два акциона плана, од којих је први, који се односи на период 2020-2022. године донет у јуну 2020. године. Овај трогодишњи акциони план као институцију одговорну за праћење и контролу реализације наведеног Посебног циља 5. (Етична и безбедна примена вештачке интелигенције) опредељује Министарство просвете, науке и технолошког развоја, док је Министарство правде одговорно за праћење и контролу реализације Мере 5.1 (Заштита личних података у области вештачке интелигенције). У оквиру реализације ове Мере предвиђене су активности на развоју методологије за примену стандарда заштите података о личности у области вештачке интелигенције, те примени стандарда заштите података о личности у софтверским решењима заснованим на вештачкој интелигенцији, које заједнички спроводе Министарство просвете, науке и технолошког развоја, Канцеларија за ИТ и еУправу и Министарство правде. Међутим, иако је у Стратегији задужен за праћење и контролу реализације ове Мере, Повереник за информације од јавног значаја и заштиту података о личности се не помиње у наведеном Акционом плану.

У контексту извршења Мере 5.3, сачињен је Нацрт Етичких смерница за развој, примену и употребу поуздане и одговорне ВИ, у вези са којим је 30.11.2022. године упућен Јавни позив од стране Министарства науке, технолошког развоја и иновација за коментаре и сугестије. Овај документ садржи део „*Приватност, заштита података о личности и управљање подацима*“ са упитником из ове области и препорукама.

Иако је Стратегијом и Акционим планом (Мера 5.1) планирано да на крају 2022. године у Републици Србији буде 25 компанија које примењују „(*корак) по корак шему приликом развоја вештачке интелигенције како би се обезбедила заштита података о личности*“, још увек у јавности није доступна информација да ли је предметна шема израђена и каква је форма исте. Такође, иако је за крај 2022. године предвиђено постојање 25 „*сертификованих решења заснованим на машинском учењу за која се потврђује да су у складу са прописима у области заштите података о личности и интернационално прихваћеним етичким стандардима*“, овај план до данас није реализован.

Разлози неиспуњавања планираних циљних вредности су вишеструки, али би њихове заједничке именитеље требало потражити у нормативном регулисању заштите података о личности у Републици Србији.

IV
НОРМАТИВНО РЕГУЛИСАЊЕ ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ У РЕПУБЛИЦИ СРБИЈИ И ЊЕГОВ ОДНОС СА ПРОПИСИМА У ОБЛАСТИ

РАДА И ЗАПОШЉАВАЊА

Основни разлог доношења новог Закона о заштити података о личности била је међународно прихваћена обавеза Републике Србије из ратификованог Споразума о стабилизацији и придруживању између Европских заједница и њихових држава чланица, са једне стране, и Републике Србије, са друге стране ("Сл. гласник РС - Међународни уговори", бр. 83/2008), да усклади своје законодавство које се односи на заштиту личних података [sic] са комунитарним законодавством и осталим европским и међународним прописима о приватности (члан 81). На овом месту поново треба указати на извесну терминолошку неконзистентност, насталу у превођењу овог документа на српски језик, јер Устав Републике Србије у члану 42. гарантује заштиту података о личности, а не заштиту личних података.

Ова међународно прихваћена обавеза није била извршена доношењем Закона о заштити података о личности из 2008. године (који је био у примени до 21. августа 2019. године), с обзиром да овај закон, према оцени европских органа, није био усклађен са тада важећом Директивом 95/46.

Доношење GDPR 2016. године, те почетак његове примене, две године касније, поставили су нове захтеве за изменама српског Закона о заштити података о личности. Методологија израде новог Закона о заштити података о личности ("Сл .гласник РС", број 87/2018), садржана у комбиновању превода одредби GDPR и Директиве 680/2016 (тзв. Law Enforcement Directive или „Полицијска директива“), уз потпуни изостанак одредби преамбула ова два документа, довела су до законских решења која нису у потпуности дефинисана, нити усклађена са другим прописима Републике Србије, што у пракси доводи до изостанка правне сигурности, како за руковаоце, тако и за лица на која се подаци односе. На овом месту важно је напоменути да су експерти Европске комисије, још у мају 2019. године, сачинили Студију у којој су упућене бројне критике на текст српског Закона о заштити података о личности, те указано на низ потенцијалних проблема у његовој примени.[20]

Члан 2. став 2. Закона о заштити података о личности прописује да одредбе посебних закона којима се уређује обрада података о личности морају бити у складу са овим законом, док члан 100. истог закона прописује да ће се одредбе других закона, које се односе на обраду података о личности, ускладити са одредбама овог закона до краја 2020. године. Међутим, ни после скоро две године од истека овог рока сви ови прописи нису усклађени са Законом о заштити података о личности.

Као пример нормативне неусклађености управо се намећу закони који уређују рад и запошљавање, као категорије у којима производи и услуге засновани на вештачкој интелигенцији долазе до изражаја. Обраду за потребе рада и запошљавања српски законодавац, по угледу на GDPR, сврстава у категорију посебних случајева обраде, и исту регулише у члану 91. на следећи начин:

[20] www.poverenik.rs/sr/саопштења/3136-студија-европске-комисије-о-процени-усклађености-закона-о-заштити-података-о-личности-са-прописима-еу-указује-на-потребу-унапређења-овог-закона.html

„*На обраду у области рада и запошљавања примењују се одредбе закона којима се уређује рад и запошљавање и колективни уговори, уз примену одредби овог закона. (став 1) Ако закон који уређује рад и запошљавање или колективни уговор садрже одредбе о заштити података о личности, морају се прописати и посебне мере заштите достојанства личности, легитимних интереса и основних права лица на које се подаци односе, посебно у односу на транспарентност обраде, размену података о личности унутар мултинационалне компаније, односно групе привредних субјеката, као и систем надзора у радној средини. (став 2)*“

Закон о раду ("Сл. гласник РС", бр. 24/2005, 61/2005, 54/2009, 32/2013, 75/2014, 13/2017 - одлука УС, 113/2017 и 95/2018 - аутентично тумачење), као основни нормативни акт у области рада, чија је супсидијарна примена прописана и другим законима који регулишу исту област (нпр. Закон о државним службеницима и Закон о запосленима у аутономним покрајинама и јединицама локалне самоправе) регулише у члану 83. заштиту личних података [sic]. Усклађивање овог закона са цитираним чланом Закона о заштити података о личности подразумевало је да је исти закон морао прописати „*посебне мере заштите достојанства личности, легитимних интереса и основних права лица на које се подаци односе, посебно у односу на транспарентност обраде, размену података о личности унутар мултинационалне компаније, односно групе привредних субјеката, као и систем надзора у радној средини*“, а што није учињено, како у овом , тако и у другим прописима.

Идентична је ситуација и са Законом о запошљавању и осигурању за случај незапослености ("Сл. гласник РС", бр. 36/2009, 88/2010, 38/2015, 113/2017 и 113/2017 - др. закон), Закону о безбедности и здрављу на раду ("Сл. гласник РС", бр. 101/2005, 91/2015 и 113/2017 - др. закон), док увидом у више колективних уговора закључених у Републици Србији, није утврђено да исти посебно регулишу заштиту података о личности.

Заштиту података о личности у области рада третирао је Повереник за информације од јавног значаја и заштиту података о личности у својој Одлуци о листи врста радњи обраде података о личности за које се мора извршити процена утицаја на заштиту података о личности и тражити мишљење Повереника ("Сл. гласник РС", број 45/2019 и 112/2020). У истом акту прописано је да се иста процена мора вршити у случају обраде биометријских података у циљу јединствене идентификације запослених од стране послодавца и у другим случајевима обраде података о личности запослених од стране послодавца употребом апликација или система за праћење њиховог рада, кретања, комуникације и сл. Наведени случајеви обраде података о личности управо могу бити примери примене вештачке интелигенције у области рада.

На овом месту важно је констатовати и недовољну активност синдиката на пољу заштите података о личности, иако исто може бити предмет колективног преговарања и увођења нових обрада података о личности радника од стране послодаваца. Тако нпр, спровођење процене утицаја на заштиту података о личности, у складу са чланом 54. став 11. Закона о заштити података о личности подразумева да, према потреби, руковалац од лица на које се подаци односе или њихових представника тражи мишљење о радњама

обраде које намерава да врши, не доводећи у питање заштиту пословних или јавних интереса или безбедност радњи обраде.

С обзиром да одредбе закона којима се уређују рад и запошљавање нису усклађене са одредбама Закона о заштити података о личности, отвара се простор за правну несигурност на овом пољу, релативизовање одредби истог закона, произвољна тумачења и злоупотребе података о личности запослених и кандидата за запослење од стране послодаваца. Управо би јасним нормирањем „*посебних мера заштите достојанства личности, легитимних интереса и основних права лица на које се подаци односе, посебно у односу на транспарентност обраде, размену података о личности унутар мултинационалне компаније, односно групе привредних субјеката, као и систем надзора у радној средини*“ биле отклоњене многе сумње у области обраде података о личности у радно-правним односима, где вештачка интелигенција може имати уплив.

V
СЕРТИФИКАЦИЈА У ОБЛАСТИ ЗАШТИТЕ ПОДАТАКА О ЛИЧНОСТИ У РЕПУБЛИЦИ СРБИЈИ

Улога сертификата у Закону о заштити података о личности, као и у GDPR, је вишеструка. Руковалац може користити издати сертификат као доказ да предузима одговарајуће техничке, организационе и кадровске мере и да обраду врши у складу са законом. Такође, издати сертификат служи и као доказ да изабрани обрађивач примењује одговарајуће организационе, техничке и кадровске мере. Надаље, издати сертификат служи и као механизам обезбеђивања одговарајућих мера заштите приликом преноса података о личности у другу државу, на део њене територије или у један или више сектора одређених делатности у тој држави или у међународну организацију за коју није утврђено постојање примереног нивоа заштите, у складу са законом, под условом да је лицу на које се подаци односе обезбеђена остваривост његових права и делотворна правна заштита.

У складу са законом, Повереник подстиче издавање сертификата за заштиту података о личности и одговарајућих жигова и ознака и прописује критеријуме за сертификацију, спроводи периодично преиспитивање сертификата, прописује и објављује критеријуме за акредитацију сертификационог тела и проверава испуњеност услова за сертификацију. Повереник је овлашћен да укине сертификат или да наложи сертификационом телу укидање сертификата који је издат, да наложи сертификационом телу да одбије издавање сертификата ако нису испуњени услови за његово издавање, као и да издаје сертификате и прописује критеријуме за издавање сертификата.

Закон прописује да се у циљу доказивања поштовања одредби овог закона од стране руковаоца и обрађивача, могу установити добровољни и транспарентни поступци издавања сертификата о заштити података о личности, са одговарајућим жиговима и ознакама за заштиту података. Сертификат, у складу са законом, издаје сертификационо тело или Повереник, на период који не може бити дужи од три године и који се може обновити, на основу критеријума које прописује Повереник. Издати сертификат се може и укинути уколико руковалац или обрађивач престану да испуњавају исте критеријуме.

Повереник прописује критеријуме за акредитацију сертификационог тела, а сертификационо тело може бити акредитовано, у складу са законом којим се уређује акредитација, само ако испуни услове прописане законом. Акредитација се издаје сертификационом телу на период до пет година и може се обновити, али и укинути.

Употреба сертификата издатих од сертификованог тела друге државе у Републици Србији је могућа, уколико је исти издат у складу са потврђеним међународним споразумом. Ако је сертификационо тело које је спровело сертификацију акредитовано од стране националног тела друге државе, које је са Акредитационим телом Србије потписало споразум којим се међусобно признаје еквивалентност система акредитације у обиму који је одређен потписаним споразумом, у Републици Србији се могу прихватити сертификати тог сертификационог тела, без поновног спровођења поступка сертификације.

Иако ова законска решења представљају модификацију чл. 42. и 43. GDPR, неопходно је имати у виду да је механизам сертификације у самој Европској унији још увек у зачетку. Јануара 2020. године објављен је Документ о процедури за одобрење критеријума за сертификацију од стране Европског одбора за заштиту података, која за резултат има заједничку сертификацију, Европски печат заштите података (European Data Protection Seal)[21]. Први критеријуми за сертификацију у складу са GDPR усвојени су тек крајем јуна 2022. године, од стране националног органа за заштиту података Луксембурга (GDPR – CARPA).[22] Европски одбор за заштиту података је током септембра 2022. издао друго Мишљење о критеријумима за сертификацију European Privacy Seal (EuroPriSe), који се односе само на обрађиваче, [23] а током октобра Мишљење о критеријумима за сертификацију Europrivacy.[24]

Поред нејасне улоге Повереника у поступку акредитације сертификационих тела у Закону о заштити података о личности, на коју је својевремено указивала и Европска комисија у својој Студији, као претходно питање стратешки постављеним циљевима, намеће се и чињеница да Повереник још увек није прописао критеријуме за сертификацију, нити критеријуме за акредитацију сертификационог тела. У контексту неразвијене праксе по истом питању у Европској унији, поставља се питање изводљивости остварења постављеног циља у овом тренутку. Механизам усвајања критеријума за сертификацију у Европској унији подразумева процедуру, у коју су укључени национални органи за заштиту података и Европски одбор за заштиту података, као међународно стручно тело. За разлику од ове процедуре, Закон о заштити података о личности само прописује надлежност Повереника да пропише наведене две врсте критеријума.

ЗАКЉУЧАК

[21] https://edpb.europa.eu/our-work-tools/our-documents/procedure/edpb-document-procedure-approval-certification-criteria-edpb_en
[22] https://edpb.europa.eu/news/national-news/2022/cnpd-adopts-certification-mechanism-gdpr-carpa_en
[23] https://edpb.europa.eu/news/news/2022/new-edpb-opinion-certification-criteria-0_en
[24] https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282022-europrivacy-criteria-certification_en

Стратегија развоја вештачке интелигенције за период 2020-2025. године представља плански документ који је било неопходно донети, у контексту свеприсутне употребе технологије засноване на вештачкој интелигенцији и глобално убрзане планске и нормативне делатности у овој области. Машинско учење и употреба алгоритама у одлучивању доносе низ користи и унапређења у свакодневном животу грађана Републике Србије, али могу довести и до нежељених последица, угрожавања њиховог права на приватност и дискриминације. Овај плански документ треба да представља стратешки одговор на постојеће и будуће изазове које ова технологија доноси, како са становишта развоја науке и привреде, пружања услуга у јавном сектору, тако и са становишта заштите основних људских права. Управо из наведених разлога, дефинисању појединих мера је требало приступити уз детаљније сагледавање стања и прецизније дефинисање циљних вредности.

Развој вештачке интелигенције у Републици Србији и њена примена у области рада и запошљавања нераскидиво је везана са низом нерешених питања у области заштите података о личности. Стратегија развоја вештачке интелигенције за период 2020-2025. године несумњиво је потврдила да се највећи изазови управо налазе у овој области, али је на исте изазове одговорила постављањем појединих циљева који су се, у овом тренутку, показали као неостварив.

Израда Етичких смерница за развој, примену и употребу поуздане и одговорне ВИ представља корак напред у регулисању ове области, који може послужити као алат за самопроцену приликом развијања производа и услуга заснованих на овој врсти технологије. Из овог разлога важно је препознати смисао и домашај овог документа, посебно због његовог непосредног упућивања на одредбе Закона о заштити података о личности и GDPR, посебно из перспективе начела обраде података о личности, те конкретних обавеза руковалаца.

Неусклађеност Закона о заштити података о личности са другим прописима који уређују обраду података о личности, па и у области рада и запошљавања, представља системски проблем, који се не може игнорисати. У недостатку системских решења у области заштите података о личности у Републици Србији, отварају се широке могућности за неконтролисану употребу софтверских и хардверских иновација за обраду података запослених и кандидата за запослење, која може довести до угрожавања њихове приватности и достојанства и проузроковати разне облике дискриминације. Из овог разлога неопходно је предузети стратешки, осмишљен приступ и координисане активности на успостављању хармонизованог правног оквира.

У том смислу, препорука је да се у што краћем року обезбеди пуна примена Закона о заштити података о личности, кроз његове измене и допуне, те накнадно доношење подзаконске регулативе у области сертификације, уз консултацију актуелне европске праксе у овој области. Такође, неопходно је ускладити све прописе који уређују обраду података о личности са Законом о заштити података о личности, што је и истим законом прописано. Будући стратешки документи у области заштите података о личности треба да узму у обзир све наведено. У нормативи која регулише рад и запошљавање потребно је прописати „*посебне мере заштите достојанства личности, легитимних интереса и*

основних права лица на које се подаци односе, посебно у односу на транспарентност обраде, размену података о личности унутар мултинационалне компаније, односно групе привредних субјеката, као и систем надзора у радној средини“.

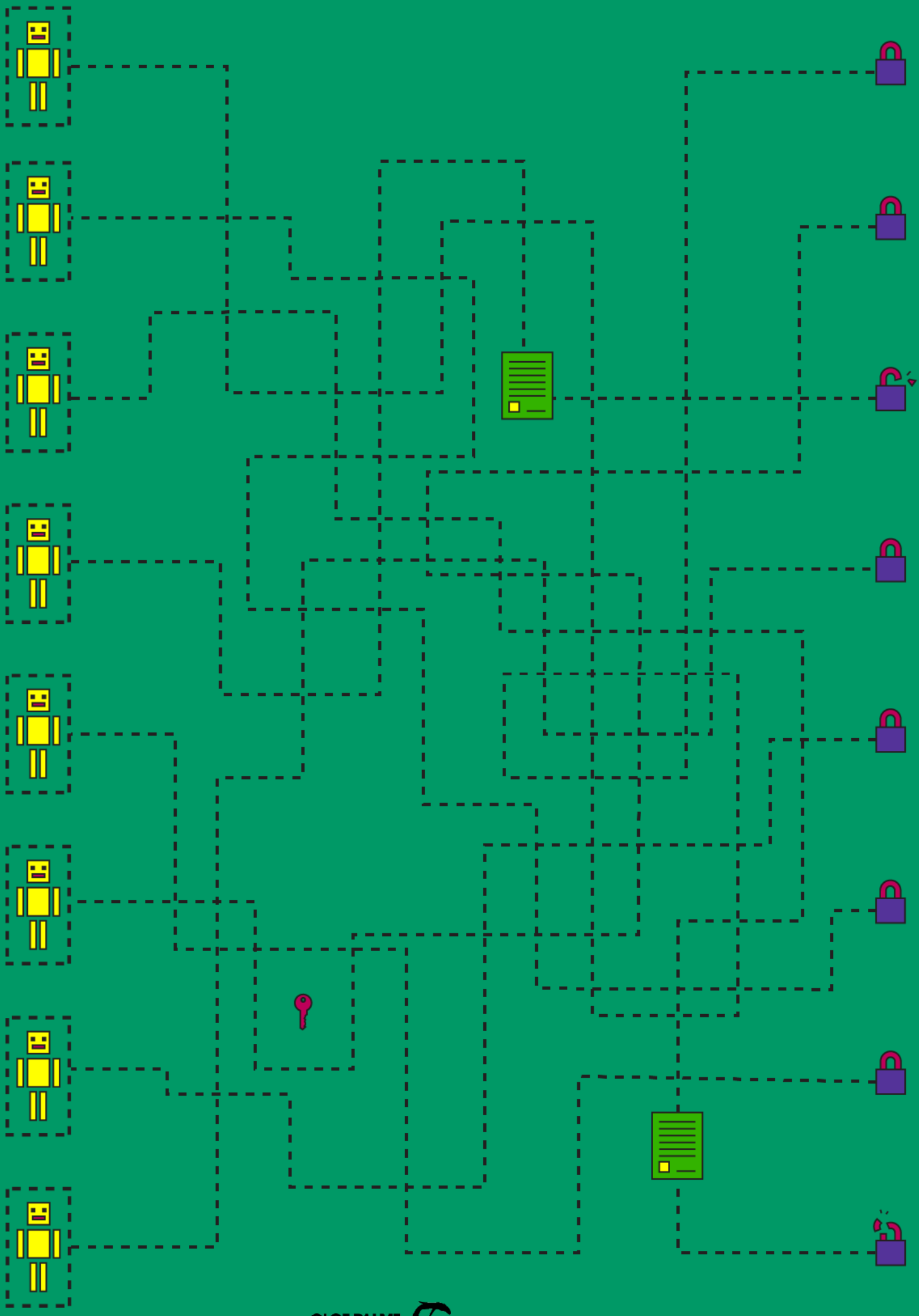
Такође, препорука је да се континуирано спроводе активности на едукацији из области заштите података о личности субјеката који се баве развојем вештачке интелигенције у Републици Србији, те јачање капацитета лица за заштиту података о личности и успостављање мреже професионалаца у овој области.

Посебно препоручујемо укључивање синдиката, као организација за заштиту права радника, у овај процес, имајући у виду њихове капацитете, те чињеницу да заштита података о личности није посебно била предмет колективног преговарања, према нашим сазнањима. Управо недостајуће одредбе о *„посебним мерама заштите достојанства личности, легитимних интереса и основних права лица на које се подаци односе, посебно у односу на транспарентност обраде, размену података о личности унутар мултинационалне компаније, односно групе привредних субјеката, као и систем надзора у радној средини“* би знатно утицале на радно-правни положај радника.

Препорука је да се, у складу са европским нормативним стремљењима, правно унапреди рад на платформама, као нови облик радног ангажовања, где вештачка интелигенција има значајан уплив.

Остваривање ових препорука јесте услов како би грађани могли у пуној мери да остваре своје право на заштиту података о личности, посебно у радном окружењу, које је све више изложено аутоматизованој обради њихових података о личности.

01.12.2022. године


OLOF PALME
INTERNATIONAL
CENTER
Sverige