Финансирано од Европска Унија

ЕУ со ТЕБЕ

ЦЕНТАР ЗА ПРАВНИ ИСТРАЖУВАЊА И АНАЛИЗИ
CENTER FOR LEGAL RESEARCH AND ANALYSIS

МЗМП

ДОКУМЕНТ ЗА ЈАВНИ ПОЛИТИКИ

КОРИСТЕЊЕ АЛГОРИТМИ И ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА (AI) ВО ПРАВОСУДСТВОТО – СО ПОСЕБЕН ОСВРТ НА ПРАВОТО ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ И ПРИВАТНОСТА

КОРИСТЕЊЕ НА АЛГОРИТМИ И ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА (AI) ВО ПРАВОСУДСТВОТО – СО ПОСЕБЕН ОСВРТ НА ПРАВОТО ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ И ПРИВАТНОСТА

Издавач:
Македонско здружение на млади правници
Центар за правни истражувања и анализи

За издавачот:
Бојана Божиновска Силјановска, Претседателка на МЗМП
Лидија Стојкова Зафировска, Претседателка на ЦПИА

Автор:
Мануела Станоевска Стоилковска

Редакција:
Милена Јосифовска, ЦПИА
Сара Марковска, ЦПИА
Маја Атанасова, МЗМП

Лектура:
Дејан Василевски

Графички дизајн:
Релатив

Оваа публикација е изработена во рамките на проектот „**Ефикасна правда за заштита на основните слободи и правото на приватност во онлајн-просторот**“, финансиран од Европската унија. Содржината на публикацијата е единствена одговорност на авторот и на никаков начин не може да се смета дека ги одразува гледиштата на Европската унија.

СОДРЖИНА

ПРЕДГОВОР

Овој документ за јавни политики е подготвен во рамките на проектот: „Ефикасна правда за заштита на основните слободи и правото на приватност во онлајн просторот“, финансиран од Европската унија и имплементиран од Центарот за правни истражувања и анализи (ЦПИА) и Македонско здружение на млади правници (МЗМП). Цел на проектот е да се зајакнат капацитетите на судството и јавното обвинителство во ефикасна заштита на приватноста на граѓаните, како и другите права и основни слободи засегнати од новите технологии во онлајн просторот во согласност со правото и стандардите на ЕУ.

Целта на овој документ за јавни политики е да обезбеди сеопфатен и стратешки пристап за решавање на клучните предизвици за Користење на алгоритми и вештачка интелигенција (AI) во правосудството – со посебен осврт на правото за заштита на личните податоци и приватноста.

Преку овој документ, се настојува да се идентификуваат и анализираат главните проблеми кои бараат интервенција, да се дефинираат приоритетите и да се предложат конкретни решенија кои ќе придонесат за унапредување на политиките за користење на алгоритми и вештачка интелигенција (AI) во правосудството – со посебен осврт на правото за заштита на личните податоци и приватноста. Посебен акцент се става на инклузивноста во пристапот, каде што заклучоците и препораките ќе бидат заеднички потврдени преку активна дебата со претставници на сите засегнати институции. Ова ќе осигури дека различните перспективи и интереси се земени предвид, создавајќи сеопфатни и балансирани политики.

Со имплементација на предложените мерки, се очекува да се постигне значителен напредок во справувањето со идентификуваните проблеми и да се создадат услови за континуирано подобрување на јавните политики и услуги во областа на користење на алгоритми и вештачка интелигенција (AI) во правосудството – со посебен осврт на правото за заштита на личните податоци и приватноста.

МЕТОДОЛОГИЈА

При изготвувањето на овој документ користени се методски и емпириски истражувања. За прибирањето на податоците за цели на изработка на анализата беа применети основните методи на сознание, а особено: анализа, синтеза, индукција, класификација, специјализација и генерализација.

Употребата на алгоритми и вештачка интелигенција во правосудството во овој документ е анализирана примарно низ призмата на заштитата на основните права, заштитата на личните податоци и приватноста, имајќи ги предвид прописите за заштита на личните податоци во РС Македонија, Европската регулатива за заштита на личните податоци, релевантните документи на Европскиот борд за заштита на личните податоци (European Board for Data Protection – EDPB), Европскиот парламент, Советот на Европа и други релевантни институции. Но, исто така, во овој документ се разгледува и етичкиот аспект на употребата на алгоритми и вештачка интелигенција во правосудството и почитувањето на човековите права.

Воедно, преку холистички пристап се анализирани и предностите, ризиците и предизвиците што ги носи употребата на алгоритми и вештачка интелигенција кај сите чинители на системот на правосудството, што на крајот имплицира со препораки и заклучок.

ВОВЕД

Човекот е суштество кое лесно се навикнува на комфор, лесно ги прифаќа новините што му овозможуваат полесно живеење, технологиите што му го олеснуваат функционирањето, притоа брзо или побавно откажувајќи се од старите правила.

Развојот на технологијата и дигитализацијата неоспорно го олеснуваат секојдневното функционирање на човекот. Но, човекот е суштество кое на моменти ја заборава границата на живеење во дигиталниот свет и битисувањето во вистинскиот живот.

Со користењето интернет и мобилни телефони, со секое инсталирање на нова апликација, вмрежување на социјална мрежа, креирање профил на платформа за симнување филмови, музика, размена на професионални искуства, купување преку онлајн-продавница, користење на електронско банкарство, закажување онлајн-термин за здравствена услуга, човекот се откажува од некој дел од неговата приватност. Цената на живеењето во дигиталниот свет ја плаќа приватноста, а валутата се личните податоци.

Употребата на новите интернет-технологии го олеснува човековото живеење, но рака под рака со употребата на современите технологии секогаш оди и нивната злоупотреба. Злоупотребата на технологиите за политичка пропаганда, терористички напади, детска порнографија, финансиски измами... тропа на вратите од нашите домови или веќе е внатре?

Развојот на новите технологии во живеењето на луѓето ја донесоа и вештачката интелигенција. Вештачката интелигенција ни овозможи поглед во иднината – со прикажување на наша фотографија на интернет ни покажува како ќе изгледаме по 10, 20, 30 години; ни даде можност да слушнеме како познатата Мона Лиза на Да Винчи зборува и пее; слушнавме како музичките ѕвезди ги пеат композициите на други ѕвезди; го слушнавме Доналд Трамп како зборува на теми несвојствени за неговите политички ставови (без првично да се посомневаме дека можеби говори вештачката интелигенција); ѝ се заблагодаривме на вештачката интелигенција за новата песна на „Битлс“ по пауза од 1995 година... Покрај забавниот аспект, вештачката интелигенција ни овозможи полесно справување со одредени работни задачи – генерирање статистики, правење презентации, генерирање текстови, класификација на симптоми и болести... секако, притоа користејќи/обработувајќи зададени податоци.

Но, дали и како вештачката интелигенција ќе помогне во „делењето правда“?

Дали и на кој начин користењето алгоритми и вештачката интелигенција може да помогне во правосудството? Кои се ризиците и предизвиците?

Дали е можно да се зачува приватноста, да се заштитат личните податоци, да се запазат начелата на обработка на лични податоци, да се овозможат правата на субјектите на личните податоци при користењето алгоритми и вештачка интелигенција во правосудството?

Дали при користење на вештачката интелигенција во правосудството ќе се почитуваат човековите права?

Дали користењето алгоритми и вештачка интелигенција ќе го подобрат функционирањето на правосудниот систем?

Целта на овој документ е да даде осврт на овие прашања, имајќи ги предвид правосудниот систем, законодавството, досегашната практика и развојот на технологиите, а притоа да се детектираат предизвиците, ризиците и можните решенија и препораки во однос на користењето алгоритми и вештачка интелигенција во правосудството.

Веројатно доколку овие прашања ѝ ги поставиме на вештачката интелигенција, одговорот ќе биде „ДА“. Но, колку и да може вештачката интелигенција „да ја предвидува иднината“, точните одговори ќе ги даде времето, особено што правдата, моралноста, етиката се неразделно поврзани со човековото битисување, однесување и расудување. Времето ќе покаже дали вештачката интелигенција ќе насобере доволно човечка интелигенција за да може поправедно од човекот да донесува одлуки и да „дели правда“. И за крај на почетниот вовед во овој документ, ќе ги поставам и прашањата:

Дали човечката интелигенција е на доволно високо ниво за да може да создаде алгоритми и вештачка интелигенција што ќе креираат предвидлива правда?

Дали вештачката интелигенција ќе создаде судии, адвокати и обвинители кои ќе бидат поправедни?

1. ПРАВОТО НА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ И ПРАВОСУДНИОТ СИСТЕМ ВО РС МАКЕДОНИЈА

Со Уставот на РС Македонија[1] како основни слободи и права на човекот и граѓанинот се гарантираат сигурноста и тајноста на личните податоци, односно на граѓаните им се гарантира заштита од повреда на личниот интегритет што произлегува од регистрирањето информации за нив преку обработка на податоците, како и почитување и заштита на приватноста на неговиот личен и семеен живот, на достоинството и угледот.

Понатаму, со Законот за заштита на личните податоци[2] се уредува заштитата на личните податоци и правото на приватност во врска со обработката на личните податоци, а особено начелата поврзани со обработката на личните податоци, правата на субјектот на личните податоци, положбата на контролорот и обработувачот, преносот на личните податоци во други држави, основањето, статусот и надлежностите на Агенцијата за заштита на личните податоци, посебните операции на обработка на личните податоци, правните средства и одговорноста при обработката на личните податоците, супервизијата над заштита на личните податоци, како и прекршоците и прекршочната постапка во оваа област и тој се применува на целосно или делумно автоматизирана обработка на личните податоци и на друга обработка на личните податоци што се дел од постојна збирка на лични податоци или се наменети да бидат дел од збирка на лични податоци.

Со овој закон целосно е транспонирана Регулативата (ЕУ) 2016/679 на Европскиот парламент и на Советот на ЕУ (General Data Protection Regulation – GDPR), регулатива со којашто, пак, е укината Директивата 95/46/ЕЗ, која беше транспонирана со претходниот Закон за заштита на личните податоци[3] од 2005 година.[4] Секое физичко лице (субјект на лични податоци) има право да поднесе барање до Агенцијата за заштита на личните податоци доколку смета дека обработката на неговите лични податоци ги прекршува одредбите од овој закон, притоа не доведувајќи ги во прашање кои било други управни или судски средства за правна заштита, а Агенцијата како самостоен и независен државен орган е надлежна да врши надзор над законитоста на преземените активности при обработката на личните податоци на територијата на РС Македонија, како и заштита на темелните права и слободи на физичките лица во однос на обработката на нивните лични податоци. Освен правото на поднесување барање до Агенцијата од страна на физичките лица кога сметаат дека обработката на нивните лични податоци ги прекршува одредбите од овој закон, овој закон овозможува и ефективна судска заштита на физичките лица кога сметаат дека се повредени нивните права утврдени со овој закон, како резултат на обработката на лични податоци спротивно од овој закон, која можат да ја остварат со поднесување тужба до надлежниот суд согласно со законот.

1 Устав на Република Северна Македонија („Службен весник на Република Македонија“, бр. 52/1991).

2 Закон за заштита на личните податоци („Службен весник на РС Македонија“, бр. 42/20 и 294/21); Закон за заштита на личните податоци („Службен весник на Република Македонија“, бр. 7/05, 103/08, 124/10, 135/11, 43/14, 153/15, 99/16 и 64/18).

3 Закон за заштита на личните податоци („Службен весник на Република Македонија“, бр. 7/05, 103/08, 124/10, 135/11, 43/14, 153/15, 99/16 и 64/18).

4 Исто така, ратификувана е и Конвенцијата за заштита на лица во однос на автоматска обработка на лични податоци, Дополнителниот протокол кон Конвенцијата за заштита на поединци во поглед на автоматска обработка на лични податоци, во врска со надзорните тела и прекуграничниот пренос на лични податоци, како и Протоколот за измена на Конвенцијата за заштита на лица во однос на автоматска обработка на лични податоци, со што законодавството на РС Македонија се усогласи со инструментите за заштита на личните податоци на Советот на Европа.

Судската власт[5] во РС Македонија ја вршат судовите, кои се самостојни и независни државни органи и своите одлуки ги засноваат врз основа на Уставот, законите и меѓународните договори ратификувани во согласност со Уставот. Пред судовите се заштитуваат слободите и правата на човекот и граѓанинот.

Со Законот за јавното обвинителство[6] се основа јавното обвинителство како единствен и самостоен државен орган, кој ги гони сторителите на кривични дела и на други казниви дела утврдени со закон и врши и други работи утврдени со законот.

Со Законот за адвокатурата[7] се уредува обезбедувањето на правна помош[8] од страна на адвокатурата на физички и правни лица во остварувањето и заштитата на нивните права и врз интересите засновани во законот во постапката пред судовите и државните органи. При остварувањето на адвокатската дејност, адвокатот се раководи исклучиво од интересите на странката што ги заштитува на најдобар начин со законски средства.

Секако, покрај судовите, обвинителствата и адвокатите, клучните чинители во правосудниот систем се и: Министерството за правда, Судскиот совет, Советот на јавните обвинители, Управата за извршување на санкции, Академијата за судии и јавни обвинители, Нотарската комора, Комората на извршители, Адвокатската комора и медијаторите.

Имајќи предвид дека заштитата на личните податоци (сигурноста и тајноста на личните податоци) е уставно загарантирано право, неговата заштита, освен од Агенцијата за заштита на личните податоци, се спроведува и од чинителите на правосудниот систем. Имено, по однос на одлуките донесени од страна на Агенцијата, секое физичко и правно лице има право на ефективна судска заштита против правно-обврзувачката одлука на Агенцијата што се однесува на него. Практично, судот има двојна улога при заштитата на личните податоци, каде што, од една страна, има надлежност да одлучи во случаите каде што физичките лица кои сметаат дека се повредени нивните права утврдени со Законот за заштита на личните податоци, како резултат на обработката на лични податоци спротивно од Законот за заштита на личните податоци, при што поднеле тужба до надлежниот суд, а од друга страна судот се јавува како „коректор“ или ја потврдува одлуката (решението) на Агенцијата за заштита на личните податоци во случаите каде што е поднесена тужба против одлуката (решението) на Агенцијата за заштита на личите податоци.

Исто така, во Кривичниот законик[9] во член 149 е утврдено и кривичното дело: „Злоупотреба на лични податоци“[10], а воедно посредно или непосредно со остварувањето на правото на заштита на личните

5 Закон за судовите („Службен весник на Република Македонија“, бр. 58/2006, 62/2006, 35/2008, 150/2010, 83/2018 и 198/2018 и „Службен весник на Република Северна Македонија“, бр. 96/2019).

6 Закон за јавното обвинителство („Службен весник на Република Северна Македонија“, бр. 42/20).

7 Закон за адвокатурата („Службен весник на Република Северна Македонија“, бр. 199/2023).

8 Правната помош се состои во давање на правни совети, застапување во водење преговори, давање правна помош во деловен протокол, составување исправи за правни дела, составување договори за основање, партнерство, соработка и слични акти во врска со основањето или работењето на деловните субјекти, составување поднесоци во судски и други постапки, застапување на странките пред судовите, државните органи, органите на единиците на локалната самоуправа и други правни и физички лица, одбрана на осомничени и обвинети лица и вршење на други работи на правна помош.

9 Кривичен законик („Службен весник на Република Македонија“, бр. 37/96, 80/99, 4/2002, 43/03, 19/04, 81/05, 60/06, 73/06, 7/08, 139/08, 114/09, 51/11, 135/11, 185/11, 142/12, 166/12, 55/13, 82/13, 14/14, 27/14, 28/14, 41/14, 115/14, 132/14, 160/14, 199/14, 196/15, 226/15, 97/17 и 248/18 и „Службен весник на Република Северна Македонија“, бр. 36/23 и 188/23).

10 (1) Тој што спротивно на условите утврдени со закон без согласност на граѓанинот прибира, обработува или користи негови лични податоци, ќе се казни со парична казна или со затвор до една година. (2) Со казна од став 1 се казнува тој што ќе навлезе во компјутерски информатички систем на лични податоци со намера користејќи ги за себе или за друг да оствари некаква корист или на друг да му нанесе некаква штета.

податоци и заштита на приватноста се поврзани и други кривични дела во Кривичниот законик: Нарушување на неповредливоста на домот (член 145), Противзаконито вршење претрес (член 146), Повреда на тајноста на писма или други пратки (член 147), Неовластено објавување на лични записи (член 148), Спречување на пристап кон јавен информатички систем (член 149-а), Неовластено откривање тајна (член 150), Неовластено прислушкување и тонско снимање (член 151), Неовластено снимање (член 152)... каде што одреден сегмент од кривичното дело опфаќа и обработка на лични податоци.

1.1. ДИГИТАЛИЗАЦИЈА НА ПРАВОСУДСТВОТО ВО РС МАКЕДОНИЈА

Последните десетина години сè поинтензивно се разговара од страна на сите актери во општеството за дигитализација на правосудството во РС Македонија. Ова говори дека свесноста за регулирање и поттикнување на дигиталните процеси во правосудството се зголемува од година в година. Се подготвуваат, изготвени се и/или донесени неколку документи на оваа тема или поврзани со оваа тема: Националната стратегијата за кибербезбедност 2023-2027; Националната ИКТ-стратегија на Република Северна Македонија 2023-2027 година; Стратегијата за информатичко-комуникациска технологија во правосудството за 2019-2024 година (ревидирана стратегија), Националната AI-стратегија[11], Концептот за дигитална трансформација на општеството[12]...

Еден од приоритетите на Европската комисија[13] е постигнување дигитализација на правосудството, при што оваа важна цел треба да се постигне како дел од новиот притисок за европска демократија и во согласност со политичкиот приоритет на Европа што одговара на дигиталната ера (во моментов судските постапки – особено во прекугранични ситуации – сè уште се одвиваат главно на хартија и се засноваат на традиционални канали за пренос. Оваа состојба не обезбедува современ пристап до правдата во средина што сè повеќе е дигитализирана и е полезна за граѓаните и бизнисите). Кога зборуваме за употреба на користење алгоритми и системи базирани на вештачка интелигенција наменети за користење во правосудството, неопходно е да ја детектираме постојната состојба на дигитализација на правосудството, бидејќи таа претставува почетен чекор за да може да се планира користење алгоритми и системи базирани на вештачка интелигенција. Согласно податоците од Стратегија за информатичко-комуникациска технологија во правосудството за 2019-2024 година[14] на Министерството за правда, во правосудството се користат или се во фаза на доградба и стартување одредени дигитализирачки решенија, при што дигиталната трансформација на правосудниот сектор во РС Македонија преминува од почетна фаза/ниво во средно ниво. Дигиталната трансформација најмногу е сосредоточена на дизајн на нови иновативни дигитални решенија и механизми, отворени податоци, обезбедување повеќе е-услуги и сл., а употребата на напредни електронски алатки во судството е следниот чекор во дигитализацијата на правосудството.

Дигитализацијата и употребата на системи базирани на вештачка интелигенција се партнери во процесот на дигитална трансформација на правосудството, при што вештачката интелигенција е клучниот двигател на дигиталната трансформација, овозможувајќи автоматизирано извршување

11 https://fitr.mk
12 https://vlada.mk/
13 https://commission.europa.eu/
14 https://www.pravda.gov.mk/

на задачите и трансформирање на аналогните процеси, додека вештачката интелигенција се сосредоточува на интелигентни системи и технологии за понатамошно оптимизирање на процесите, вклучувајќи употреба на алгоритми и машинско учење што традиционално би барало човечка интелигенција (на пример, извршување задачи за препознавање говор, препознавање слики, предлагање решенија и сл.). Без оглед на брзината со која државата се движи кон дигитализација на правосудството, паралелно во светот со галопирачки чекори се развиваат системи што користат алгоритми и вештачка интелигенција, кои порано или подоцна ќе бидат имплементирани и во нашето правосудство.

2. ЧОВЕЧКА ИНТЕЛИГЕНЦИЈА НАСПРОТИ ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА (ВИ)

2.1. ШТО ОПФАЌА ПОИМОТ „ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА“?

„Вештачката интелигенција“ (ВИ)[15] е интелигенција претставена од машини и софтвер и е гранка од компјутерската наука што развива машини и софтвер со интелигенција. Најголемите истражувања како и објавените трудови за ВИ таа ја дефинираат како проучување и дизајн на интелигентен агент, каде што под интелигентен агент се подразбира систем способен за перципирање на околината и преземање активности што му ги максимираат шансите за успех.

„Вештачка интелигенција“[16] значи систем заснован на машина што може за даден сет цели дефинирани од човекот, да прави предвидувања, препораки или одлуки што влијаат на реалните или на виртуелните средини.

Според дефиницијата предвидена во Регулативата за вештачка интелигенција на Европскиот парламент (прва Регулатива за вештачка интелигенција)[17]: Вештачката интелигенција е брзоразвивачко семејство на технологии што може и веќе придонесува за широк спектар на економски, еколошки, културолошки и општествени придобивки, доколку се развие во согласност со релевантните општи правни и етички принципи во согласност со Повелбата и вредностите на кои е основана Унијата.

Во Резолуцијата на Европскиот парламент од 20 октомври 2020 година со препораки до Комисијата за рамка на етички аспекти на вештачката интелигенција, роботиката и сродните технологии [2020/2012(INL)][18], се дефинирани следните поими:

- **„Вештачка интелигенција“** значи систем што претставува или е базиран на софтвер или вграден во хардверски уреди, кој покажува интелигентно однесување преку (меѓу другото) собирање, обработка, анализа и интерпретација на неговата околина и со преземање активности, со одреден степен на автономија, за постигнување конкретни цели;
- **„Автономија“** значи систем на вештачка интелигенција што работи со интерпретација на одредени влезни информации и користење збир на однапред одредени инструкции, без да биде ограничен на таквите инструкции, и покрај тоа што однесувањето на системот е ограничено и насочено кон исполнување на целта што му била дадена и други релевантни избори за дизајн направени од неговиот развивач;
- **„Поврзани технологии“** значи технологии што овозможуваат софтверот да контролира со делумна или целосна автономија физички или виртуелен процес, технологии способни за откривање на биометриски, генетски или други податоци и технологии што копираат или на друг начин користат човечки особини;

15 https://mk.wikipedia.org
16 https://www.state.gov/artificial-intelligence/
17 ЕУ ВИ акт: https://www.europarl.europa.eu
18 European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies [2020/2012(INL)].

- **„Висок ризик“** значи значителен ризик предизвикан од развојот, распоредувањето и употребата на вештачката интелигенција, роботиката и поврзаните технологии за да предизвика повреда или штета на поединци/физички лица или општество, што ги прекршува основните права и правилата за безбедност, како што е пропишано во правото на ЕУ, имајќи ја предвид нивната специфична употреба или цел, областа каде што се развиваат, каде што се распоредени или користат и сериозноста на повредата или штетата што може да се очекува да се случи;
- **„Развој“** значи конструкција и дизајн на алгоритми, пишување и дизајн на софтвер или собирање, складирање и управување со податоци со цел создавање или обука на вештачка интелигенција, роботика и сродни технологии или со цел да се создаде нова апликација за постојна вештачка интелигенција, роботика и сродни технологии;
- **„Развивач/создавач“** значи секое физичко или правно лице кое донесува одлуки што го одредуваат и го контролираат текот или начинот на развојот на вештачката интелигенција, роботиката и сродните технологии.

Според Принципите на Организацијата за економска соработка и развој (ОЕЦД) за вештачка интелигенција што беа усвоени во мај 2019 година од земјите-членки кои ја одобрија Препораката на Советот на ОЕЦД за вештачка интелигенција[19], како и според Рамковната конвенција на Советот на Европа за вештачка интелигенција и човекови права, демократија и владеење на правото[20], „Систем за вештачка интелигенција“ е систем заснован на машина што може за даден сет на човечки дефинирани експлицитни или имплицитни цели да донесе заклучок, од влезните податоци што ги добива, како и да генерира резултати, како што се: правење предвидувања, содржина, препораки или одлуки што можат да влијаат на физичките реални или виртуелни средини. Различни системи за вештачка интелигенција се дизајнирани да работат со различни нивоа на автономија и приспособливост по распоредувањето.

Како научна дисциплина, вештачката интелигенција вклучува неколку пристапи и техники, на пример машинско учење, машинско расудување (што вклучува планирање, распоредување, знаење, претставување и расудување, пребарување и оптимизација) и роботика (што вклучува контрола, перцепција, сензори и актуатори, како и интеграција на сите други техники во киберфизичките системи).[21]

19 https://oecd.ai/
20 Committee on Artificial Intelligence (CAI), Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, 17.05.2024 година.
21 https://www.europarl.europa.eu

2.2. ШТО ПРЕТСТАВУВА АЛГОРИТАМ?

Предвидувачките алгоритми се очекува да го рационализираат процесот на донесување одлуки со сумирање на сите релевантни информации на поефикасен начин отколку што е во состојба да направи човечкиот мозок.

„Алгоритам“[22] е конечна низа на формални правила (логички операции и инструкции) што овозможува да се добие резултат од првичното внесување информации. Оваа низа може да биде дел од автоматизиран процес на извршување и да се базира на модели дизајнирани преку машинско учење. Алгоритамскиот систем за донесување одлуки може да се дефинира како компјутерски процес што донесува одлуки самостојно или го поддржува човечкото одлучување.

„Машинското учење (ML)“ овозможува да се конструира математички модел од податоци, инкорпорирање на голем број променливи што не се однапред познати. Параметрите се конфигурираат постепено во текот на фазата на учење, која користи збирки на податоци за обука, за пронаоѓање и класификација на врски. Различните методи на машинско учењето се избираат од страна на развивачите во зависност од природата на задачите што треба да бидат завршени (групирање). Овие методи обично се класифицираат во три категории: (човечко) надгледувано учење, учење без надзор и зајакнато учење. Овие три категории групираат различни методи, вклучително и нервни мрежи, длабоко учење итн.

„Предикативна правда“ е анализа на големи количества судски одлуки со вештачки разузнавачки технологии со цел да се направат предвидувања за исходот на одредени видови специјализирани спорови (на пример, надоместоци за технолошки вишок).

22 https://rm.coe.int/

2.3. КАКО ФУНКЦИОНИРА ВЕШТАЧКАТА ИНТЕЛИГЕНЦИЈА?

Имајќи предвид дека вештачката интелигенција се однесува на системи што прикажуваат интелигентно однесување преку анализа на нивната околина и преземање акција со одреден степен на автономија за постигнување на конкретни цели, при што се опфатени многу техники и контексти, потребно е системите што се користат во советодавни улоги да се разликуваат од оние што се однесуваат на сложени алгоритми управувани од податоци што автоматски ги спроведуваат одлуките за поединци/физички лица. Воедно, важно е да се разликуваат аргументите за шпекулативните идни случувања што можеби никогаш нема да се случат од оние за моменталната вештачка интелигенција што веќе влијае на општеството денес.[23]

Првиот бран на раните техники на вештачка интелигенција е познат како „симболична вештачка интелигенција“ или експертски системи. Човечки експерти креирале прецизни процедури засновани на правила – познати како „алгоритми“ што компјутерот може да ги следи, чекор по чекор, и да одлучи како интелигентно да одговори на дадена ситуација. Овде, варијантата на пристап е случај каде што нејасната логика овозможува различни нивоа на доверба за некоја ситуација, што е корисно за доловување на интуитивно знаење, така што алгоритамот може да донесува добри одлуки наспроти широки и неизвесни променливи што комуницираат една со друга. Симболичката вештачка интелигенција е најприменлива во ограничени средини што не се менуваат многу со текот на времето, каде што правилата се строги, а променливите се недвосмислени и квантитативни.

Вториот бран на вештачка интелигенција (машинско учење – ML и вештачка интелигенција управувана од податоци) се состои од понови пристапи „водени од податоци“ што се развиле брзо во текот на последните две децении и во голема мера се одговорни за актуелното оживување на вештачката интелигенција. Во овој бран се автоматизира процесот на учење на алгоритмите, заобиколувајќи ги човечките експерти на вештачка интелигенција од првиот бран. Оваа вештачка интелигенција функционира како вештачки невронски мрежи (ANN) што се инспирирани од функционалноста на мозокот. Влезните информации се преведуваат во сигнали што се пренесуваат низ мрежа на вештачки неврони за да генерираат излезни информации што се интерпретирани како одговори на влезните информации. Длабокото учење се однесува на вештачки невронски мрежи (ANN) со неколку слоја. Машинско учење (ML) се однесува на трансформација на мрежата така што овие излезни информации се сметаат за корисни или интелигентни одговори на влезните информации.

Третиот бран на вештачка интелигенција („силна“ или „општа“ вештачка интелигенција) се однесува на „шпекулативни можни идни бранови“ на вештачка интелигенција. Додека во првиот и вториот бран техниките се опишани како „слаба“ или „тесна“ вештачка интелигенција во смисла дека тие можат да се однесуваат интелигентно во специфични задачи, „силна“ или „општа“ вештачка интелигенција се однесува на алгоритми што можат да покажат интелигенција во широк опсег на контексти и проблемски простори. Таквата вештачка „силна“ или „општа“ интелигенција (AGI) не е можна со постојната технологија и ќе бара напредок со менување на парадигмата. Овој бран на вештачка интелигенција би можел да има способност за земање предвид на пошироко контекстуално знаење со цел да се обезбедат попрецизни резултати, а притоа да се користат помали збирки податоци за обучување. Други форми на шпекулативна идна вештачка интелигенција, како што се самообјаснувачка и контекстуална вештачка интелигенција исто така треба да бидат земени предвид и нивното потенцијално влијание и бариери

23 Artificial intelligence: How does it work, why does it matter, and what can we do about it? – Philip Boucher; https://www.europarl.europa.eu/

за имплементација не треба да се потценува. Воедно, како дел од новата генерација на вештачката интелигенција се појавува и „генеративната вештачка интелигенција“ што претставува фундаментална промена на вештачката интелигенција.

Генеративната вештачка интелигенција[24] е тип технологија за вештачка интелигенција што има способност да креира различни типови нови содржини и податоци во многу големи размери, вклучувајќи текст, слики, аудио и синтетички податоци. Брзиот напредок во таканаречените големи јазични модели (LLM) – т.е. модели со милијарди, па дури и трилиони параметри – отвора нова ера во која генеративните модели со вештачка интелигенција можат да пишуваат текст, да сликаат фотореалистични слики, да генерираат содржина преку повеќе видови медиуми, вклучувајќи текст, графика и видео, за неколку секунди.

Можеби овој вид интелигенција, конечно, во блиска иднина ќе го може да го даде одговорот на прашањето поставено во 1950 година од страна на Алан Матисон Тјуринг: **„Дали машините можат да мислат?“**

„Тестот на Тјуринг“[25] е тест првпат предложен од Алан Матисон Тјуринг во 1950 година, а тој е дизајниран да биде врвен експеримент за тоа дали вештачката интелигенција постигнала интелигенција на човечко ниво или не. Концептуално, ако вештачката интелигенција може да го помине тестот, таа има постигнато интелигенција што е еквивалентна или не се разликува од онаа на човекот.[26] Обратна форма на Тјуринговиот тест, која е ширококористена на интернет е тестот CAPTCHA[27], што е наменет за да се утврди дали корисникот е човек или сметач (компјутер).

Тешко е да се каже какво ќе биде влијанието на генеративната вештачка интелигенција во иднина. Но, во моментот, користењето на ваков вид алатки за автоматизирање задачи што ги извршувал човекот, ветува поедноставување на извршувањето на определени задачи што можат да најдат и соодветна примена во правосудството, на пример олеснување на работата на адвокатите во пишувањето договори или пишување пресуди или други правни акти на судиите, каде што говорот на судијата се претвора во текст. Имајќи предвид дека при носењето на одлуките влијаат многу околности, традиционални вредности, важечки прописи, автентични олеснувачки или отежнувачки околности, морални норми, прашање е дали „судија-робот“ – систем со вештачка интелигенција би можел самостојно да носи поисправни одлуки од човек-судија или „адвокат-робот“ би подготвил подобра одбрана од адвокат-човек, а „обвинител-робот“ би изнел поаргументирано обвинение од обвинител-човек?

24 https://www.techtarget.com
25 „Компјутерски машини и интелигенција“, Алан Матисон Тјуринг, 1950 година.
26 Тјурингова проверка (Тјурингов тест) е предлог-проверка на машинската способност да ја покаже интелигенцијата, еквивалентна или што не може да се разликува од онаа на човекот, а која Алан Тјуринг ја опишал во 1950 година во трудот „Компјутерски машини и интелигенција“. Тестот се содржел во тоа што тој се обидел да го дефинира стандардот на машина за да може да се нарече интелигентна. Идејата била човек-испитувач да поставува прашања на сметач и човек сместени во различни соби. Во моментот кога испитувачот нема да може да препознае кој е сметачот, а кој е човекот, тогаш заклучиле дека машината достигнала ниво на човечка интелигенција.
27 https://mk.wikipedia.org/wiki/

3. ЕТИКА НА ВЕШТАЧКАТА ИНТЕЛИГЕНЦИЈА ВО ПРАВОСУДСТВОТО

Во дефиницијата на дигиталниот речник на македонскиот јазик[28], етика е наука за моралот, за моралните принципи и норми и за нивната улога во општествениот и во личниот живот на човекот, т.е. однесување во согласност со нормите и правилата на моралот.

Во Рамката на етичките аспекти на вештачката интелигенција, роботика и поврзани технологии[29] на Европскиот парламент, дефинирани се правила што мораат да се почитуваат при создавањето и примената на системи што користат вештачка интелигенција. При креирањето системи што употребуваат вештачка интелигенција и алгоритми, а се наменети за користење во правосудството, мораат да бидат запазени етичките норми. Впрочем, етиката, правото и моралот отсекогаш ги испреплетувале, повеќе или помалку своите вредности и се темелеле на исти постулати. Имајќи ја предвид важноста на етиката и етичкото постапување во креирањето, создавањето и применувањето системи што користат вештачка интелигенција, а кои би се употребувале во правосудството, во „Европската етичка повелба за употреба на вештачка интелигенција во судските системи и нивната околина“[30], се дефинирани пет основни принципи за употреба на вештачка интелигенција во судските системи и нивната околина:

1. **Принцип на почитување на основните права:**
   Овој принцип подразбира дека при дизајнирањето системи што користат алгоритми за вештачка интелигенција, а се наменети да се користат во правосудството, потребно е да бидеме сигурни дека дизајнот и имплементација на алатките за вештачка интелигенција и услугите што ќе ги остваруваат се компатибилни и целосно усогласени со основните човекови права. Обработката на судските одлуки и податоци мора да служи за јасни цели, во целосна согласност со основните права загарантирани од ЕКЧП[31] и Конвенцијата за заштита на лични податоци 108[32]. Кога алатките за вештачка интелигенција се користат за решавање на определен спор или како алатка за помош при донесување на судски одлуки или за давање насоки на јавноста, од суштинско значење е да постои сигурност дека тие нема да ги поткопаат гаранциите на правото за пристап до судијата и правото на правично судење (еднаквост на оружјата и почитување за контрадикторен процес). Воедно, треба да се користат и со должно почитување на принципите на правилото на правото и

28 http://drmj.eu/

29 Framework of ethical aspects of artificial intelligence, robotics and related technologies – European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies [2020/2012(INL)]: човекоцентрична и вештачка интелигенција создадена од човекот; процена на ризик; безбедносни карактеристики, транспарентност и одговорност; непристрасност и недискриминација; социјална одговорност и родова рамнотежа; заштита на животна средина и одржливост; правила за приватност и биометриско препознавање; добро владеење; почитување на потрошувачите и внатрешниот пазар; правила во безбедноста и одбраната; правила во транспортот, вработувањето, работнички права, дигитални вештини и работното место, образованието и културата.

30 European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment, одобрена од Европската комисија за ефикасност на правдата (CEPEJ), што е иновативно тело за подобрување на квалитетот и ефикасноста на европските судски системи и зајакнување на довербата на корисниците на судот во таквите системи, воспоставени од Комитетот на министри на Советот на Европа.

31 European Convention on Human Rights (ECHR).

32 Convention on the Protection of Personal Data (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108 as amended by the CETS amending protocol No. 223).

независноста на судиите во нивниот процес на одлучување и притоа треба да се даде предност на „етички-по-дизајн“ пристап или пристапи кон почитување на човекови права по дизајн. Ова значи дека токму од дизајнот и учењето во фази, правилата што забрануваат директни или индиректни прекршувања на основните вредности заштитени со конвенциите се целосно интегрирани во системите што користат алгоритми и вештачка интелигенција, а се наменети да се користат во правосудството.

2. Принцип на недискриминација:

Овој принцип подразбира конкретно спречување развој или интензивирање на каква било дискриминација помеѓу поединци или групи поединци при дизајнирањето и примената на системи што користат алгоритми за вештачка интелигенција, а се наменети да се користат во правосудството.

Со оглед на можноста и способноста на методите на вештачката интелигенција при обработката на податоци да ја откријат постојната дискриминација, преку групирање или класификација на податоци што се однесуваат на физички лица или групи на физички лица, јавните и приватните чинители мораат да обезбедат дека методите на креирање и развивање на системите што користат вештачка интелигенција не ја репродуцираат или влошуваат таквата постојна дискриминација и дека не водат до дискриминаторски анализи или употреба на системот за таа цел. Посебна грижа мора да се води и при развојот чекор по чекор, особено кога обработката директно или индиректно се заснова на „чувствителни“ податоци (посебни категории на лични податоци)[33]. Во случај ако во некој од чекорите, т.е. фазите на развивање на системите се идентификува можност за каква било дискриминација, неопходно е да се разгледаат и да се применат корективни мерки за ограничување, односно минимизирање или, доколку е можно, неутрализирање на овие ризици, особено што, со употребата на машинско учење, треба да се поттикнат анализи за борба против таквата дискриминација.

3. Принцип на квалитет и безбедност:

Во однос на обработката на судските одлуки и податоци мораат да се користат проверени, овластени (сертифицирани) извори и податоци со модели елаборирани и конципирани на мултидисциплинарен начин, во безбедна технолошка средина.

Дизајнерите/развивачите на системите кои користат вештачка интелигенција, а се наменети да се користат во правосудството и моделите за машинско учење, треба да бидат способни да користат широка експертиза на релевантни професионалци во правосудниот систем (судии, обвинители, адвокати и др.), истражувачи, односно предавачи од областа на правото и општествените науки (на пример, економисти, социолози, филозофи...), како и експерти за заштита на личните податоци. Формирање на мешовити проектни тимови составени од професионалци од повеќе релевантни области (во различни фази од создавањето) ќе резултира со дизајнирање на функционални модели за машинско учење со вграден мултидисциплинарен пристап. Постојните етички заштитни мерки постојано треба да се споделуваат, надградуваат и пренесуваат помеѓу сите тимови вклучени при дизајнирањето и развивањето на овие модели и системи, заради континуитет и доследност во почитувањето на етичките принципи. Во случаите каде што во

33 Член 4 став (1) точка 13 од Законот за заштита на личните податоци („Службен весник на РС Македонија“, бр. 42/20 и 294/21).

софтвер што имплементира алгоритам за машинско учење се внесуваат податоци врз основа и/или произлезени од судски одлуки, овие податоци треба да доаѓаат од сертифицирани извори и не треба да се менуваат сè додека не се искористат од/за машинското учење. Затоа, мора да биде овозможено целиот процес да може да се следи за да се обезбеди дека не се појавуваат измени, кои ќе ги променат содржината или значењето на одлуката. Создадените модели и алгоритми, исто така, мораат да се чуваат и да се развиваат во безбедни средини, за да се обезбеди интегритет на системите што користат вештачка интелигенција, а се наменети да се користат во правосудството.

4. Принцип на транспарентност, непристрасност и правичност:

Овој принцип подразбира дека при создавањето, развивањето и примената на системите што користат вештачка интелигенција, а се наменети да се користат во правосудството, неопходно е да се постигне рамнотежа меѓу интелектуалната сопственост на одредени методи на обработка, потребата за транспарентност (пред сè, во процесот на дизајнирање), правичност и интелектуален интегритет (приоретизирање на интересите на правдата кога се користат алатки што можат да имаат законски последици или значително можат да влијаат на животот на луѓето). Се препорачува да се користат поразновидни збирки податоци и мултидисциплинарен пристап, како и континуирана ревизија на аспектите, како што се обработката на податоците и начинот на кој е конструиран системот. Секако, овие принципи се однесуваат на целиот дизајн и на оперативниот синџир, како на процесот на селекција, така и на квалитетот и организацијата на податоците што директно влијаат во фазата на учење. Целосната техничка транспарентност (на пример, отворен изворен код и документацијата) понекогаш е ограничена поради заштита на деловните тајни. Системот може да се објасни и јасно на разбирлив јазик (да опише како се произведуваат резултати), на пример, природата на понудените услуги, алатките што биле развиени, перформанси и ризици од грешка. Експертите би можеле да бидат задолжени за сертифицирање и ревизија на методите на обработка или давање совети претходно, а јавните власти би можеле да доделат сертификација и редовно да ја прегледуваат, со цел да се обезбеди неутралност на алгоритмите и непристрасност. За цели на транспарентност, треба да постои можност да бидат достапни клучните подмножества информации за алгоритмите, тие да бидат достапни за јавноста, на пример кои променливи се користат, кои цели на алгоритмите се оптимизирани, кои податоци за обука се користат и просечните вредности и стандардните отстапувања на произведените резултати или количеството и видот на податоци што ги обработува алгоритамот.

5. Принципот „под контрола на корисникот“:

При креирањето и користењето на системите што користат вештачка интелигенција, а се наменети да се користат во правосудството, подразбира сигурност дека корисниците на овие системи се информирани и дека можат да ги контролираат направените избори.

Автономијата на корисниците на овие системи мора да биде испочитувана и да не се ограничува преку употреба на алатките и услугите од вештачка интелигенција. Професионалците во правосудниот систем кои ќе ги користат овие алатки и системи во секој момент треба да имаат можност да ги прегледаат судските одлуки и податоците користени за да се добие резултат и секако да не бидат обврзани задолжително да ги користат добиените резултати, како и да можат да ги вклучат и да ги земат предвид специфичните карактеристики за секој одделен случај. Корисниците на овие системи и алатки мораат да бидат информирани на јасен и разбирлив

јазик дали понуденото решение од алатките за вештачка интелигенција е обврзувачко; да бидат информирани за различните опции што ги имаат на располагање, како и дека имаат право на правен совет и право на пристап до суд. Корисникот, исто така, мора да биде јасно информиран за секое претходно процесирање на случајот со вештачка интелигенција пред или за време на судски процес, при што ќе има право на приговор, така што неговиот случај да може директно да биде сослушан од суд во смисла на член 6 од ЕКЧП.

При носењето одлуки, решенија и мислења во која било област секогаш најголем придонес имаат професионалците од соодветната фела. Дефиницијата на „етиката“ го вклучува моралот, моралните принципи и норми и нивната улога во општествениот и во личниот живот на човекот, како и однесување во согласност со нормите и правилата на моралот. Ако се има предвид дефиницијата за етика, произлегува дека при креирањето на овие системи мораат да се создадат „правила за правилата на однесувањето на човекот, согласно нормите и правилата на моралот“. Системите не знаат што е тоа морал и етичко однесување и тие ќе нудат резултати согласно она што ќе им го „кажат“ нивните креатори/развивачи.

Системите што користат вештачка интелигенција, а се наменети да се користат во правосудството, ќе бидат сетирани согласно етичките принципи на нивните развивачи/дизајнери, а етичките принципи се морална категорија неспоиво поврзана со човекот. Од друга страна, за да се добијат применливи резултати од овие системи, неопходно е при нивното дизајнирање да бидат вклучени професионалци од областа на правосудството кои имаат знаење и искуство и можат да придонесат за подобри и поефикасни системи што користат вештачка интелигенција, а се наменети да се користат во правосудството. При креирањето и развивањето на овие системи мораат да бидат поставени соодветни алгоритми што ќе креираат релевантни резултати, а вештачката интелигенција мора да биде „нахранета“ со големи бази на податоци за да може да понуди соодветни решенија и притоа човекот (судија, адвокат, обвинител) е тој што мора да има можност да одлучи во која мера ќе се потпре на понудените резултати, при што во преден план мора да ги има правдата, човекот и човековите права.

Имајќи го предвид наведеното, неоспорно произлегува дека кога зборуваме за етика во применувањето системи што користат вештачка интелигенција, а се наменети да се користат во правосудството, во преден план се истакнува етичноста на креаторите/дизајнерите/развивачите на овие системи. Неоспорно е дека етички пристап мораат да имаат и оние за кои се наменети овие системи (судиите, адвокатите, обвинителите), но се наметнува прашањето: кој ќе биде судијата кој може да пресуди дали креаторите на системите се или можат да бидат поетични од чинителите на правосудството?

4. ВЛИЈАНИЕ НА ПРАВИЛАТА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ ПРИ РАЗВИВАЊЕ И КОРИСТЕЊЕ АЛГОРИТМИ И ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА ВО ПРАВОСУДСТВОТО

При дизајнирањето, развивањето и користењето системи што користат вештачка интелигенција во правосудството, особено треба да се земе предвид правото за заштита на личните податоци и заштита на приватноста. Секако, оваа констатација во никаков случај не треба да се сфати како некакво правење градација на важноста на човековите права. Поентата на ова констатација се однесува на фактот дека при обезбедување на остварувањето на кое било човеково право, помалку или повеќе е вмешана и обработка на лични податоци. Имено, кога зборуваме за недискриминација, право на еднаквост, заштита на достоинството... сите овие права се однесуваат на лица кои се претходно идентификувани посредно или непосредно обработувајќи нивни податоци. Практично, за да стане збор, на пример, за навреда на честа и угледот или достоинството, всушност физичкото лице чие право е загрозено најпрвин е идентификувано со неговите лични податоци, а потоа се изнесени одредени информации или поведенија со кои се загрозило правото на достоинство, еднаквост, недискриминација...

Во Законот за заштита на личните податоци[34] се дефинирани и следните поими[35]:

- **„Личен податок“** е секоја информација што се однесува на идентификувано физичко лице или физичко лице кое може да се идентификува (субјект на лични податоци), а физичко лице кое може да се идентификува е лице чиј идентитет може да се утврди директно или индиректно, особено врз основа на идентификатор, како што се име и презиме, матичен број на граѓанинот, податоци за локација, идентификатор преку интернет или врз основа на едно или повеќе обележја специфични за неговиот физички, физиолошки, генетски, ментален, економски, културен или социјален идентитет на тоа физичко лице;[36]
- **„Профилирање“** е секоја форма на автоматска обработка на лични податоци, која се состои од користење на лични податоци за оценување на одредени лични аспекти поврзани со физичкото лице, а особено за анализа или предвидување аспекти што се однесуваат на извршување на професионалните обврски на тоа физичко лице, неговата економска состојба, здравје, лични преференции, интереси, доверливост, однесување, локација или движење;

34 Закон за заштита на личните податоци („Службен весник на РС Македонија“, бр. 42/20 и 294/21).

35 „Контролор“ е физичко или правно лице, орган на државната власт, државен орган или правно лице основано од државата за вршење на јавни овластувања, агенција или друго тело, кое самостојно или заедно со други ги утврдува целите и начинот на обработка на личните податоци, а кога целите и начинот на обработка на личните податоци се утврдени со закон, со истиот закон се определуваат контролорот или посебните критериуми за негово определување; „Обработувач на збирка на лични податоци“ е физичко или правно лице, орган на државната власт, државен орган или правно лице основано од државата за вршење на јавни овластувања, агенција или друго тело кое ги обработува личните податоци во име на контролорот.

36 „Посебни категории на лични податоци“ се лични податоци што откриваат расно или етничко потекло, политички ставови, верски или филозофски убедувања или членство во синдикални организации, како и генетски податоци, биометриски податоци, податоци што се однесуваат на здравјето или податоци за сексуалниот живот или сексуалната ориентација на физичкото лице; „Биометриски податоци“ се лични податоци што се добиваат преку специфична техничка обработка на физичките и физиолошките карактеристики на физичкото лице или карактеристики на неговото однесување, а преку кои се овозможува или се потврдува единствената идентификација на физичкото лице.

- **„Псевдонимизација“** е обработка на личните податоци на таков начин што личните податоци веќе не можат да се поврзат со одреден субјект на лични податоци без да се користат дополнителни информации, под услов таквите дополнителни информации да се чуваат одделно и да подлежат на технички и организациски мерки со кои ќе се обезбеди дека личните податоци не се поврзани со идентификувано физичко лице или физичко лице кое може да се идентификува;

Голем број апликации што користат вештачка интелигенција обработуваат лични податоци, од причина што, од една страна, личните податоци што се користат за машинско учење несомнено можат да придонесат за структурирање на подобри алгоритамски модели. Од друга страна, таквите алгоритамски модели можат да придонесат за донесување на подобри одлуки и заклучоци поврзани со физичките лица за кои се користат овие модели. Со користењето на вештачката интелигенција, сите категории на лични податоци можат да бидат искористени за некаква анализа, предвидување на човечкото однесување, автоматско одлучување во сложени ситуации, каде што се нудат повеќе избори, со што се зголемува вредноста на личните податоци.

4.1. НАЧЕЛА ПОВРЗАНИ СО ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

Во Законот за заштита на личните податоци (член 9) се дефинирани и начелата поврзани со обработката на личните податоци:

- **Начело на „законитост, правичност и транспарентност“,**
  според кое личните податоци се: обработуваат согласно со закон, во доволна мера и на транспарентен начин во однос на субјектот на личните податоци.

  Запазувањето на ова начело при дизајнирањето, развивањето и користењето алгоритми и системи базирани на вештачка интелигенција што се наменети за користење во правосудството, подразбира дека овие системи се во функција на остварување права што се гарантирани со законот или таа да се базира на одредбите за законитост на обработката на личните податоци.[37] Сегментот за транспарентност се сосредоточува на концизноста, пристапноста и разбирливоста, при што подразбира дека субјектот на личните податоци или јавноста треба да биде сеопфатно информиран/и за обработката на личните податоци, при што секоја информација мора да биде концизна, лесно достапна и лесно разбирлива, на јасен и разбирлив јазик (дополнително, каде што е соодветно, да се користи и визуализација).[38] Ова начело во контекст на користењето системи што користат вештачка интелигенција, особено мора да биде запазено и во случаите кога за обучување на системот се користат лични податоци, при што информациите на субјектите на личните податоци треба да им бидат дадени/овозможени пред обработката на овие податоци за цели на обука/учење на апликацијата што користи вештачка интелигенција.

37 Член 10 од Законот за заштита на личните податоци („Службен весник на РС Македонија“, бр. 42/20 и бр. 294/21).
38 Член 17 и 18 од Законот за заштита на личните податоци („Службен весник на РС Македонија“, бр. 42/20 и бр. 294/21).

- **Според начелото на „ограничување на целите“:**
  Личните податоци се собираат за конкретни, јасни и легитимни цели и нема да се обработуваат на начин што не е во согласност со тие цели. Понатамошната обработка за цели на архивирање од јавен интерес, за научни или за историски истражувања или за статистички цели, нема да се смета дека не е во согласност со првичните цели за кои се собрани личните податоци.

  Сосредоточувањето на начелото на „ограничување на целите“ е на поврзаноста на целта со основата за обработка на личните податоци. Според ова начело, личните податоци можат да се обработуваат само за целта и во согласност со основата според кои се собрани. Примената на ова начело претставува предизвик за технологиите што користат вештачка интелигенција, бидејќи тие, во принцип, овозможуваат користење, односно повторна употреба или „пренамена“ на личните податоци за нови цели што се различни од оние за кои првично се собрани податоците. За да се утврди дали пренамената на личните податоци е легитимна, првично треба да се утврди дали новата цел е „компатибилна“ или „некомпатибилна“ со целта за која првично биле собрани личните податоци.[39]

- **Начело на „минимален обем на податоци“:**
  Личните податоци се соодветни, релевантни и ограничени на она што е неопходно во однос на целите заради кои се обработуваат.

  Начелото на минимален обем на податоци воедно претставува и мерка за заштита на личните податоци вклучена во интегрираната техничка заштита на личните податоци (Privacy by design and privacy by default). Балансирањето помеѓу ова начело и користењето на големи бази на податоци при креирањето системи со вештачка интелигенција првично треба да се почне со преиспитување на пропорционалноста помеѓу овие два концепта. Ова начело не исклучува вклучување на дополнителни лични податоци во обработката сè додека дополнителните лични податоци обезбедуваат корист, во однос на целите на обработката што ги надминува дополнителните ризици за субјектите на личните податоци. Во определени случаи користа од идната обработка може да го оправда обработувањето на личните податоците, но доколку се обезбедени соодветни заштитни мерки, на пример псевдонимизација, во комбинација со други безбедносни мерки, кои можат да придонесат за намалување на ризиците. Понатаму, кога се врши обработка на личните податоци само за статистички цели постои можност за обработка на поголем сет на лични податоци, а во тој случај податоците на субјектите на личните податоци можат да се обработат само како влезни податоци за обука (или за статистичка база на податоци) и нема да се користат за предвидувања или за одлуки што се однесуваат на поединци. Во ваков случај, обработката на личните податоци за статистички цели не треба да дава лични податоци како конечен резултат (да не извојува определено лице од групата и да не се открива идентитетот на субјект на лични податоци). Особено, личните податоци обработени за статистичка цел не треба да се користат за донесување одлуки за поединци, при што статистичката цел подразбира дека резултатот од обработката за статистички цели се збирни податоци (не лични податоци) и дека овој резултат или лични податоци не се користат за поддршка на мерки или одлуки во однос на кое било одредено физичко лице.

39 The impact of the General Data Protection Regulation (GDPR) on artificial intelligence – European Parliament.

- **Начело на „точност“:**
  Личните податоци се точни и каде што е потребно ажурирани, при што ќе се преземат сите соодветни мерки за навремено бришење или коригирање на податоците што се неточни или нецелосни, имајќи ги предвид целите заради кои биле обработени. При дизајнирањето, развојот и користење системи со вештачка интелигенција, ова начело е многу важно, особено во ситуациите кога со помош на вештачката интелигенција се прави некаква оценка за корисниците, кога им се даваат насоки или кога се носи одлука за нив. Користењето на неточни лични податоци може да предизвика штета не само за правото на приватност и заштита на личните податоци туку и за други права што се поврзани со алатката или апликацијата што се користи. Особено во контекстот на дизајнирање, развивање и користење алгоритми и системи на база на вештачка интелигенција што се наменети за користење во правосудството, користењето на неточни или произволни податоци може да предизвика огромни штети за физичките лица, не само од аспект на заштита на личните податоци и приватноста туку и за сите други права, на пример, доколку за учење на системот се користат неточни податоци, а тој предлага резултати, одлуки и решенија, секако дека овие предлози никако не можат да бидат релевантни.

- **Според начелото на „ограничување на рокот на чување“:**
  Личните податоци се чувани во форма што овозможува идентификација на субјектите на личните податоци, не подолго од она што е потребно за целите поради кои се обработуваат личните податоци. Личните податоци можат да се чуваат подолго од нивниот рок на чување ако се обработуваат само за целите на архивирање од јавен интерес, за научни или за историски истражувања или за статистички цели, а со применување на соодветни технички и организациски мерки заради заштита на правата и слободите на субјектот на личните податоци. Ова начело претставува голем предизвик за системите за вештачка интелигенција. Воедно, ова начело е поврзано и со целите за кои личните податоци се првично собрани и понатаму обработувани. За соодветно придржување кон начелото на „ограничување на рокот на чување“, секаде каде што е применливо, неопходно е да се преземат мерките на анонимизација, псевдонимизација, односно примена на соодветни мерки за безбедност на обработката на личните податоци.

- **Начелото „интегритет и доверливост“**
  подразбира дека личните податоци се обработени на начин што обезбедува соодветно ниво на безбедност на личните податоци, вклучувајќи заштита од неовластена или незаконска обработка, како и нивно случајно губење, уништување или оштетување, со примена на соодветни технички или организациски мерки. Притоа, **безбедноста на обработката на личните податоци**[40] подразбира дека: според најновите технолошки достигнувања, трошоците за спроведување и природата, обемот, контекстот и целите на обработката, како и ризиците со различен степен на веројатност и сериозноста за правата и слободите на физичките лица, контролорот и обработувачот се должни да применат соодветни технички и организациски мерки за да обезбедат ниво на безбедност соодветно на ризикот, вклучувајќи мерки, според потребата.[41]

40 Член 36 од Законот за заштита на личните податоци.

41 (а) псевдонимизација и криптирање на личните податоци; (б) способност за обезбедување на континуирана доверливост, интегритет, достапност и отпорност на системите и услугите за обработка; (в) способност за навремено, повторно воспоставување на достапноста до личните податоци и пристапот до нив во случај на физички или технички инцидент; (г) процес на редовно тестирање, оценување и евалуација на ефективноста на техничките и организациските мерки со цел да се гарантира безбедноста на обработката.

Воедно, концептот на **Техничка и интегрирана заштита на личните податоци (Data protection by design and by default)**[42] подразбира дека: Контролорот во моментот на дефинирање на средствата за обработка, како и во моментот на обработката е должен да примени соодветни технички и организациски мерки, како што е псевдонимизацијата, мерки што се развиени со цел ефикасно спроведување на начелата за заштита на личните податоци, како што е сведувањето на минимален обем на податоците и вклучување на потребните заштитни мерки во процесот на обработка, со цел да се исполнат барањата на овој закон и да се обезбеди заштита на правата на субјектите на личните податоци. Контролорот е должен да примени соодветни технички и организациски мерки за обезбеди дека интегрирано се обработуваат само оние лични податоци што се неопходни за секоја посебна цел на обработката.

Оваа обврска се однесува на количеството собрани лични податоци, опсегот на нивната обработка, рокот на чување и нивната достапност. Таквите мерки особено треба да обезбедат дека личните податоци, без согласност на субјектот на личните податоци, не се автоматски достапни за неограничен број лица.

- **Начелото на отчетност:**
  Опфаќа усогласеност со сите претходни начела на обработка на личните податоци, при што одговорноста за усогласеноста со начелата ја има и е должен да ја демонстрира контролорот.

4.2. ЗАКОНИТОСТ НА ОБРАБОТКАТА НА ЛИЧНИТЕ ПОДАТОЦИ

Согласно Законот за заштита на личните податоци, обработката на личните податоци е законита, само ако и до оној степен доколку е исполнет најмалку еден од следните услови[43]: субјектот на лични податоци дал согласност за обработка на неговите лични податоци за една или за повеќе конкретни цели; обработката е потребна за исполнување договор каде што субјектот на лични податоци е договорна страна или за да се преземат активности на барање на субјектот на лични податоци пред неговото пристапување кон договорот; обработката е потребна за исполнување на законска обврска на контролорот; обработката е потребна за заштита на суштинските интереси на субјектот на лични податоци или на друго физичко лице; обработката е потребна за извршување работи од јавен интерес или при вршење на јавно овластување на контролорот утврдено со закон; обработката е потребна за целите на легитимните интереси на контролорот или на трето лице, освен кога таквите интереси не преовладуваат над интересите или основните права и слободи на субјектот на лични податоци што бараат заштита на личните податоци, особено кога субјектот на личните податоци е дете. Ова нема да се применува за обработка на личните податоци од страна на органите на државната власт при спроведување на нивните надлежности.

Согласноста на субјектот на податоци[44] за обработка на неговите лични податоци преку систем за вештачка интелигенција може да се разгледа од два аспекта: субјектот на личните податоци да се согласи за вклучување на неговите лични податоци во сет податоци за обука или согласноста за неговите лични податоци да придонеси при креирање на алгоритамски модел наменет да дава

42 Член 29 од Законот за заштита на личните податоци.
43 Член 10 од Законот за заштита на личните податоци.
44 „Согласност“ на субјектот на лични податоци е секоја слободно дадена, конкретна, информирана и недвосмислена изјавена волја на субјектот на личните податоци, преку изјава или јасно потврдено дејство, а со кои се изразува согласност за обработка на неговите лични податоци.

индивидуализирани одговори. Субјектот на личните податоци треба да има можност да побара повлекување на согласноста на истиот начин по истиот пат по кој и првично ја дал, односно ако согласноста била дадена по електронски пат, со испраќање на електронска порака или одбирање на соодветно поле, на истиот начин треба да може и да ја повлече. Имајќи ги предвид условите за согласноста и правото на повлекување на согласноста, предизвик е согласноста да биде самостојна и релевантна основа како правна основа за обработка на лични податоци преку системите со вештачка интелигенција, особено во правосудството. Повлекувањето на согласноста не влијае на законитоста на обработката што се вршела врз основа на согласност пред отповикувањето. Во однос на легитимниот интерес како основа за обработка на личните податоци за креирање алгоритми и системи со вештачка интелигенција што би се користеле во правосудството, тој може да биде применлив само доколку биде утврден со законот.[45]

4.3. ПРАВА НА СУБЈЕКТИТЕ НА ЛИЧНИТЕ ПОДАТОЦИ

Понатаму, во Законот за заштита на личните податоци се утврдени и правата на субјектите на личните податоци:

- **Транспарентност:**
  Подразбира транспарентни информации, комуникација и начини на остварување на правата на субјектот на личните податоци. Ова право на субјектите на личните податоци им овозможува да добијат целосни информации во однос на обработката на нивните лични податоци.

  Во контекст на дизајнирањето, развивањето и користењето системи што користат вештачка интелигенција и кога за нивно креирање се обработуваат лични податоци, согласно ова право, информации што се доставуваат при собирање на лични податоци од субјектот на личните податоци се: информации за контролорот кој ќе ги користи при дизајнирање алгоритам или систем со вештачка интелигенција; која е основата за обработка на личните податоци (закон, согласност, договор, легитимен интерес...); за која цел се собираат личните податоци (на пример, влезни податоци за машинско учење, креирање алгоритам...); кои категории на лични податоци се обработуваат (на пример, име, презиме, податок за казнена осуда и сторено кривично дело...); колку долго се чуваат личните податоци (рокот во кој личните податоци ќе бидат обработувани во врска со конкретната цел); дали се врши пренос на личните податоци во друга земја и која е таа земја; дали постои автоматизиран процес на одлучување, вклучувајќи го и профилирањето и доколку постои, тогаш која е целта за тоа; дали личните податоци се откриваат на трети страни, доколку се откриваат, кои се третите страни; кои се правата на субјектите на лични податоци и како тие можат да се остварат[46].

45 Член 10 став (3) од Законот за заштита на личните податоци.

46 Правото на добивање информации, во контекст на користењето системи што користат вештачка интелигенција, се зема предвид во случаи каде што, покрај за првично дефинираната цел, личните податоци на субјектите на лични податоци се користат и за усовршување, унапредување на функционалностите на системот и намалувањето на можностите за грешки. Во овие случаи, информациите што треба да се дадат се: кои лични податоци ќе бидат предмет на дополнителна обработка; на кој начин ќе се врши профилирањето за да се оствари целта; на кој начин податоците ќе бидат заштитени при вршењето на дополнителната обработка; што презема контролорот за да обезбеди заштита на правата на субјектите од потенцијални ризици поврзани со дискриминација. Правото на субјектот да се добие копија од личните податоци што се користени при креирањето и развивање на алгоритмите или апликацијата со вештачка интелигенција, не смее да влијае негативно врз правата и слободите на другите физички лица.

- **Право на пристап:**
  Освен за субјектите на лични податоци чии податоци се користени при креирање, развивање апликација што користи вештачка интелигенција, ова право треба да биде овозможено и за корисниците на таа апликација. На локацијата каде што е достапна алатката или апликацијата што користи вештачка интелигенција потребно е да има достапни (објавени) информации за: целите на обработката, категории на лични податоци што се обработуваат, корисници на кои личните податоци се даваат на користење, рок на чување, право на исправка или бришење, ограничување на обработка, приговор, право да поднесе барање до надлежен орган за заштита на личните податоци, постоење на автоматизиран процес на одлучување, вклучувајќи и профилирање, а кога личните податоци не се собираат од субјектот на личните податоци и сите достапни информации за нивниот извор.

- **Право на исправка:**
  Во случај кога при остварувањето пристап, субјектот забележи дека неговите лични податоци се неточни или непотполни, има право да побара нивна исправка и надополнување. Во случаите каде што личните податоци се користат за надградување или за подобрување на апликацијата (земајќи ги предвид целите на обработката) субјектот на личните податоци има право да ги дополни нецелосните лични податоци, со давање на дополнителна изјава.

- **Право на бришење („право да се биде заборавен“):**
  Субјектот има право да побара неговите лични податоци да бидат избришани во случаите кога се исполнети целите заради кои се обработени; ако е повлечена согласноста, а притоа нема друга правна основа; ако приговара на обработката на податоците; ако личните податоци биле незаконски обработени, заради почитување на законска обврска или ако податоците биле собрани во врска со понуда на услуги на информатичко општество. На пример, субјектот на лични податоци има право да побара неговите податоци да бидат избришани во случаите кога тие се обработени за цели на машинско учење на апликацијата, а целта е остварена.

- **Право на ограничување на обработката:**
  Субјектот на личните податоци може да побара ограничување (блокирање) на обработката на личните податоци во случаи кога: ја оспорува нивната точност; обработката е незаконита, а тој се спротивставува на бришење на податоците; податоците веќе не се потребни да бидат чувани, но потребни му се на корисникот за остварување на неговите правни барања и кога корисникот вложил приговор, па се чека исходот од приговорот (се чека верификација дали легитимните интереси на контролорот преовладуваат над интересите на субјектот на личните податоци). При остварувањето на правото на ограничување на обработката, личните податоци се чуваат и не се вршат други операции на обработка.

- **Право на преносливост:**
  Субјектот има право да ги добие своите лични податоци во структуриран, вообичаено користен и машински читлив формат и нив да ги пренесе на друго место, без попречување од страна на контролорот на системот за вештачка интелигенција. Ова право е применливо кога се врши обработка врз основа на согласност или договор и кога обработката се врши на автоматизиран начин.

- **Право на приговор:**
  Субјектот на личните податоци врз основа на конкретната ситуација поврзана со него има право да поднесе приговор, и тоа кога обработка на личните податоци се заснова на јавен или легитимен интерес, вклучувајќи и профилирање; обработка на лични податоци се врши за цели на директен маркетинг и профилирање поврзано со директниот маркетинг; обработката на личните податоци се врши за цели на научни или историски истражувања или за статистички цели.

- **Автоматско донесување на поединечни одлуки, вклучувајќи и профилирање:**
  Кога станува збор за влијанието на правилата за заштита на личните податоци при развивање и користење алгоритми и вештачка интелигенција во правосудството, од суштинско значење е член 26 од Законот за заштита на личните податоци: „Субјектот на личните податоци има право да не биде предмет на одлука заснована единствено на автоматизирана обработка, вклучувајќи го и профилирањето што предизвикува правни последици за него или на сличен начин значително влијае на него. Ова не се однесува на одлуки што се засноваат на договор, закон или согласност. Ако одлуката се заснова на договор или согласност, субјектот има право да бара да биде обезбедена човечка интервенција, право на оспорување на одлуката и право да изрази личен став“.

Следствено на наведеното, заштитните мерки што треба да им се обезбедат на субјектите на податоци во случај на донесување на автоматизирана одлука вклучуваат: конкретни информации; право да се добие човечка интервенција; право да го изрази своето гледиште; право да се добие образложение за одлуката донесена по таквата процена и право на оспорување на одлуката.

4.4. ПРОЦЕНА НА ВЛИЈАНИЕТО НА ЗАШТИТАТА НА ЛИЧНИТЕ ПОДАТОЦИ (ПВЛЗП)

Имајќи ги предвид правилата од Законот за заштита на личните податоци (член 39), при дизајнирањето, а пред развивањето системи базирани на вештачката интелигенција, каде што е вклучена и обработка на лични податоци, а се наменети за користење во правосудството, задолжително треба да се направи процена на влијанието на заштитата на личните податоци. Имено, контролорот е должен да изврши процена на влијанието на предвидените операции на обработката во однос на заштитата на личните податоци, кога при користење на нови технологии за некој вид обработка, според природата, обемот, контекстот и целите на обработката постои веројатност таа да предизвика висок ризик за правата и слободите на физичките лица пред да биде извршена обработката. Една процена може да се однесува на серија слични операции на обработка, кои претставуваат слични високи ризици. Контролорот спроведува ПВЗЛП пред да почне со обработка на личните податоци, притоа обезбедувајќи техничка и интегрирана заштита на личните податоци, односно во фаза на планирање на операциите на обработка, како и кога некои од операциите на обработка сè уште се непознати.[47] Согласно Законот за заштита на личните податоци, процената на влијанието врз заштитата на личните податоци се бара особено во случај на: систематска и сеопфатна оценка на личните аспекти што се поврзани со физички лица, која

47 Контролорот бара мислење од субјектите на личните податоци или нивните претставници за планираната обработка, без да се влијае на заштитата на комерцијалните или јавните интереси или безбедноста на операциите на обработката. Контролорот има обврска да изврши преиспитување за да процени дали обработката се врши во согласност со процената на влијанието на заштитата на личните податоци најмалку во случаите кога има промена на ризикот предизвикана од операциите на таа обработка.

се заснова на автоматска обработка, вклучувајќи и профилирање, а врз основа на која се донесуваат одлуки што произведуваат правно дејство во врска со физичкото лице или значително влијаат на физичкото лице; обемна обработка на посебните категории на лични податоци или на лични податоци поврзани со казнени осуди и казнени дела или систематско набљудување на јавно достапни простори во големи размери. Имено, контролорот, за да определи кои операции на обработка веројатно ќе резултираат со висок ризик и за кои ПВЗЛП е задолжителна, мора да ги има предвид најмалку еден од критериумите определени во Правилникот за процесот на процена на влијанието на заштитата на личните податоци.[48] Контролорот задолжително донесува соодветна методологија за спроведување на ПВЗЛП според наведените критериуми. Агенцијата за заштита на личните податоци воедно има донесено и објавено и Листа на видовите операции на обработка за кои се бара процена на влијанието врз заштитата на личните податоци[49].

4.5. ПОЛИЦИСКА ДИРЕКТИВА

Кога зборуваме за влијанието на правилата за заштита на личните податоци при развивање и користење алгоритми и вештачка интелигенција во правосудството, значајно е да се спомене и Директивата (ЕУ) 2016/680 на Европскиот парламент и Советот за заштита на физичките лица во однос на обработката на личните податоци од страна на надлежните тела за цели на спречување, истрага, откривање или гонење на кривичните дела или за извршување на кривичните санкции и за слободното движење на овие податоци (Полициска директива). Оваа директива сè уште не е транспонирана во РС Македонија, иако уште во 2021 година е изработен предлог-закон[50] за заштита на физичките лица во врска со обработката на личните податоци заради цели на спречување, истрага, откривање или гонење на кривични дела или за извршување на кривични санкции[51]. Со овој предлог-закон е предвидено да се уреди заштитата на физичките лица во врска со обработката на личните податоци од страна на надлежните органи за цели на спречување, истрага, откривање или гонење на кривични дела или за извршување на кривични санкции, вклучувајќи и заштита и спречување закани во однос на јавната безбедност. Во овој предлог-закон е содржан и член што се однесува на автоматско донесување на поединечни одлуки.[52]

48 Правилник за процесот на проценка на влијанието на заштитата на личните податоци („Службен весник на РС Македонија“, бр. 122/20).

49 https://azlp.mk/

50 Целта на овој предлог-закон е да се обезбеди: заштита на основните права и слободите на физичките лица, а особено нивното право на заштита на личните податоци; размена на личните податоци помеѓу надлежните органи, а која е предвидена со закон, без да се ограничи или да се забрани од причини што се однесуваат на заштитата на физичките лица во врска со обработката на нивните лични податоци. Со одредбите од овој закон нема да се ограничи примената на повисоки мерки за заштита на правата и слободите на физичките лица во врска со обработката на нивните лични податоци од страна на надлежните органи доколку такви мерки се предвидени со друг закон.

51 https://ener.gov.mk/

52 „(1) Забрането е донесување на одлука која произведува правно дејство за субјектот на личните податоци заснована единствено на автоматска обработка на личните податоци.

(2) По исклучок од ставот (1) на овој член, донесување на одлука која предизвикува или влијае на правните последици на субјектот на личните податоци, а се заснова исклучиво на автоматска обработка на личните податоци, вклучувајќи и профилирање, е дозволена само ако донесувањето на таквата одлука е предвидена со овој закон или друг закон со кој се обезбедува соодветна заштита на правата и слободите на субјектот на личните податоци, а најмалку право на обезбедување на човечка интервенција од страна на контролорот.

(3) Одлуките од ставот (2) на овој член не смеат да се засноваат на посебни категории на личните податоци освен ако се воспоставени соодветни мерки за заштита на правата и слободите, како и легитимните интереси на субјектот на личните податоци.

(4) Забрането е профилирање кое доведува до дискриминација на субјектите на личните податоци која се заснова на посебни категории на лични податоци.“

5. ФАКТОР „РИЗИК“ – РЕГУЛАТИВА ЗА ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА: РАЗЛИЧНИ ПРАВИЛА ЗА РАЗЛИЧНИ НИВОА НА РИЗИК

Регулативата за вештачка интелигенција (Artificial intelligence act) воспоставува заедничка регулаторна и правна рамка за вештачката интелигенција во рамките на Европската унија (ЕУ)[53]. Регулативата ги опфаќа сите видови на вештачка интелигенција во широк опсег на сектори, со исклучоци за системи за вештачка интелигенција што се користат исклучиво за воени цели, национална безбедност, истражувачки и непрофесионални цели. Како дел од регулативата за производи, оваа регулатива за ВИ не им дава права на поединци, туку ги регулира давателите на услуги на системи за вештачка интелигенција и ентитети кои користат вештачка интелигенција во професионален контекст.[54] Регулативата класифицира различни категории на ризик во зависност од видот на апликацијата, со специфична категорија посветена на генеративната вештачка интелигенција за општа намена. Класификацијата на ризикот се заснова на намената на системот за вештачка интелигенција, на функцијата што ја врши системот за вештачка интелигенција и специфичната намена и модалитети за кои се користи системот се клучни за да се утврди дали системот за вештачка интелигенција е со висок ризик или не.

> **Неприфатлив ризик** –
> Системите со вештачка интелигенција со неприфатлив ризик се системи што се сметаат за закана за луѓето и ќе бидат забранети. Тие вклучуваат: Когнитивна бихевиорална манипулација на луѓе или одредени ранливи групи; Социјално бодување: класификација на луѓето врз основа на однесување, социоекономски статус или лични карактеристики (рангирање поединци врз основа на нивните лични карактеристики, социоекономски статус или однесување); Биометриска идентификација и категоризација на луѓе: биометриски системи за идентификација во реално време и далечина, како што е препознавање лица.

Некои исклучоци можат да се дозволат за цели на спроведување на законот. Системи за далечинска биометриска идентификација „во реално време“ ќе бидат дозволени во ограничен број сериозни случаи, додека на „постдалечинските“ биометриски системи за идентификација, каде што идентификацијата се случува по значително одложување, ќе биде дозволено да гонат тешки кривични дела и само по одобрение од судот.

53 Законот за вештачка интелигенција беше предложен од Европската комисија на 21 април 2021 година, усвоен од Европскиот парламент на 13 март 2024 година, и беше едногласно одобрен од Советот на ЕУ на 21 мај 2024 година. Законот за ВИ, исто така, создава Европски одбор за вештачка интелигенција за да ја промовира националната соработка и да обезбеди усогласеност со регулативата. Како и Општата регулатива за заштита на личните податоците во ЕУ, Законот може да се применува вонтериторијално на давателите на услуги надвор од ЕУ доколку имаат корисници во ЕУ.

54 Нацрт-законот беше ревидиран за да се одговори на порастот на популарноста на генеративните системи за вештачка интелигенција, како што е „Чет џи-пи-ти“, чии можности за општа намена не одговараа на главната рамка. Се планираат порестриктивни регулативи за моќни системи за генерирање на вештачка интелигенција со системско влијание.

Висок ризик –
Апликации за вештачка интелигенција за кои се очекува да претставуваат значителна закана за здравјето, безбедноста или основните права на луѓето, како што се системи за вештачка интелигенција што се користат во здравството, образованието, регрутирањето, управувањето со критичната инфраструктура, спроведувањето на законот или правдата. Тие подлежат на обврски за квалитет, транспарентност, човечки надзор и безбедност, а во некои случаи бараат „Проценка на влијанието на основните права“ пред распоредувањето. Тие мораат да бидат евалуирани и пред да бидат ставени на пазарот и во текот на нивниот животен циклус. Списокот на апликации со висок ризик може да се прошири со текот на времето, без потреба да се менува Регулативата за вештачка интелигенција.[55]

Во Регулативата за вештачка интелигенција исто така се содржани одредби за барањата за информираност и транспарентност, авторски права, обврска за означување содржина генерирана (креирана или изменета) од вештачка интелигенција, објавување резимеа на податоци заштитени со авторски права што се користат за обука, доброволни кодекси за однесување, одредби за казни за непочитување на законот, одредби за создавање regulatory sandbox, т.е. контролирана средина што го олеснува развојот, правила за тестирањето и валидацијата на иновативни системи за вештачка интелигенција за ограничен временски период (пред да бидат пуштени во промет, која ќе им овозможи на учесниците да користат лични податоци за поттикнување на иновациите со вештачка интелигенција, во согласност со барањата на GDPR). Воедно, Регулативата содржи и одредби во насока на поддршка на иновациите: предложените мерки се приспособени за малите провајдери и почетните претпријатија.[56]

55 Воедно, класификацијата ги опфаќа и следните категории: Вештачка интелигенција за општа намена (додадена во 2023 година), категорија што вклучува особено модели на основа како „Чет џи-пи-ти“. Тие се предмет на барања за транспарентност. Системите за вештачка интелигенција за општа намена со високо влијание што можат да претставуваат системски ризици (особено оние обучени со поголема пресметковна способност), исто така, мораат да поминат низ темелен процес на евалуација. Ограничен ризик – Системите за вештачка интелигенција во оваа категорија имаат обврски за транспарентност, обезбедувајќи им на корисниците информации дека имаат интеракција со систем на вештачка интелигенција и овозможувајќи им да прават информирани избори. Оваа категорија вклучува, на пример, апликации за вештачка интелигенција што овозможуваат генерирање или манипулирање со слики, звук или видеа (како deepfakes). Во оваа категорија, бесплатните модели што се со отворен код (т.е. чии параметри се јавно достапни) не се регулирани, со некои исклучоци. Минимален ризик – Оваа категорија вклучува, на пример, системи за вештачка интелигенција што се користат за видеоигри или филтри за спам. Повеќето апликации за вештачка интелигенција се очекува да спаѓаат во оваа категорија. Овие системи не се регулирани, а земјите-членки не можат да наметнуваат дополнителни регулативи поради правилата за максимална хармонизација.

56 Од друга страна, креаторите на високоризични системи за вештачка интелигенција ќе мораат да поминат процедура за усогласеност, со вклучена процена на ризик, пред нивните производи да бидат продадени и употребени во ЕУ. Тие ќе треба да се усогласат со низа барања, вклучително и за тестирање, обука за лични податоци и кибербезбедност и во некои случаи, ќе мора да спроведе процена на влијанието на основните права за да се обезбеди дека нивните системи се усогласени со правото на ЕУ. Оцената на сообразноста треба да се изврши или врз основа на внатрешна контрола (самооценување) или со вклучување на нотифицирано тело. Откако таквите системи за вештачка интелигенција ќе се пласираат на пазарот, провајдерите мораат да спроведат мониторинг по продажбата и да преземате корективни активности доколку е потребно.

6. КОРИСТЕЊЕ АЛГОРИТМИ И ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА ВО ПРАВОСУДСТВОТО

Постојните ИТ-системи што се користат во правосудството со употребата на алгоритми и вештачка интелигенција можат да бидат надградени, поефикасни и покорисни. Секако, при развивањето на овие софтверски решенија, како и на идните решенија што ќе бидат базирани на вештачка интелигенција, а ќе бидат користени во правосудството, мораат да се почитуваат етичките принципи за дизајнирање и развивање на овие решенија, заштита на правата на учесниците во судските постапки, правото на приватност и заштита на личните податоци и другите човекови права, начелата за заштита на личните податоци, интегрираната техничка заштита (*privacy by design and privacy by default*) и примената на соодветни мерки за безбедност на обработката на податоците. Согласно Рамковната конвенција на Советот на Европа за вештачка интелигенција и човекови права, демократија и владеење на правото[57], принципи што треба да се запазат, а се поврзани со активности во рамките на животниот циклус на системите за вештачка интелигенција се: Човеково достоинство и индивидуална автономија; Транспарентност и надзор; Отчетност и одговорност; Еднаквост и недискриминација; Приватност и заштита на личните податоци и Безбедна иновација.

6.1. ЗАШТИТА НА ЛИЧНИ ПОДАТОЦИ ВО ПОЛИТИКИТЕ ЗА ОТВОРЕНИ ПОДАТОЦИ ЗА СУДСКИ ОДЛУКИ

ИМИЊАТА НА СТРАНКИТЕ И СВЕДОЦИТЕ

Со цел да се постигне правична рамнотежа во дигиталната ера помеѓу потребата јавно да се објавуваат судските одлуки и да ги почитуваат основните права на странките или сведоците, нивните имиња и адреси не смеат да се појавуваат во објавените одлуки, особено во поглед на ризикот од злоупотреба и повторна употреба на таквите лични информации и особената чувствителност на податоците што најверојатно ќе бидат содржани во одлуките. Автоматизираните процеси можат да се користат за систематско прикривање на таквите податоци. Други информации за идентификација, исто така, можат да бидат прикриени (на пример, телефонски броеви, адреси на е-пошта, датуми на раѓање, дадени имиња на децата, ретки имиња, прекари и имиња на места). Во однос на личните податоци како заштитни принципи, ова прикривање значи едноставна псевдонимизација на податоците, а не целосна анонимизација. Обемот и разновидноста на информациите содржани во судските одлуки, во комбинација со растечката леснотија на вкрстување со други бази на податоци, оневозможува, во практиката, да се гарантира дека засегнатото лице не може повторно да се идентификува. Во отсуство од таква гаранција, овие податоци не можат да се квалификуваат како анонимни и затоа подлежат на правилата за заштита на личните податоци. Некои особено чувствителни категории на лични податоци налагаат особено внимание, како податоци што откриваат етничко или расно потекло, политички мислења, членство во синдикат, верски или други верувања, физичко или ментално здравје или сексуален живот, кои се сметаат за интимни детали. Судските одлуки можат да содржат други, многу различни видови на лични податоци што спаѓаат во оваа категорија на чувствителни податоци.

57 Committee on Artificial Intelligence (CAI), Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, 17.05.2024 година.

Судовите што се занимаваат со кривична материја особено веројатно е да обработуваат чувствителни податоци како што се оние за кривични дела. Затоа, сите овие чувствителни податоци заслужуваат посебна будност. Нивното масовно ширење би предизвикало сериозни ризици од дискриминација, профилирање и нарушување на човечкото достоинство.

ИМИЊА НА ПРОФЕСИОНАЛЦИ, ВКЛУЧИТЕЛНО И СУДИИ

Важен елемент за адвокатите во предвидувањето на исходот на случајот и како ќе се донесе пресудата е знаењето на информацијата кој е судијата на случајот и адвокатите веруваат дека познавањето на работата на судијата понекогаш е речиси исто толку важно како и познавањето на законот. Адвокатите долго време се обидуваат да прават споредби меѓу судиските совети, повеќе или помалку емпириски, за да се дадат подобри совети на клиентите. Затоа не можеме да ја исклучиме можноста дека во иднина многу ќе бидат корисни, а со тоа и многу скапи апликациите за машинско учење, но многу поефективно од искуството и „добрата смисла“ на адвокатите во парничните спорови што работат низ случаите на традиционален начин. Употребата на такви апликации дополнително може да го нагласи нарушувањето на конкуренцијата и нееднаквоста со цел да се анализира и да се предвиди нивното однесување или нивната ситуација, на пример утврдување на нивните перформанси на работа, финансиската состојба, здравјето, преференциите, животните навики итн. Од тие причини треба да се има претпазливост, да се процени интересот, според видот на парницата и степенот на јурисдикција, за објавување на имињата на професионалците во базата на податоци што може да се преземе. Исто така, не може да се исклучи можноста судските институции или овластени трети страни да ги искористат овие информации надвор од контекстот на отворени/јавнообјавени податоци.

6.2. ПОЛИТИКИ ЗА ОТВОРЕНИ ПОДАТОЦИ ШТО СЕ ОДНЕСУВААТ НА СУДСКИТЕ ОДЛУКИ ВО СУДСКИТЕ СИСТЕМИ НА ЗЕМЈИТЕ-ЧЛЕНКИ НА СОВЕТОТ НА ЕВРОПА

Достапноста на податоците е суштински услов за развој на вештачката интелигенција, овозможувајќи му да извршува одредени задачи што претходно ги извршувале луѓето на неавтоматски начин. Колку повеќе податоци се достапни, толку повеќе вештачката интелигенција може да ги усоврши моделите и да ја подобри нивната способност за предвидување. Затоа, пристапот за отворени податоци за судските одлуки е предуслов за работата на правните технолошки компании специјализирани за пребарување или анализа на трендови („предвидлива правда“). Обработката на овие податоци иницира голем број прашања, како што се промените во формирањето на судската практика и заштитата на личните податоци (вклучувајќи ги и имињата на професионалците).

Податоците собрани од компјутер се „гориво“ на 21 век, бидејќи нивната употреба и вкрстувањето создаваат сосема ново богатство. Квантификацијата на човечките активности, сега на глобално ниво, би можела да не пропушти да ги допре податоците што ги произведува јавниот сектор. Оттука, отворените податоци вклучуваат само дисеминација на „необработени“ податоци во структурирани компјутерски бази на податоци. Овие податоци, собрани во целост или делумно со други структурирани извори, го сочинуваат она што го нарекуваме „големи податоци“. Консултативниот комитет на Конвенцијата 108 на Советот на Европа ги дефинира големите податоци како „растечката технолошка способност за собирање, обработка и екстракција на ново и предвидливо знаење од голем волумен, брзина и разновидност на податоци“. Во однос на заштитата на личните податоци, главните прашања не се

однесуваат само на обемот, брзината и разновидноста на обработените податоци туку и на анализата на податоците, користејќи софтвер за извлекување ново и предвидливо знаење за целите на донесување одлуки во врска со поединци или групи.

- **„Аналитика на податоци“**

  Забележливо е од дефиницијата, отворените податоци не треба да се мешаат со нивните средства за обработка. Дел од дискурсот за ова прашање, всушност, се однесува на обработката извршена со различни напредни методи што генерално се дефинираат како наука за податоци. Предвидлива правда со помош на вештачка интелигенција и напредни пребарувачи кои применуваат исклучително прецизни критериуми и правни роботи се сите алгоритамски апликации што се хранат со податоци, но имаат врска со политиката на отворени податоци. Сепак, оваа политика мора да се испита во светлината на можностите да се нуди за понатамошна обработка, без оглед на нејзината природа. Доколку одредени податоци се филтрираат, земајќи ја предвид, на пример, потребата за доверливост и почитувањето на приватноста, се чини дека се намалуваат последователните ризици од злоупотреба. Во однос на состојбата на развој на отворени податоци за судството, одлуки во земјите-членки на Советот на Европа и последици за развојот на судската практика, отворени податоци за судски одлуки, фокусот е ставен на прашањето дали се обезбедуваат судски одлуки со отворени податоци, за кои се користи одредена обработка од вештачка интелигенција, како и прашањето за анонимизација или псевдономизација на личните податоци. Во однос на заштитата на личните податоци, потребна е псевдонимизација барем на некои видови спорови (на пример, личен статус, семеен статус) со бришење на податоците што прават странките или сведоците да можат да се идентификуваат (имиња, адреси, телефонски броеви, лични броеви, банка, броеви на сметки, даночни броеви, здравствена состојба итн.) што е одговорност на судскиот персонал. Сепак, постои вистинска тешкотија во мерењето на влијанието на отворените податоци за ефикасноста и квалитетот на правдата.

- **Оперативни карактеристики на вештачката интелигенција (машинско учење) применето на судските одлуки**

  Обработка на природен јазик и машинско учење се двете суштински техники за обработката на судските одлуки со користење на вештачка интелигенција. Во повеќето случаи, целта на овие системи не е да репродуцира правно размислување, туку да ги идентификува корелациите помеѓу различните параметри на одлуката (на пример, при барање за развод должината на бракот, приходот на сопружниците, постоење прељуба, висината на изречената корист и сл.) преку употребата на машинско учење, за да се определи/создаде еден или повеќе модели. Таквите модели се наменети да се користат за „прогнозирање“ или „предвидување“ на идна судска одлука.

- **Теоретските функционалности на софтвер за „предвидливата правда“**

  Функционалностите што ги ветува „предвидливиот“ софтвер се во насока на давање предлози да се утврдат веројатностите на успехот (или неуспехот) на случајот пред суд. Овие веројатности се воспоставуваат преку статистичко моделирање на претходни одлуки со помош на методи од два широки домена на компјутерски науки: обработка на природни јазици и машинско учење. Тие даваат графички приказ на веројатноста за успех за секој исход од спор врз основа на критериуми внесени од корисникот (специфични за секој вид спор).

- **Машинско учење и алгоритми**

  Машинското учење е област на компјутерската наука во која компјутерот и програмите учат од искуство. Алгоритмите прават машината да извршува задачи преку процес на тренирање, како дете кое учи во неговата околина. Овие техники за учење можат или не можат да бидат надгледувани од човек. Сепак, овие алгоритми остануваат високоспецијализирани за една особена задача и претставување проблеми со проникливост кога се соочуваат со хаотични ситуации или со недоволни податоци за да се овозможи предвидување (како што е вистинското разбирање на природниот јазик). Во општествените науки, на кои припаѓаат правото и правдата, неуспехот дури би изгледал неизбежен во отсуство на убедливи аргументи. Покрај тоа, единствеността на сегашните системи за обработка на големи податоци е дека тие не се обидуваат да го репродуцираат нашиот когнитивен модел, туку произведуваат контекстуални статистики за невидена големина на податоци, без вистинска гаранција за исклучување на лажни корелации.

- **Можат ли моделите на вештачка интелигенција правно да расудуваат однапред и дали вештачката интелигенција може да го објасни однесувањето на судиите во ретроспектива?**

  Своите одлуки судиите ги донесуваат врз основа на изборот на релевантните факти и нивното толкување според правните норми. Со други зборови, судијата во реалноста може само да произведе веројатност со лексички материјал во голема мера изведен од образложението и неговата мотивацијата (на судијата). Вештачката интелигенција, пак, е воспоставена на начин што создава голема веројатност за кореспонденција помеѓу групи зборови и одлука што може да доведе само до ограничен број можни исходи. Под никакви околности не може само да се репродуцира резонирањето на судиите ниту, пред сè, да предвидува исход, на пример, необработена тужба на иден апликант пред суд, заснована во голема мера на примената на стандардите за оценување (важноста и сериозноста на жалбата итн.) остава значителна слобода во одлучувањето.

Но, дали навистина можат да се постигнат такви толкувања врз основа на алгоритамска обработка на судските одлуки?

Процесите на донесување одлуки (што се разликуваат од нивните лични и јавни изјави во односниот случај), нивното однесување или, во овој случај, нивната одлука, треба да се определат според нивните особини на личноста, мислењата или религијата. Меѓутоа, таквото каузално објаснување не може едноставно да се заклучи од веројатниот резултат што го даваат алгоритмите. Напротив, тоа бара дополнителна аналитичка работа со цел да се изолираат, меѓу многуте корелирани фактори (вклучувајќи го и идентитетот на членовите на советот на судии), оние што се вистински одлучувачки фактори. На пример, тоа што судија кој најчесто суди предмети поврзани со семејно право статистички почесто одлучува дека децата треба да живеат со својата мајка го прави предвидлив фактор, но не мора да ја одразува пристрасноста на судијата во корист на жените, туку, напротив, постоење на психосоцијални, економски, па дури и културни фактори специфични за јурисдикција, како што е работното време на секој од родителите, нивниот приход, локалната достапност на колективна грижа за децата, без разлика дали детето оди на училиште, без разлика дали еден од родителите е во нова врска или дури, едноставно, незаинтересираност од страна на кој било родител да се грижи за мало дете.

6.3. КАКО ДА СЕ ПРИМЕНУВА ВЕШТАЧКАТА ИНТЕЛИГЕНЦИЈА ВО ГРАѢАНСКО И УПРАВНО ПРАВО?

Состојбата на развој на техниките за машинско учење не дозволува денес да се постигнуваат сигурни резултати во однос на „предвидувањето" на судските одлуки. Првото прашање што се поставува за употреба на вештачката интелигенција во областа на граѓанското и управното право не е дали е корисно или штетно, пожелно или непожелно, туку дали предложените алгоритми можат да го постигнат типот на бараниот резултат. Во исто време, носителите на јавни одлуки го гледаат ова како можност подобро да се регулира текот на новите постапки во судовите и да се намалат судските оперативни трошоци.

Главни гаранции што треба да се реафирмираат во граѓански и управни постапки при употребата на ВИ:

- **Право на пристап до суд:** Обезбедувањето онлајн-алатки за решавање спорови не треба да влијае на правото на пристап до суд, дури и ако ова право не е апсолутно и е подложно на имплицитни ограничувања. Во граѓанските постапки, на пример, секој парничар има право да поведе спор што се однесува на неговите „граѓански права и обврски" и право да биде сослушан пред суд.
- **Противнички принцип (правило на спротивставување на фактите):** Императив да се направи одредено количество на квантитативни информации (на пример, бројот на одлуки обработени за да се добие скалата) и квалитативни информации (потекло на одлуките, репрезентативност на избрани примероци, распределба на одлуките меѓу различни критериуми, на пример, економскиот и социјалниот контекст) достапни за граѓаните е, пред сè, за странките на судење, со цел да се разбере како се конструирани мерилата, да се измерат нивните можни граници и да може да ги дебатира пред судија.
- **Еднаквост на оружјата:** Употребата на технолошки средства не треба да предизвикува нерамнотежа помеѓу странките, бидејќи употребата на дигитални средства навистина може да ја олесни постапката.[58] За разлика од одредени чинители (институции, фирми со средства, компјутерски писмени лица) употребата на технолошки средства, напротив, претставува тешкотии за одредена популација лица кои се помалку запознаени со компјутерите.
- **Непристрасност и независност на судиите:** Употребата на ВИ-апликациите може да има индиректни ефекти врз независноста и непристрасноста на судството, особено во системите каде што независноста на судството не е целосно постигната.
- **Право на бранител:** Постојат предности што произлегуваат од примената на алатките за предвидување на правдата за адвокатите и особено можноста на адвокатите да им дадат на своите клиенти подобро информирани совети преку емпириско и систематско оценување на шансите за успех на постапката. Сепак, за пример да земеме случај за оценување на шансите за успех на парницата на екстремно сиромашен клиент: дали ова може да влијае на одлуката на адвокатот да му помогне на својот клиент? Практиката на правните професионалци треба да има цел да го минимизира ризикот, да не се дојде до ситуација лицата кои го бараат правниот совет, на крајот, да можат да бидат лишени од него.

58 Резолуција 2054 (2015) на Парламентарното собрание на Советот на Европа (PACE), 10 ноември 2015 година, http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=22245&lang=en

6.4. ПРАШАЊА СПЕЦИФИЧНИ ЗА КРИВИЧНОТО ПРАВО: СПРЕЧУВАЊЕ ПРЕКРШОЦИ, РИЗИК ОД РЕЦИДИВ И ПРОЦЕНА НА СТЕПЕНОТ НА ОПАСНОСТ

Дури и системите со ВИ да не се конкретно дизајнирани да бидат дискриминаторски, употребата на статистика и вештачката интелигенција во кривичната постапка покажала ризик да поттикне повторно оживување на детерминистички доктрини на штета на доктрините за индивидуализација на санкцијата. Употребата на науката и технологијата за вештачка интелигенција во кривичната материја е специфична со многу предизвици, бидејќи неговата примена може да потврди или да негира некои актуелни јавни дебати за наводната предвидливост на навредливото однесување, да се утврдат вообичаени или професионални криминални карактеристики, склоноста за извршување кривично дело, карактерот и личноста на обвинетиот и, воопшто, психолошките квалитети на обвинетиот, без оглед на патолошките причини. Во однос на користењето на овие системи во предвидување рецидив или процена на степенот на опасност, постои можноста за генерирање на дискриминирачки или неточни резултати поради нивното засновање на влезни податоци – одлуки што можат да генерираат дискриминаторски резултат по основа на определени карактеристики (пол, потекло, географско подрачје каде што е извршено кривичното дело, социјален статус, раса...) на физичко лице кое е осомничено за сторување на кривично дело, како и субјективни принципи на развивачите/дизајнерите на алгоритмите што ги нудат/генерираат резултатите/одлуките. Затоа, алатките со ВИ што би се користеле во кривичното право треба да бидат дизајнирани во согласност со основните принципи на недискриминација и рехабилитација, вклучувајќи ја и улогата на судија во индивидуализацијата на казната, врз основа на објективни елементи на личноста (обука, вработување, редовни лекарства и социјална грижа) без каква било друга форма на анализа, освен онаа спроведена од специјално обучени професионалци.

6.5. ПОТЕНЦИЈАЛОТ И ОГРАНИЧУВАЊАТА НА АЛАТКИТЕ ЗА ПРЕДВИДУВАЊЕ НА ПРАВДАТА

ДОПОЛНИТЕЛНИ АРГУМЕНТИ „ЗА“ И „ПРОТИВ“

Подобрување на судската практика: техниките за машинско учење сè повеќе се употребливи во областа на обработката на природните јазици во изминатите години (ова ги вклучува почетните напори за разбирање на природниот јазик) и се значителна предност за наоѓање опции за пребарување за дополнување на тековниот клучен збор или пребарување во цел текст. Природен јазик е јазик што е мајчин говор на еден народ (на пример, македонски јазик, англиски јазик, француски јазик...).[59] Овие алатки би можеле да поврзуваат различни извори (на пример, устави и конвенции, закони, случаи од правото и правна теорија). Техниките за визуализација на податоците би можеле да илустрираат резултати од пребарувањето.

Автоматизација на едноставни и повторливи случаи: врз основа на претходни одлуки засновани на исти факти, исти околности и иста применлива регулатива, би можело да нудат/генерираат судски предлог-одлуки (што ќе им даде повеќе време на судиите да се посветат на одлучување во посложени судски предмети).

59 Обработка на природни јазици (NLP) е гранка на вештачката интелигенција (ВИ) што им овозможува на компјутерите да разберат, генерираат и манипулираат со човечкиот (природниот) јазик.

Апликации што ќе претвораат говор во текст: со помош на вакви апликации би се скратило времето за постапување на правните професионалци (практично, правните професионалци преку овие апликации ќе можат да ги издиктираат правните акти, при што апликацијата ќе има улога на дактилограф).

Пристап до закони: без замена на човечка интервенција, четботите – средствата за виртуелен агент би можеле да се постават за да се олесни пристапот до различните постојни извори на информации со користење на природен јазик. Шаблони за документи (барања, договори за закуп итн.) можат да се генерираат и преку интернет.

Создавање нови стратешки алатки: употреба на наука за податоци и вештачки разузнавачки техники за податоците за судската активност можат да помогнат во подобрувањето на ефикасноста на правдата преку овозможување, на пример, да се спроведат квантитативни и квалитативни процени и да се прават проекции (на пример, идни човечки и буџетски ресурси).

Терминот предвидувачка правда треба да се отфрли затоа што е двосмислен и погрешен. Овие алатки се засноваат на методи на анализа на судската практика, користејќи статистички методи што на ниеден начин не репродуцираат правно расудување, но можат да се обидат да го направат тоа. Мораат да се идентификуваат аналитичките предрасуди, доколку не можат да се отстранат целосно. Процесот на дизајнирање и употребата на алатките мораат да бидат вградени во јасна етичка рамка.

Веќе ја истакнавме двосмисленоста и заблудата на концептот на предвидлива правда. Ветувањата на овој концепт треба да се испитаат на објективен и научен начин, врз основа на цврсти основи на фундаментални истражувања, со цел да се идентификуваат можни ограничувања. Во врска со ова, треба да се забележи дека ризиците од искривените толкувања на судските одлуки се крајно високи кога се засноваат само на статистичко моделирање. Оваа опсервација е потврдена понатаму поради недостатокот на прецизно разбирање на врските помеѓу податоци и очигледно присуство на лажни корелации што не можат да се забележат во големи сетови податоци. Освен тоа, неутралноста на алгоритмите е мит, бидејќи нивните креатори можат свесно или ненамерно да ги пренесуваат во нив сопствените вредносни системи.

И покрај овие значајни ограничувања, дали треба да го предвидиме придонесот на технологијата со неспоредлива моќ?

Употребата на вештачка интелигенција веројатно ќе понуди исклучително значајна поддршка за професионалците, вклучувајќи ги судиите и адвокатите, но и за пошироката јавност, особено ако еден ден тие овозможат да се конструираат неспоредливи истражувачки и документарни аналитички алатки во законодавната, регулаторната, правната и доктриналната материја и да создадат динамични врски меѓу сите овие извори. Во овој динамичен контекст, се чини суштински е прво да не се брза со одлуки и да се одвои време однапред да се дебатира за ризиците и практичните примени на овие инструменти за судските системи и да се тестираат во првата фаза. Судскиот систем, во согласност со своето време, би бил способен да воспостави, администрира и гарантира вистински одлуки за јавниот и приватниот сектор и инсистирањето на целосна транспарентност и правичност во функционирањето на алгоритмите, би можело да придонесе до идно помагање во судското одлучување.

7. ПРЕДИЗВИЦИ И РИЗИЦИ ВО УПОТРЕБАТА НА АЛГОРИТМИ И ВЕШТАЧКА ИНТЕЛИГЕНЦИЈА ВО ПРАВОСУДСТВОТО ВО РС МАКЕДОНИЈА

Предизвиците и ризиците од примената на алгоритми и вештачка интелигенција што постојат во државите-членки на Советот на Европа разгледани во овој документ секако се однесуваат и на правосудството во РС Македонија. Имајќи предвид дека непремостлив ризик претставува користење систем со вештачка интелигенција во правосудството што самостојно би носел одлуки без човечка интервенција, во моментот и во блиска иднина ваков систем не би требало да биде ни предмет на разгледување. Но, секако, потребно е интензивно и внимателно да се разгледува потребата и начинот на регулирање и употреба на вакви системи како помошна алатка при носењето одлуки во секторот на правосудството.

1. Најголемиот ризик, а воедно и предизвик претставува правната нерегулираност на алгоритмите и системите што користат вештачка интелигенција, односно непостоењето на јасни правила, ограничувања и насоки за примена на вакви системи во нашата држава. Ова претставува предизвик и ризик за доменот на правосудството, имајќи ги предвид чувствителноста и важноста на овој сектор. Имено, во судските постапки се одлучува не само за права и обврски туку и посредно се одлучува за човечки судбини и иднината на учесниците во постапките.

2. Предизвик за нашето правосудство во контекст на употребата на алгоритми и вештачка интелигенција претставуваат човечките ресурси – знаењето, практиката и искуството на дизајнерите и развивачите на ваквите системи. Имено, при дизајнирањето и развивањето на овие системи, дизајнерите мораат да имаат познавања од областа на правото, постапките, етички вредности, знаење и практики во создавањето на безбедни системи со примена на соодветни технички и организациски мерки за заштита на овие системи, како и знаења и способности да ги проценат ризиците и влијанието на овие системи врз човековите права.

3. Од друга страна, предизвик претставува и обученоста на професионалците од правосудната фела, кои по развивањето алгоритми и системи со вештачка интелигенција наменети да се користат во правосудството, ќе ги користат овие системи. Имено, за да имаат корист професионалците од правосудната фела, односно помош при донесувањето на одлуките, тие мораат да имаат обука и знаења како да ги користат овие системи.

4. Понатаму, предизвик претставува и начинот на составување на сетовите податоци во случаите кога тие ќе се користат во создавањето алгоритми и систем со вештачка интелигенција, кои ќе се обучуваат, т.е. ќе учат од овие податоци, односно ќе предлагаат резултати. Предизвик претставува заштитата на личните податоци во судските одлуки (потреба од анонимизација), доколку во сетот податоци што ќе се користат за развивање на овие системи се внесуваат судски одлуки. Имајќи предвид дека овие системи би биле наменети за нашето правосудство, ќе биде потребно да се користат прописите од домашното законодавство, одлуки од македонските судови, а во посебен сет модули (согласно потребата и случаите) и компарирање со резултати што ќе бидат понудени врз основа на сет одлуки од европските судови и од европската регулатива.

5. Како посебен предизвик е етичноста при дизајнирањето, развивањето и креирањето на овие системи, на сите чинители, особено на развивачите на системите.

6. Како значаен ризик се издвојува безбедноста на овие системи, од аспект на нивна заштита од корисниците, но уште повеќе и заштитата од надворешни напади, односно ризик претставува од една страна можната злоупотреба од корисниците на системите, а од друга страна пробивање на системите однадвор (на пример, преку кибернапади) и евентуално менување на алгоритмите, податоците што се користат за генерирање резултати што може да предизвика огромна штета.

7. Почитувањето на човековите права исто така претставува предизвик при дизајнирањето, развивањето и креирањето алгоритми и системи со вештачка интелигенција наменети да се користат во правосудството. Поради тоа, при креирањето на овие системи мора да се обезбеди дека тие нема да нудат резултати што негативно би влијаеле на човековите права. А воедно и корисниците на овие системи исклучително внимателно мораат да пристапуваат при земањето предвид на понудените резултати и да внимаваат на почитувањето на гарантираните човекови права.

8. Предизвик при дизајнирањето, развивањето алгоритми и системи со вештачка интелигенција претставува и овозможувањето транспарентност. Притоа, ова се однесува и на транспарентните информации при креирањето на системите и при/пред користењето на овие системи, а воедно таа треба да биде остварена и при евентуална надградба и развивање во функција на подобрување на системите.

9. Предизвик и воедно ризик претставува начинот на кој ќе се користат понудените одлуки генерирани од овие системи. Тие мораат да се земаат предвид со голема внимателност и резерва, во функција на насока и понудено решение, кои мораат да бидат проверени преку човечка интервенција од корисникот на системот (професионалец во правосудството).

10. Предизвик ќе биде и контролата на алгоритмите и системите со вештачка интелигенција што би се користеле во правосудството, а во однос на нивната ефикасност и ефективност, како и на вистинитоста и релевантноста на понудените резултати и придобивките и нанесената штета од системите.

ПРЕПОРАКИ

Во овој документ веќе се предложени поголем број препораки во однос на дизајнирањето, развивањето и примената на алгоритми и системи со вештачка интелигенција во правосудство, при што во овој дел ќе ги издвоиме оние препораки што можат да се сметаат за најсуштински.

1. Неопходно е правно регулирање на користењето алгоритми и системи со вештачка интелигенција во РС Македонија, односно **донесување закон** каде што ќе бидат опфатени развивањето и користењето на овие системи за цели на употреба во правосудството.

   Со законското регулирање на системите со вештачка интелигенција ќе се постават јасни правила во однос на основаноста, оправданост за креирање и користење на вакви системи, ќе се постават условите што мораат да ги исполнуваат системите: од аспект на безбедност, почитување на човековите права, етички норми, начин на контрола, процена на ризик и влијание врз човековите права и слободи.

   Притоа, потребно е при донесувањето на овој закон претходно да се направи и процена според Методологија за хармонизација на секторската легислатива донесена од Агенцијата за заштита на личните податоци[60].

2. Понатаму, потребно е да се донесе **национална стратегија** во однос на креирање, развивањето и примената на алгоритми и системи со вештачка интелигенција вклучително и оние што се наменети за користење во правосудството, каде што подетално ќе бидат дадени насоки, како и временска рамка и чекори како и на кој начин државата ќе се справува со овие предизвици и ризици (дизајнирање, области на примена, правила обука на чинителите, контрола и проверка на системите и сл.), заради безбедно и одговорно воведување на овие технологии.

3. Донесување на **Етички кодекс**: Државата да даде посебен осврт на етичките принципи, пред сè, при дизајнирањето и развивањето, како и на корисниците на овие системи, преку изработка и донесување кодекс/етички правила, што ќе вклучува механизми што ќе спречуваат пристрасност и дискриминација во неговиот дизајн што ќе важат во сите области на примена на овие системи, но ќе бидат посебно акцентирани ризичните сектори во кои спаѓа и секторот правосудство.

4. При дизајнирањето, развивањето алгоритми и системи со вештачка интелигенција наменети за употреба во правосудството мора да биде запазено **почитувањето на човековите права**, вклучително и правото на заштита на личните податоци и приватноста доколку овие системи обработуваат лични податоци.

5. При дизајнирањето, развивањето алгоритми и системи со вештачка интелигенција наменети за употреба во правосудството мора да се почитува **транспарентноста** при развивањето, но и при/пред користењето на овие системи.

60 Одлука за утврдување на методологија за хармонизација на секторската легислатива („Службен весник на РС Македонија“, бр. 38/22).

6. Особено понудените резултати при користењето на овие системи во правосудството мораат да овозможуваат **човечка интервенција, проверливост и право на избор**. Понудените резултати мораат да се земаат предвид со голема внимателност и резерва, во функција на насока и понудено решение.

7. Овие системи мораат да бидат безбедни. **Безбедноста при дизајнирањето, развивањето и користењето** алгоритми и системи со вештачка интелигенција наменети за употреба во правосудството е од големо значење, од аспект на нивна заштита од корисниците, но уште повеќе и заштитата од надворешни напади. Секако, предуслов за ова е, пред сè, создавање на ефикасна и доверлива судска дигитална инфраструктура.

8. При дизајнирањето и развивањето алгоритми и системи со вештачка интелигенција наменети за употреба во правосудството мораат да бидат **вклучени сите релевантни чинители**, вклучително и професионалци од правната фела.

9. **Државата треба да обезбеди ресурси:** финансиски, технички, човечки ресурси за дизајнирањето, развивањето и користењето алгоритми и системи со вештачка интелигенција. Воедно, потребна е обука и на дизајнерите/развивачите и на корисниците на овие системи во која ќе бидат опфатени сите аспекти.

10. Корисно би било воведување на сертифицирање на методите на развивање и креирање алгоритми и системи со вештачка интелигенција наменети за користење во правосудството, со цел да се обезбеди **неутралност, непристрасност и стандардизирана рамка од правила** за овие системи, со цел безбедно и одговорно воведување на овие технологии.

11. Потребно е да се испланира и да се имплементира **контролата** на алгоритмите и системите со вештачка интелигенција што би се користеле во правосудството, а во однос на нивната ефикасност и ефективност, како и на вистинитоста и релевантноста на понудените резултати.

12. Исто така, од значење е и правното регулирање на чување податоци, вклучително и личните податоци на територија на РС Македонија, на пример со донесување **закон за државен облак (cloud) лоциран на територијата на РС Македонија**, каде што ќе се чуваат податоците што ги обработуваат институциите од целокупниот јавен сектор на РС Македонија, сè со цел податоците на граѓаните на РС Македонија да бидат безбедни, соодветно заштитени и граѓаните да бидат сигурни дека државата се грижи за заштита на нивните лични податоци.

13. Следствено, потребно е и донесување на национална стратегија за национален облак (cloud) што ќе определи подетално временска рамка, чекорите, начините, мерките, активностите во функција на операционализирање на законската рамка за национален склад на податоци. Исто така, од значење е и донесување на национална стратегија за кибербезбедност за одржувањето на безбедноста и градењето на сигурна дигитална средина за државата и граѓаните, која ќе биде актуелна и соодветна на новите опасности во дигиталниот свет.[61]

61 Националната стратегија за кибербезбедност 2018-2022 веќе не е актуелна, а изработената Национална стратегија за кибербезбедност 2023-2026 сè уште не е усвоена.

14. Државата, при регулирањето на дизајнирањето, развивањето и користењето алгоритми и системи со вештачка интелигенција, треба ја има предвид и **поддршката кон иновативноста и да се стреми кон промовирање и поттикнување иновации** во согласност со човековите права, демократијата и владеењето на правото. Еден соодветен начин да се стимулира одговорна иновација во однос на вештачката интелигенција е овозможување на властите во соодветниот сектор на активност да воспостават „контролирани средини“ или „рамки“ за да овозможат развој, обука, експериментирање во живо и тестирање на иновациите под надзор од надлежните органи – со вклучен директен надзор, особено за да се поттикне инкорпорирањето на квалитетот, приватноста и другите грижи за човековите права, како и загриженоста за безбедноста и безбедноста во раните фази. Ова е особено важно затоа што одредени ризици поврзани со системите за вештачка интелигенција ефективно можат да се решат само во фазата на дизајнирање.

15. Воедно, треба да се истакнат и важноста и потребата од **длабинска јавна дебата** за овие алатки и системи пред спроведувањето на јавните политики за нивното дизајнирање, развивање и користење.

Посебна препорака: За дизајнирање, развивање алгоритми и системи со вештачка интелигенција наменети за употреба во правосудството особено е препорачливо да не се користат лични податоци што ги идентификуваат или можат да ги идентификуваат физичките лица (да се користат мерки за анонимизација, генерализација или рандомизација). Податоците што ќе се користат мораат да бидат соодветни, релевантни, да се користат за целата за која се собрани, при што ќе се применуваат соодветни мерки за нивна безбедност соодветни на ризикот.

ЗАКЛУЧОЦИ

Имајќи ги предвид наведените предизвици и ризици, како и фактичката состојба во технолошката еволуција, општеството сè уште не е подготвено за целосно да ја имплементира вештачката интелигенција во областа на правосудството, без какви било етички грижи и со целосно почитување на човековите права. Затоа постои и загриженост за компатибилноста и имплементацијата на алгоритми и вештачка интелигенција во правосудството. Овие системи во најголемиот број случаи ќе користат профилирање групи и поединци и од таа причина мораат да се вбројат во групата на високоризични.

Но, државата мора да преземе чекори да се подготви за новите технолошки решенија што ги нудат овие системи и да ги детектира нејзините предности и поволности, при што ќе создаде правила за процена на ризиците што ги носат, како и правила каде, за која цел, по која основа, како, со кои мерки и на кој начин можат да се дизајнираат, креираат и користат алгоритми и системи со вештачка интелигенција во правосудството. Секако, во тој процес потребно е да бидат вклучени сите релевантни чинители. И под услов да бидат запазени сите безбедносни, етички, морални, законски правила, сепак вештачката интелигенција сè уште не може да биде поправедна од професионалците во правосудниот систем. Но, секако, доколку овие системи бидат создадени и користени, почитувајќи ги стандардите и правилата, алгоритмите и вештачката интелигенција во правосудството во голема мера можат да помогнат во носењето на поправедни одлуки, при што мора да постои правото на избор, проверливост и човечка интервенција.

Можеби предвидувањата дека за десет години вештачката интелигенција ќе биде поинтелигентна од човечката, ќе се остварат и „машините“ ќе станат попаметни од човекот, но тешко дека „машините“ ќе станат поразумни и поморални од човекот (имајќи предвид дека поимот „интелигенција“ опфаќа и „капацитет за разум“, а моралот вклучува разликување на доброто и лошото). Но, вештачката интелигенција секако може да придонесе човекот да биде поразумен, поефикасен и да носи подобри одлуки, но само доколку овие системи што користат вештачка интелигенција се развиени согласно етички стандарди и утврдени правила.

Човекот е суштество кое има тенденција пронајдоците што биле креирани за да имаат полза за човештвото, да ги пренамени за добивање моќ и деструктивност. Затоа и при употребата на системи за вештачка интелигенција во правосудството што би давале позитивни резултати, мора да постои контрола и преиспитување на користењето и корисноста на овие системи.

Дали во догледно време вештачката интелигенција ќе стане попаметна од човечката интелигенција и дали ќе може да ја предвидува правдата, во најголема мера зависи од човечката интелигенција, односно од податоците, правилата и можностите што човекот ќе ѝ ги даде на вештачката интелигенција?

Можеби ќе дочекаме да видиме дека вештачката интелигенција научила, но и разбрала, што е правда, право, морал, етички вредности, традиционални, социјални и културни белези на нашето општество, па ќе нуди решенија на кои ќе можеме да ги градиме нашите одлуки. Но, особено во правосудството не смееме да дозволиме вештачката интелигенција да одлучува наместо правните професионалци.

Предвидувањата за иднината на вештачката интелигенција се движат од дистописки до утописки сценарија. Можеби вештачката интелигенција ќе стане попаметна од човечката интелигенција, но бидејќи правдата, моралноста, етиката се неразделно поврзани со човековото битисување, однесување и расудување, дискутабилно е дали може да биде поправедна.

Секако, постои можност одговорот на прашањето на Тјуринг „дали машината може да мисли“ да биде позитивен, како и можност за остварување на предвидувањето дека вештачката интелигенција ќе биде попаметна од човечката интелигенција, но имајќи ја предвид човековата природа, сè додека вештачката интелигенција не почне да чувствува, човештвото е безбедно.

Или токму напротив?