Изазови дигиталног друштва

Посебан изазов представља опасност да у будућности роботи развију способност саморепродуковања, евентуално стекну свест и онда закључе да им човек није потребан

НОВЕ ТЕХНОЛОГИЈЕ

*Никола Марковић**

Цивилизација је стигла у фазу када савремене информационе и комуникационе технологије (ИКТ) обезбеђују основну инфраструктуру за свакодневни живот грађана, функционисање државе и јавних служби и обављање привредних делатности. Најмање једна трећина данашње популације не може да замисли живот без коришћења ИКТ опреме (рачунара, мобилних телефона, скенера и сл.) и дигиталних услуга.

Но, последњих година се поред задовољства корисним ефектима дигиталне цивилизације, уочавају и појаве које нису пожељне, представљају ризике, имају нежељене ефекте и манифестују појединачне сукобе с постојећим правним системом, етиком и моралом. Ове појаве представљају изазов, отварају многе дилеме и траже адекватан одговор јавности и државе.

Све ове нежељене појаве, изазови и дилеме могли би да се сврстају у две категорије: изазови и дилеме који су последице неумитности технолошког развоја и злоупотребе тековина технолошког развоја кроз асоцијално и неетичко понашање корисника.

Досадашњи технолошки развој је доносио изузетно велике позитивне ефекте, али се ипак појављују и неки нежељени ефекти, изазови, ризици и штетне појаве као што је опасност да после масовне аутоматизације пословања и дигиталне трансформације пословања дође до раста незапослености. Међутим, и када аутоматизација пословања и посебно роботизација постану масовне појаве, поставља се питање да ли ће због потпуне аутоматизације послова доћи до појаве глобалне незапослености. У фабрикама будућности ће претежно радити роботи, а човек ће служити само за надзор и сервисирање робота, и то све дотле док роботи не преузму и ту функцију. Посебан изазов представља опасност да у будућности роботи развију способност саморепродуковања, евентуално стекну свест и онда закључе да им човек није потребан. Социолог Питер Сингер се пита: „Шта ће бити кад суперинтелигентне машине закључе да су им људи сувишни?"

Имплантати у мозгу

Дозвољен, недозвољен и невидљив надзор над људима се шири и представља све већу опасност за приватност. Дозвољени надзор, односно евидентирање личних података, регулисано је законима или сагласношћу грађана. Међутим, расту недозвољени видео-надзори, прислушкивање, крађа идентитета и др. Невидљиви надзор се одвија преко сателита и разних сензора који се подмећу у разним електронским уређајима, а које користе обавештајне службе, детективске агенције, конкурентске фирме и други.

Социјални инжењеринг подразумева психолошко манипулисање људима коришћењем скривених намера. Циљ је масовна обмана становништва ради политичких или пословних интереса. Користе се медији, у последње време све више интернет и друштвене мреже. Рачуна се на људске слабости као што су: лаковерност, егзистенцијални страх, површност, необразованост, преокупираност личним проблемима и сл. Ангажују се спин доктори, ботови, корисни идиоти и сл. Ефекат је масовно обмањивање становништва. Данашње велике друштвене супротности између народа и држава управо су резултат примене друштвеног инжењеринга преко интернета и друштвених мрежа.

Вештачка интелигенција је област рачунарства која се брзо развија и која се заснива на развоју интелигентног хардвера и софтвера који ради и реагује као људи. Користи се за планирање, управљање, препознавање говора, учење и сл. Србија је усвојила Стратегију развоја вештачке интелигенције за период 2020–2025. и има Институт за вештачку интелигенцију. Предвиђене су примене у области јавне управе (убрзање рутинских послова), здравства (рана дијагноза), саобраћај (оптимизација саобраћаја) и развоју нових производа и услуга.

Проширена стварност је област рачунарске технологије која се бави допуњавањем физичке стварности новим елементима на повећавању људске интелигенције имплантатима у људски мозак. Тиме се бави и Илон Маск у компанији „Неуролинк" у САД у настојању да преко можданих чипова повеже човека и компјутер. У оквиру Система за вештачки вид ИЦВП (Intracortical Visual Prothesis) оперативним путем је успешно уграђен чип у мозак првог пацијента у Прицкер институту за биомедицинске науке и инжењеринг у Илиноису. У току су припреме за све масовнију примену разних имплантата у људском организму. То у перспективи може да доведе до развоја „киборга" (пола човек, пола машина). Овим се покреће низ социјалних и етичких питања и дилема за будућност човечанства у погледу граница хумане примене дигиталних имплантата.

Заштита приватности и личних података се налази пред све већим изазовима. Лични подаци се налазе у многобројним компјутеризованим евиденцијама о грађанима, од којих неке нису довољно заштићене. Лични подаци се неодговорно остављају на друштвеним мрежама и компјутеризованим апликацијама и комуникацијама. Развијена су решења за видеонадзор на јавним местима, а технологија препознавања лица (Facial Recognition Technology) лако може да буде злоупотребљена у незаконитој идентификацији личности. Примена технологије препознавања лица и видео-надзора нису регулисани у већини држава и представљају велику опасност да се успостави друштво тоталног надзора над људима.

Крађа идентитета

Млађа популација показује све већу зависност, јер проводи дневно у просеку око четири сата користећи пре свега мобилни телефон и његове сервисе за информисање и забаву, и то на рачун одмора, корисног рада, друштвених веза и сл. Расте и број оних који су толико зависни да се то манифестује као болест.

Технолошки развој у области ИКТ се убрзава и изгледа да у све више подручја не може више да се контролише и усмерава, па се развија спонтано логиком научнотехнолошке знатижеље научника и иноватора, интереса власника институција, потреба обавештајних служби, борбе за профит, интереса за доминацију и сл.

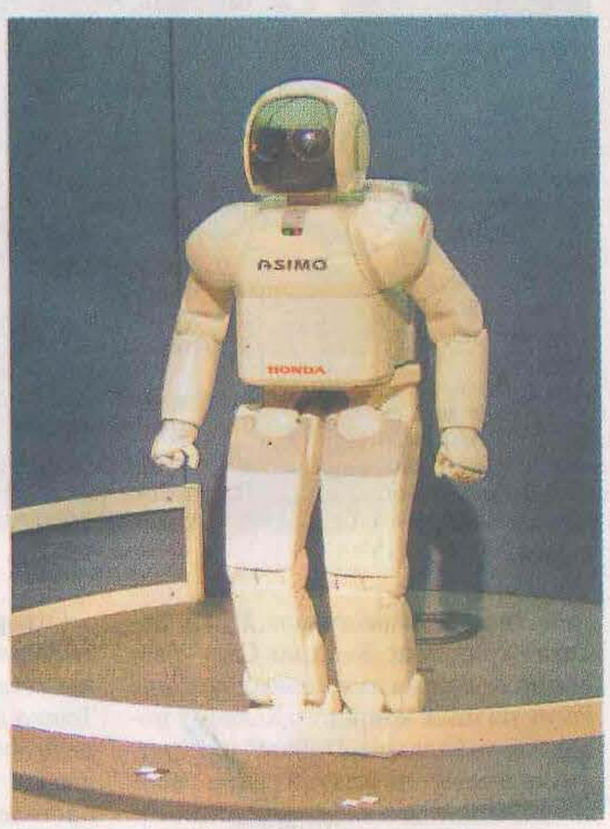
За даљи развој цивилизације важно је ко и за шта користи врхунска технолошка знања. Опасност је да се до неких знања и технологија домогну и почну да их користе криминалци, недемократски режими и болесни појединци.

Последњих година уочава се пораст злоупотреба и нежељених ефеката из примена технолошког развоја, посебно у примени ИКТ. Користе се могућности за стварање лажног идентитета, крађе идентитета, спамовања, ширење лажних вести, спиновања, развоја сајбер криминала и сајбер силеџијства, девијантног сексуалног понашања појединаца, злоупотребе личних података, сајбер тероризма, сајбер претњи, фалсификовања слика и видео-записа и др. То све доводи до угрожавања сајбер безбедности држава, компанија и појединаца и појаве нових видова вређања људског достојанства и угрожавања функција државе и пословања у привреди и других нежељених ефеката.

Неке од штетних појава су:

Сајбер криминал – противзаконито понашање појединаца или група који рачунаре користе за оштећење рачунарских података и програма, крађу података и новца, прављење рачунарских вируса, организацију рачунарске саботаже, неовлашћен приступ информационим системима и сл.

Сајбер силеџијство – употреба ИКТ, посебно друштвених мрежа, ради грубог, силеџијског, хулиганског, увредљивог и некоректног понашања с намером да се повреде појединац или група.



Хуманоидни робот Фото Википедија/CC BY SA 3.0

Мере за смањивање нежељених појава

Спамовање је противзаконита, непрофесионална и некултурна активност слања незатражених порука. Најчешће се користи за слање незатражених реклама, малвера, интернет преваре и др. У Србији је спамовање већ регулисано као прекршај, али се прекршиоци врло ретко гоне.

Спиновање је слање вести базираних на лажним вестима или полуистини у циљу обмане јавности за потребе неког политичког или економског интереса и користи се на појединим друштвеним мрежама, у таблоидима и др.

Spyware (шпијунски софтвер) врста је злонамерног софтвера који служи за праћење активности корисника без његовог знања и слања података нападачу. Он се најчешће инсталира уз бесплатни софтвер и користи за крађу лозинки, бројева платних картица и сл.

Постоји још читав низ других манифестација злоупотреба ИКТ од стране појединаца и организација. Оне су у порасту и представљају све већу друштвену опасност.

Ширење нежељених појава утицало је на успостављање мера и активности у циљу сузбијања или умањивања њихових ефеката. Неке од потребних мера су развој етике дигиталног друштва, примена и развој техничких мера заштите података, креирање адекватних мера у оквиру правног система, дигитално васпитање и образовање, развој одговорности и способности корисника високих технологија за њихову исправну примену и сл.

Потребно је развијати и примењивати техничке мере заштите података као што су добре шифре и лозинке, резервне копије, криптовање података, заштитни зид (firewall), рачунари изван мреже (air gapping) и др.

ИКТ системи од посебног значаја дужни су да донесу и примењују Акт о безбедности и провери безбедности, сагласно Закону о информационој безбедности, који је усвојен 2016. године. Овим се регулишу питања као што су заштита од губитака података, безбедност ресурса ИКТ система, провера