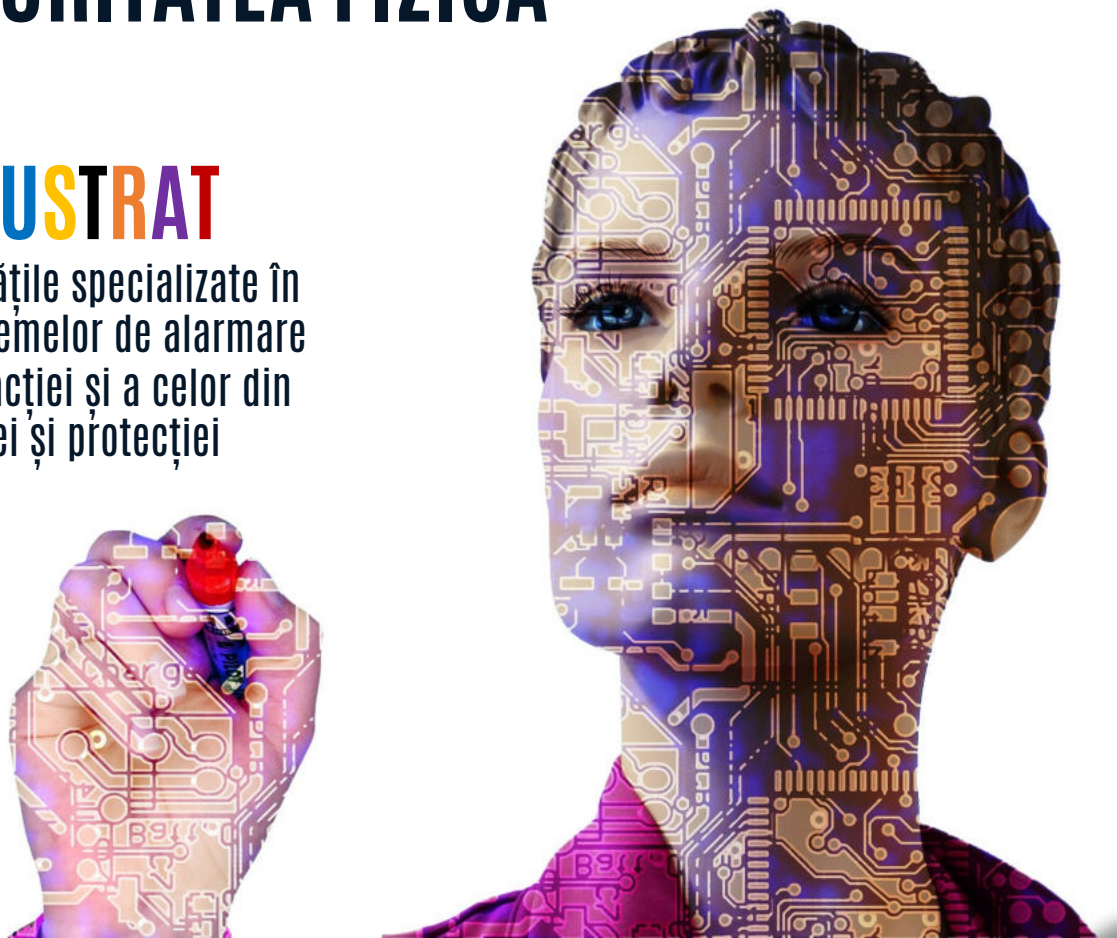
Ion Iordache
Alexandru Mihai Caplescu

INTELIGENTA ARTIFICIALĂ
ÎN SECURITATEA FIZICĂ

GHID ILUSTRAT

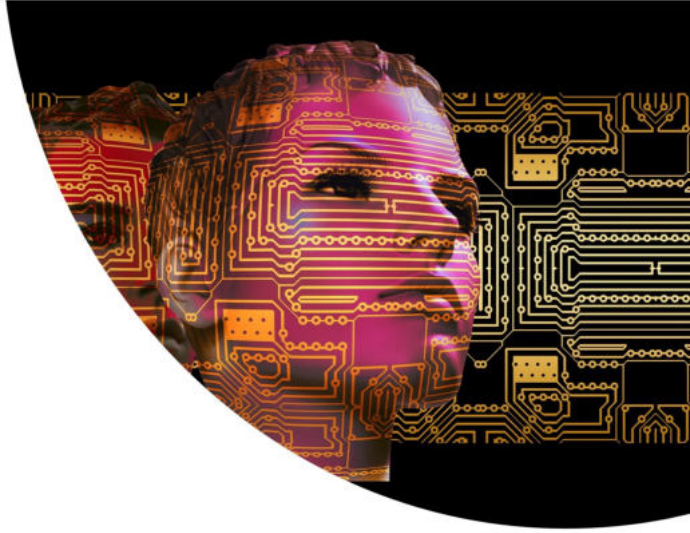
pentru societățile specializate în domeniul sistemelor de alarmare împotriva efracției și a celor din domeniul pazei și protecției



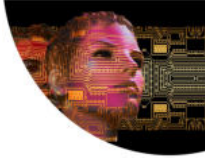
Principalele riscuri legate de utilizarea IA vizează aplicarea normelor menite să protejeze drepturile fundamentale (cum ar fi protecția datelor cu caracter personal și a vieții private și nediscriminarea), precum și aspectele legate de siguranță și de răspundere.

Colectarea și utilizarea datelor biometrice pentru identificarea la distanță, de exemplu prin implementarea recunoașterii faciale în locurile publice, prezintă riscuri specifice pentru drepturile fundamentale."

(Cartea albă inteligența artificială)



CUPRINS



INTRODUCERE

Prima data a fost șahul...

sau mai bine zis, totul a început la 11 mai 1997, data în care campionul mondial la șah, Garry Kasparov, a fost învins de supercomputerul „Deep Blue" construit de IBM. Tot de atunci a început și confuzia a ceea ce poate face noua tehnologie deși conceptul de "inteligență artificiala" (IA) este mult mai vechi, domeniul cercetării IA având bazele la un workshop organizat la Colegiul Dartmouth în 1956 tot atunci fiind fondat și ca disciplină academică.

Ceea ce se considera, însă, în anii '50 inteligență artificială, astăzi nu mai este deloc o tehnologie avansată, acest fenomen fiind cunoscut sub numele de "paradoxul ciudat" adică odată ce noile tehnologii devin parte a vieții noastre cotidiene, ele devin invizibile pentru noi și nu le mai percepem ca fiind parte a inteligenței artificiale. (21)

În domeniul securității, una dintre confuziile actuale este agravată, de conceptul de recunoaștere facială cu care IA este asociat. Despre acest subiect și confuziile generate voi avea o prezentare mai amplă în acest material.

În prezent, UE consideră că *"IA este o parte importantă a transformării digitale a societății. Viața fără utilizarea IA în producerea multor bunuri și servicii este dificil de imaginat, multe schimbări în ceea ce privește munca, afacerile, finanțele, sănătatea, securitatea, agricultura și alte domenii fiind pe cale de a se produce." (1)*

Inteligența artificială (IA) „tehnologie determinantă a viitorului"

Deși descrierea concretă a inteligenței artificiale nu este ușor de făcut pentru că, așa cum spune Ammy Webb(21) "ea reprezintă multe lucruri diferite", Uniunea Europeană a sintetizat-o în următoarea descriere, inclusiv cu o descriere a tipurilor de IA:

"IA este capacitatea unei mașini de a imita funcții umane, cum ar fi raționamentul, învățarea, planificarea și creativitatea. IA permite sistemelor tehnice să perceapă mediul în care funcționează, să prelucreze această percepție și să rezolve probleme, acționând pentru a atinge un anumit obiectiv. Calculatorul primește datele (deja pregătite sau colectate prin intermediul propriilor senzori, cum ar fi o cameră video), le prelucrează și reacționează. Sistemele IA sunt capabile să își adapteze, într-o anumită măsură, comportamentul, analizând efectele acțiunilor anterioare și funcționând autonom." (2)

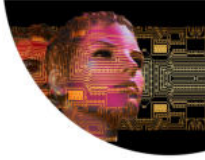
Tipuri de IA (definiția CE)

- **Software:** asistenți virtuali, programe informatice de analiză a imaginilor, motoare de căutare, sisteme de recunoaștere vocală și facială.
- **IA încorporată:** roboți, automobile autonome, drone, internetul obiectelor

O serie de sisteme tehnologice integrate ajută securitatea fizică să fie eficientă în problema siguranței publice și a combaterii criminalității din localități sau din diferite alte obiective. Este vorba, în special, de integrarea datelor colectate în timp real de diferiți senzori și camere de supraveghere, conectivitatea omniprezentă și platformele de date deschise, transparente și accesibile.

Toate acestea, siguranța cetățenilor, a bunurilor și persoanelor din diferite organizații și companii vin însă cu un preț legat de confidențialitate și protecția datelor personale.

IMPORTANT! Vă rog, pe toți cei care veți citi acest document, să luați în calcul sursele mele de informare pe care le-am prezentat în capitolul "Bibliografie" pentru că așa veți înțelege corect tot ceea ce am sintetizat eu aici.
Vă mulțumesc!



SECȚIUNEA 1
Abordarea europeană privind inteligența artificială

Foto: Capri23auto (Pixabay)

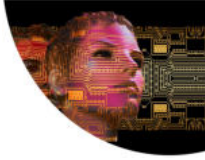
În luna aprilie a acestui an (2021), mass-media prezenta *"un document revoluționar privind inteligența artificială"* emis de Comisia Europeană prin care a fost propus un set de acțiuni menite să stimuleze excelența în domeniul IA și norme care să asigure fiabilitatea tehnologiei garantând prin acestea siguranța și drepturile fundamentale ale cetățenilor și întreprinderilor, consolidând, în același timp, investițiile și inovarea în toate țările UE.

Din păcate, majoritatea acestor infomări au pus accentul pe senzațional, dovedind că autorii articolelor ori n-au citit toată documentația ori au ales doar părțile cu tentă de senzațional întrebându-se chiar din titlu, de exemplu dacă *"Preiau roboții controlul?" [18]* întrebare fără nicio legătură cu subiectul extrem de serios care trebuia prezentat.

Comisia Europeană propune noi norme și măsuri menite să transforme Europa în polul mondial al unei inteligențe artificiale (IA) de încredere.

Îmbinarea primului cadru juridic privind IA cu un nou plan coordonat cu statele membre va garanta siguranța și drepturile fundamentale ale cetățenilor și ale întreprinderilor, consolidând totodată adoptarea IA, precum și investițiile și inovarea în domeniul IA în întreaga UE.

Existența unor tehnici fiabile de inteligență artificială (IA) poate aduce numeroase beneficii: asistență medicală mai bună, procese de fabricație mai eficiente, un transport mai sigur și mai curat, surse de energie mai ieftine și mai durabile dar și o securitate mai eficientă a cetățenilor și a bunurilor acestora. Abordarea UE cu privire la inteligența artificială (IA) are scopul de a convinge cetățenii să adopte aceste tehnologii și, în același timp, să încurajeze întreprinderile să le dezvolte.



SECȚIUNEA 1

Abordarea europeană privind inteligența artificială

Cartea albă privind inteligența artificială - o abordare europeană axată pe excelență și încredere

În **"Cartea albă Inteligența artificială – O abordare europeană axată pe excelență și încredere"** din 19.02.2020, Comisia Europeană în parteneriat cu sectorul privat şi cel public, urmăreşte să mobilizeze resurse de-a lungul întregului lanţ valoric şi să creeze stimulentele potrivite pentru a accelera introducerea şi utilizarea IA, inclusiv de către întreprinderile mici şi mijlocii.


COMISIA EUROPEANĂ

Bruxelles, 19.2.2020
COM(2020) 65 final

CARTE ALBĂ

Inteligența artificială - O abordare europeană axată pe excelență și încredere

Se precizează în mod direct că "având în vedere impactul major pe care IA îl poate avea asupra societății noastre și necesitatea asigurării încrederii, este esențial ca, la nivel european, IA să se bazeze pe valorile și drepturile noastre fundamentale, cum ar fi demnitatea umană și protecția vieții private."

Riscurile pentru drepturile fundamentale, inclusiv protecția datelor cu caracter personal și a vieții private și discriminarea.

Principalele riscuri legate de utilizarea IA vizează aplicarea normelor menite să protejeze drepturile fundamentale (cum ar fi protecția datelor cu caracter personal și a vieții private și nediscriminarea), precum și aspectele legate de siguranță și de răspundere.

IA oferă posibilități sporite de a urmări și de a analiza obiceiurile zilnice ale oamenilor. De exemplu, există riscul potențial ca IA să fie utilizată, cu încălcarea normelor privind protecția datelor și a altor norme ale UE, de către autoritățile de stat sau de către alte entități pentru supravegherea în masă, iar de către angajatori pentru a observa modul în care se comportă angajații.

În cazul sistemelor cu risc ridicat, cum ar fi cele din domeniul securității acestea ar trebui să fie transparente, trasabile și să garanteze supravegherea umană.

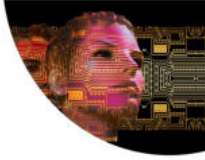
De exemplu, recunoașterea facială care poate avea diferite forme, poate fi utilizată pentru autentificarea utilizatorului pentru, de exmplu verificare/autentificare la intrarea în diferite instituții pentru a verifica identitatea unei persoane în raport cu nivelul său de acces (corelare unu-la-unu) dar recunoaşterea facială ar putea fi utilizată şi pentru identificare biometrică la distanţă, atunci când imaginea unei persoane este verificată într-o bază de date *("corelare unu-la-o mulțime")*.

Atenție! Aceasta este cea mai agresivă formă de recunoaștere facială iar Regulamentul general privind protecția datelor (GDPR) interzice deja prelucrarea datelor biometrice cu scopul unic de identificare a unei persoane fizice, cu excepţia cazului în care sunt îndeplinite anumite condiţii.

Utilizarea aplicațiilor IA în scopul identificării biometrice la distanță și al altor tehnologii de supraveghere intruzivă ar fi întotdeauna considerată „cu risc ridicat".

Este important de precizat că *"identificarea biometrică la distanță ar trebui să fie diferențiată de autentificarea biometrică (acesta din urmă este un proces de securitate care se bazează pe caracteristicile biologice unice ale unei persoane pentru a verifica dacă aceasta este cine spune că este). În cazul identificării biometrice la distanță, identitatea mai multor persoane este stabilită cu ajutorul elementelor biometrice (amprente digitale, imagini faciale, iris, modelele venelor etc.) la distanță, într-un spațiu public și în mod continuu sau permanent, prin verificarea lor în comparație cu datele stocate într-o bază de date." [19]*

Pentru susține prevederile din Cartea albă privind inteligența artificială România a a adoptat Hotărârea nr. 28 din 8 septembrie 2020 privind adoptarea opiniei referitoare la Cartea albă - Inteligența artificială - O abordare europeană axată pe excelență și încredere - COM (2020) 65.



SECȚIUNEA 1
Abordarea europeană privind inteligența artificială

Excelență și încredere în inteligența artificială (I)

„Inteligența artificială reprezintă un mijloc, nu un scop în sine. Este prezentă în viața noastră de zeci de ani, însă în momentul de față a atins noi capacități, alimentate de puterea de procesare, oferind un potențial imens în domenii foarte diverse, cum ar sănătatea, transporturile, energia, agricultura, turismul sau securitatea cibernetică. Totodată, inteligența artificială implică o serie de riscuri. Propunerile prezentate astăzi au ca obiect să consolideze poziția Europei în calitate de pol mondial al excelenței în domeniul inteligenței artificiale, de la laborator la piață, să asigure faptul că, în Europa, inteligența artificială respectă valorile și normele noastre și să valorifice potențialul inteligenței artificiale pentru utilizare industrială."

(Comisarul pentru piața internă, Thierry Breton)

Înainte de a putea fi introduse pe piață, sistemele de IA care prezintă un grad ridicat de risc vor face obiectul unor **obligații stricte**, astfel încât să se asigure următoarele:

- **sisteme adecvate de evaluare și reducere a riscurilor;**
- **calitatea ridicată a seturilor de date** care alimentează sistemul, pentru a se reduce la minimum riscurile și rezultatele discriminatorii;
- **înregistrarea activității** pentru a asigura trasabilitatea rezultatelor;
- **documentația detaliată** care să furnizeze toate informațiile necesare privind sistemul și scopul acestuia, pentru ca autoritățile să poată evalua conformitatea sistemului în cauză;
- **informații clare și adecvate** pentru utilizatori;
- **măsuri** care să garanteze o **supraveghere umană corespunzătoare**, în vederea reducerii la minimum a riscului;
- **un nivel ridicat** de robustețe, securitate și precizie.

În special, se consideră că toate sistemele de identificare biometrică la distanță prezintă un grad ridicat de risc și fac obiectul unor cerințe stricte.
În principiu, este interzisă utilizarea lor în timp real în spații accesibile publicului în scopuri de asigurare a respectării legii.

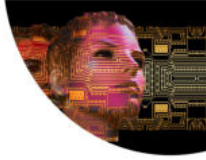
Consolidarea încrederii prin intermediul primului cadru juridic privind IA

Noile reguli vor fi aplicate pretutindeni în UE, cu o abordare bazată pe niveluri de risc clasificate astfel:

Risc inacceptabil - Orice aspect considerat a fi o amenințare clară la adresa cetățenilor UE va fi interzis: sistemele bazate pe IA considerate o amenințare clară pentru securitate, mijloace de trai și drepturile oamenilor cum ar fi, de exemplu, sisteme sau aplicații IA care manipulează comportamentul uman pentru a eluda liberul arbitru al utilizatorilor cum ar fi jucăriile care folosesc asistența vocală pentru a încuraja comportamentul nesigur al minorilor sau sistemele care permit guvernelor să efectueze o evaluare a comportamentului social („social scoring").

Risc ridicat - Sunt considerate ca prezentând un grad ridicat de risc sistemele în care tehnologia IA este utilizată în:

- **infrastructurile critice** (de exemplu, transporturile), care ar putea pune în pericol viața și sănătatea cetățenilor;
- **formarea educațională sau profesională**, care poate determina accesul la educație și traiectoria profesională a unei persoane (de exemplu, sistemul de notare utilizat în cadrul examenelor);
- **componentele de siguranță ale produselor** (de exemplu, o aplicație a IA utilizată în chirurgia robotică);
- **ocuparea forței de muncă, gestionarea lucrătorilor și accesul la activități** independente (de exemplu, software de selecție a CV-urilor pentru procedurile de recrutare);
- **serviciile publice și private esențiale** (de exemplu, evaluarea bonității care îi împiedică pe cetățeni să aibă posibilitatea de a obține un împrumut);
- **activitatea de asigurare a respectării legii care poate aduce atingere drepturilor fundamentale ale cetățenilor** (de exemplu, evaluarea fiabilității probelor);
- **gestionarea migrației, a azilului și a controlului la frontiere (**de exemplu, verificarea autenticității documentelor de călătorie);
- **administrarea justiției și procesele democratice** (de exemplu, aplicarea legii în cazul unui set concret de date factuale).



SECȚIUNEA 1
Abordarea europeană privind inteligența artificială

Excelență și încredere în inteligența artificială (II)

Pentru sistemele de identificare biometrică la distanță sunt prevăzute câteva excepții limitate, strict definite și reglementate (cum ar fi utilizarea în cazurile în care este strict necesar pentru a căuta un copil dispărut, pentru a preveni o amenințare teroristă specifică și iminentă sau pentru a detecta, a localiza, a identifica sau a urmări în justiție persoane care au comis ori sunt suspectate că au comis infracțiuni grave).

O astfel de utilizare este condiționată de obținerea unei autorizații din partea unui organism judiciar sau a unui alt organism independent și de termene adecvate, de acoperirea geografică și de bazele de date în care se efectuează căutări.

Risc limitat - Sistemele de IA care fac obiectul unor obligații specifice în materie de transparență: atunci când utilizează sisteme de IA, cum ar fi roboții de chat, utilizatorii ar trebui să fie conștienți de faptul că interacționează cu un aparat, astfel încât să aibă posibilitatea de a lua o decizie în cunoștință de cauză *(fie să folosească în continuare respectivul sistem de IA, fie să renunțe la serviciile acestuia)*.

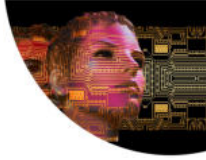
Risc minim - Utilizarea gratuită a unor aplicații precum jocurile video sau filtrele spam bazate pe IA.

Marea majoritate a sistemelor de IA se încadrează în această categorie. Prin urmare, noile norme nu li se aplică, deoarece în cazul acestor sisteme riscul la adresa drepturilor sau siguranței cetățenilor este fie minim, fie inexistent.

Noi norme pentru furnizorii de sisteme de IA cu risc ridicat

Etapa 1	Etapa 2	Etapa 3	Etapa 4	
Se dezvoltă un sistem de IA cu grad ridicat de risc	Sistemul trebuie să facă obiectul unei evaluări a conformității și să respecte cerințele în materie de IA Pentru unele sisteme este implicat un organism notificat	Se înregistrează sistemele de IA autonome într-o bază de date a UE	Trebuie semnată o declarație de conformitate, iar sistemul de IA ar trebui să poarte marcajul CE. Sistemul poate fi introdus pe piață	*Dacă apar schimbări substanțiale în ciclul de viață al sistemului de IA, se revine la etapa 2*

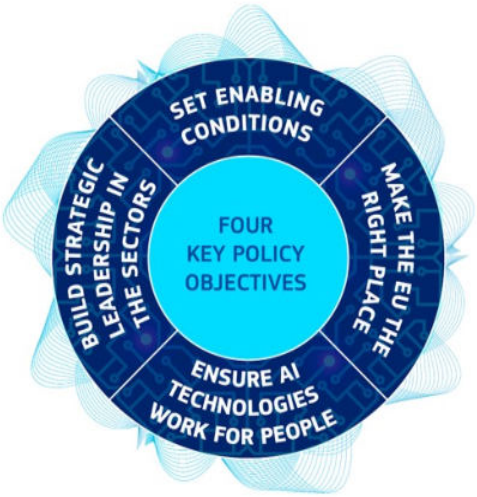
Sursa: [17] Excelență și încredere în inteligența artificială



SECȚIUNEA 1
Abordarea europeană privind inteligența artificială

Excelență și încredere în inteligența artificială (III) Promovarea excelenței în domeniul IA

Actualizarea din 2021 a Planului coordonat privind IA pune strategia în practică și este conformă cu dubla prioritate digitală și verde a Comisiei, precum și cu răspunsul Europei la pandemia de COVID-19.



Principalele obiective de politică:

- stabilirea condițiilor favorabile pentru dezvoltarea și adoptarea IA
- consolidarea poziției de lider strategic în sectoarele cu impact puternic
- transformarea UE într-un loc prielnic pentru IA
- garantarea faptului că tehnologiile IA sunt în beneficiul cetățenilor

Sursa: [17] Excelență și încredere în inteligența artificială

Beneficiile inteligenței artificiale

UE are potențialul de a deveni lider mondial în domeniul inteligenței artificiale sigure. Elaborând un cadru solid de reglementare, bazat pe drepturile omului și valorile fundamentale, UE poate dezvolta un sistem de IA care să le aducă beneficii cetățenilor, întreprinderilor și administrațiilor publice.

IA și UE în cifre

1 miliard EUR
Comisia intenționează să investească 1 miliard EUR pe an în IA din bugetele programelor Europa digitală și Orizont Europa.

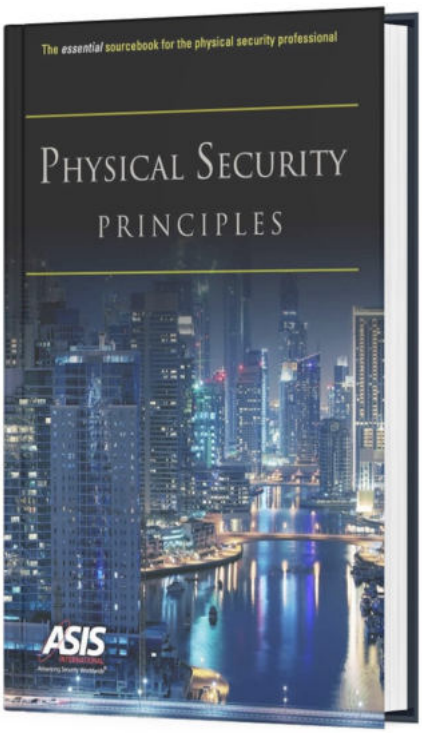
20 de miliarde EUR
Scopul este ca domeniul IA să atragă investiții totale de peste 20 de miliarde EUR pe an în cursul acestui deceniu. Mecanismul de redresare și reziliență va contribui la accelerarea investițiilor și chiar la depășirea obiectivului propus.

> 25%
din toți roboții industriali și personali sunt fabricați în Europa.

Sursa: [17] Excelență și încredere în inteligența artificială

SECȚIUNEA 2
Ce este securitatea fizică și securitatea IA

În legislația din România termenul de securitate fizică este definit ca ***"starea de fapt în care riscul determinat de factorii de amenințare și vulnerabilitățile care pot pune în pericol viața, integritatea corporală sau libertatea persoanei ori pot aduce prejudicii valorilor deținute de unități se situează la un nivel acceptabil."*** *(Instrucțiunile nr. 9 din 1 februarie 2013 privind efectuarea analizelor de risc la securitatea fizică a unităților ce fac obiectul Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor și protecția persoanelor).*



Conform ASIS International, cea mai importantă organizație profesională pentru profesioniștii în securitate din lume, prin securitate fizică se înțelege ***"acea parte a securității care se referă la măsurile fizice menite să protejeze oamenii; pentru a preveni accesul neautorizat la echipamente, facilități, materiale și documente; și pentru a le proteja împotriva unui incident de securitate."*** *[ASIS GDL FPSM-2009].*

După cum vedeți, cele două definiții nu se exclud ci se completează reciproc, profesioniștii în securitate lucrând cu ambele.

Securitatea fizică are două componente de bază cum ar fi **supravegherea** care include alarme antiefracție, supraveghere video sau agenți de securitate și **controlul/admiterea accesului** care include orice barieră de pătrundere în zona supravegheată.

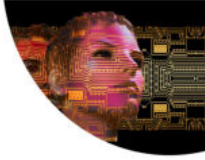
Securitatea IA se referă la instrumente și tehnici care utilizează inteligența artificială pentru a identifica în mod autonom și/sau a răspunde la potențiale amenințări de securitate fizică și/sau cibernetice pe baza activității similare sau anterioare.

Cele mai multe și mai accesibile instrumentele de securitate IA funcționează pentru a descoperi, a prezice, a justifica, a acționa și a afla despre potențiale amenințări la adresa securității fizice și/sau cibernetice, fără a fi nevoie de o intervenție umană prea mare.
Un sistem de admitere acces pe baza unei baze de date poate identifica rapid dacă o persoană are autorizație să intre în zona protejată și să decidă, de exemplu, dacă aceasta este validă sau nu între anumite ore dacă "învățarea" s-a făcut pe baza comportamentului din trecut.
Practic, pe baza acestui comportament din trecut, IA poate crea și acționa în baza unui un context atunci când i se prezintă informații/comportamente noi.

Fac precizarea că termenul de "control acces" utilizată în absolut toate evaluările, proiectele și/sau rapoartele de securitate ar trebui utilizat doar atunci când se referă la detectarea materialelor, substantelor, obiectelor care sunt sau pot deveni un pericol pentru organizatia interesata. În principal, este vorba de descoperirea materialelor interzise: munitie, armament, explozibili, substante halucinogene, radioactive sau toxice.

Pentru toate activitățile care constau în identificarea unei persoane cu o baza de date de cunostinte, pentru permiterea sau interzicerea patrunderii în obiectivul controlat, recomand utilizarea termenului de "admitere acces".

Concluzia este una foarte clară: atacurile fizice pot provoca pagube însemnate și chiar rănirea gravă sau chiar moartea unor persoane; așa că trebuie să existe o securitate foarte bună pentru a le ține la distanță și a evita riscurile oricărei agresiuni.



SECȚIUNEA 2
Ce este securitatea fizică și securitatea IA

Conectarea securității fizice cu IA

Se poate defini sistemul de securitate integrat ca fiind o platformă de securitate care oferă caracteristici de securitate pe mai multe straturi, unii specialiști fiind de acord ca sistemele de securitate integrate sunt multiplicatori de forță pentru că pot extinde aria de acoperire a personalului de securitate, de exemplu prin alertarea sa cu privire la comportamente suspecte sau inadecvate utilizând supravegherea video, subsistemele de control/admitere acces sau subsistemele de alarmare la efracție.

Tot mai frecvent, aceste sisteme integrate de securitate sunt conectate la programe și aplicații de inteligență artificială care preiau din rolul agentului de securitate deși există și unele lacune în funcționare.

Uneori, de exemplu, se produc alarme false pentru că IA nu recunoște când apare o eroare în sistemul de supraveghere video dacă în acesta a fost setată o alarmă care ar putea provoca o serie de alarme false mari consumatoare te timp pentru a fi verificate.

Concluzia este că integrarea subsistemelor de securitate video, alarmare la efracție, și a controlului/admiterii accesului într-o singură platformă (hardware/software) permite o utilizare mult mai eficientă a personalului de securitate.

În următoarea perioadă, și nu vorbesc despre un interval mare de timp, IA va schimba modul în care oamenii văd securitatea în ansamblul său. Fără prea multe forțe de securitate umană, aplicațiile IA vor putea pune în funcțiune mijloace eficiente de protecție a persoanelor sau a bunurilor acestora.

Controlul/admiterea accesului, așa cum am mai precizat, are rolul de a permite sau interzice pătrunderea în anumite locuri dar acest lucru făcut doar cu operator uman nu elimină toate vulnerabilitățile. Operatorul uman poate face diverse compromisuri sau pur și simplu nu este atent la tot ceea ce se întâmplă dar IA utilizată pentru a admite/interzice accesul va crea alerte în situația detectării unei posibile amenințări și va efectua opriri de urgență sau blocaje în zona respectivă.

Pentru operațiunile de prevenire și detectare a criminalității, inteligența artificială este concepută pentru a învăța diferite sarcini schimbătoare și/sau repetitive care se desfășoară în cadrul sistemului; utilizând o serie de algoritmi aceîtia îi permite să distingă și să detecteze personal neautorizat din numeroasele persoane înregistrate.

În concluzie: inteligența artificială va ajuta la luarea unor decizii eficiente crescând foarte mult capacitatea de răspun la diferite incidente.

Una dintre problemele unui sisteme de supraveghere video este aceea că numărul de persoane care să vadă imaginile în timp real și/sau înregistrările este limitat iar asta înseamnă că analiza imaginilor se va face după ce infracțiunea a avut loc. Avantajul utilizării unui instrument video analitic bazat pe IA este că toată această analiză se face în timp real făcând astfel posibilă intervenția promptă a forțelor de intervenție.

Utilizarea dronelor în operațiuni de supraveghere, căutare și salvare este tot mai des întâlnită în controlul mulțimilor la diferite evenimente, în centre comerciale sau parcuri de agrement mai ales acolo unde personalul de securitate este deficitar.

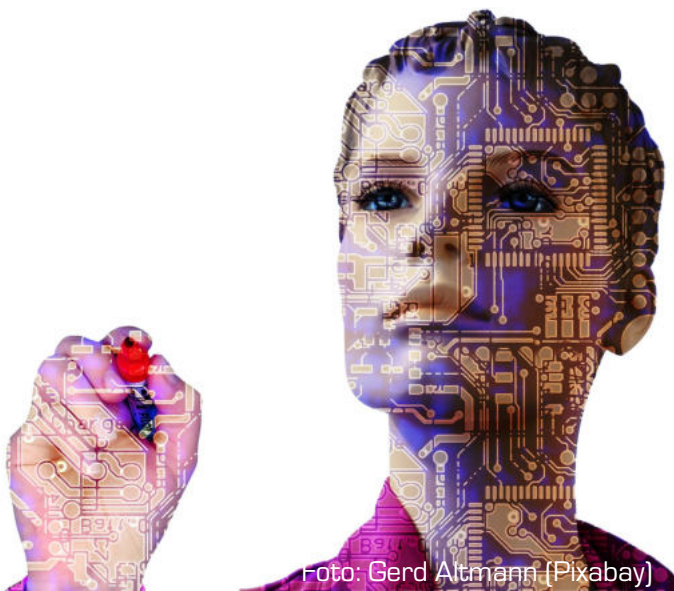
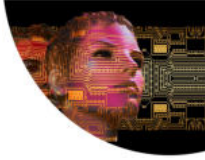


Foto: Gerd Altmann (Pixabay)



SECȚIUNEA 2

Ce este securitatea fizică și securitatea IA

Cum ajută AI securitatea fizică să facă locurile publice mai sigure (I)

Din ce în ce mai des întâlnesc situații în care primarii localităților, mai mari sau mai mici situate atât în mediul urban cât și în mediul rural sunt extaziați de introducerea supravegherii video în localitățile lor.

Pentru asta scriu cu frenezie proiecte pentru a primi finanțare europeană să instaleze cât mai multe camere, neapărat cu "face recognition" pentru a-i prinde pe infractori încă dinainte ca ei să treacă la fapte.

Lăsând la o parte faptul că majoritatea habar n-au despre ce anume vor să facă, dacă încalcă vre-o lege sau nu, că au sau n-au consilieri buni pe acest subiect, nevoia de a proteja viețile cetățenilor, bunurile acestora și bunurile comunității este reală și este esențială.

Aici intervin cerințele unui "smart city" de a asigura securitatea și siguranța propriilor cetățeni unde supravegherea este intensificată de inteligența artificială care poate clasifica oameni, animale, vehicule și obiecte statice pentru a detecta anomalii, adică poate determina ceea ce este considerat normal și poate semnala un comportament suspect pentru ca acesta să fie urmărit.

De exemplu, *"în anumite situații, din cauza calității video slabe, a iluminării deficitare sau a unghiurilor camerei, imaginile de la camerele de supraveghere pot fi de calitate scăzută. IA poate ajuta la reconstituirea imaginilor din camerele de supraveghere video neclare, permițând persoanelor autorizate să vadă mai bine filmările"*. (14)

Echipamentele de securitate fizică acoperă o gamă largă de aplicații menite să descurajeze infractorii. Supravegherea video, de exemplu este utilizată de multă vreme în locuri precum aeroporturi, hoteluri, magazine, mall-uri și aproape oriunde în altă parte se adună oameni sau se vând bunuri.

Astăzi, IA intervine și oferă un ajutor important securității fizice prin operațiuni de supraveghere a mulțimilor și a împrejurimilor detectând și prevenind amenințările. Totul se face utilizând tehnologii video performante, exemplul dat mai devreme cu "face recognition" fiind, într-adevăr, una dintre cele mai adoptate tehnologii în aeroporturi, de exemplu.

Călătorind frecvent în ultimii zece ani între România și Australia, am observat cum treptat noile tehnologii IA de ***"face recognition"*** au apărut în mai toate aeroporturile prin care am trecut *(Dubai, Doha, Singapore sau Melbourne)*. Sistemul scanează rapid fețele pasagerilor, identifică persoanele în baza documentului de călătorie și de identitate reducând, în acest fel blocajele din zonele de tranzit.

Unul dintre cele mai avansate sisteme de recunoaștere facială din lume care utilizează IA, primul de acest fel, **"Smart Tunnel"** este utilizat în Aeroportul din Dubai unde pasagerii nu mai trebuie să prezinte pașapoarte și permisele de îmbarcare la ghișeul de check-in înainte de a merge la aeronavă.

Un pasager care utilizează Smart Tunnel care permite pasagerilor să termine procedurile de control al pașapoartelor în câteva secunde, mergând pur și simplu prin acest sistem de recunoaștere biometrică la terminalul 3 al aeroportului internațional Dubai.

Credit de imagine: Virendra Saklani / Gulf News

SECȚIUNEA 2
Ce este securitatea fizică și securitatea IA

Cum ajută AI securitatea fizică să facă locurile publice mai sigure (II)

Pe lângă acest sistem IA utilizat în zonele de tranzit, Aeroportul Dubai a introdus din februarie 2021 un nou serviciu rapid de control al pașapoartelor care utilizează tehnologii de recunoaștere a feței și irisului pentru a accelera procesul de imigrație. Sunt utilizate 122 de porți inteligente la terminalele de sosire și plecare din aeroport care scanează irisul după ce s-a făcut check-in.

Potrivit declarației biometrice de confidențialitate a Emirates, compania aeriană leagă fețele pasagerilor cu alte date de identificare personală, inclusiv informații despre pașaport și zbor, păstrându-le *„atâta timp cât este în mod rezonabil necesar pentru scopurile pentru care au fost colectate”.* Acordul oferea câteva detalii despre modul în care datele vor fi utilizate și stocate dar precizând că, în timp ce compania nu a făcut copii ale fețelor pasagerilor, alte date personale *„pot fi prelucrate în alte sisteme ale Emiratelor”.*

KAMRAN JEBREILI/AP

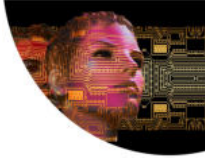
Iris scans, requiring people to stare into a camera as though they're offering a fingerprint, have become more widespread worldwide.

Un alt domeniu în care IA ajută securitatea fizică ajută este automatizarea sarcinilor repetitive.

Sistemele tradiționale de supraveghere înregistrează sute de ore de filmare, dar este de datoria unui om să vadă înregistrările pentru a detecta activitățile suspecte.

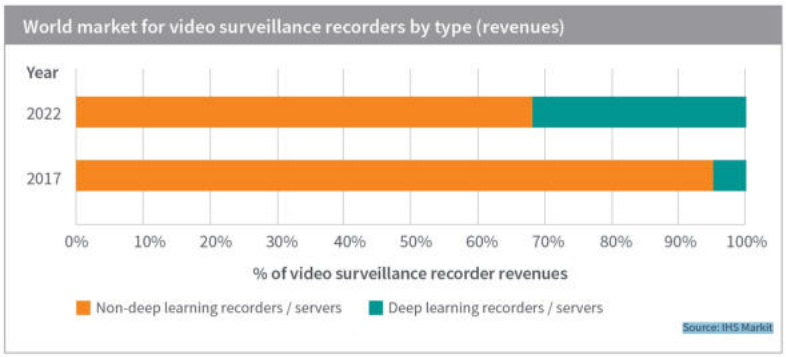
IA contribuie acum la distincția între diferite imagini, eliminând nevoia oamenilor de a face munca laborioasă de a privi aceste ore de înregistrare video. În schimb, acum sistemul IA poate clasifica diferite obiecte și oameni în imagini și poate face legăturile corecte între acestea.

"La fel ca în toate domeniile legate de siguranță și securitate, este important să nu scoți complet omul din buclă. Sistemele de inteligență artificială sunt excelente pentru a-i identifica pe potențiali infractori, pentru a detecta anomalii și comportamente suspecte, dar ar trebui să fie folosite ca instrumente augmentate pentru a ajuta oamenii să își facă treaba mai bine decât să le înlocuiască complet." [14]



SECȚIUNEA 3
Rolul IA în securitatea fizică

Piața securității fizice caută din ce în ce mai mult să adopte aplicații de inteligență artificială, în special în cazul algoritmilor de învățare profundă (deep learning algoritms) pe piața supravegherii video fiind rognozată o creștere importantă a veniturilor așa cum rezultă din sursa IHS Markit. [25]



Percepția despre inteligența artificială, așa cum am precizat chiar la începutul acestui material, oscilează între înțelegere și teoria conspirației. Foarte puțini sunt cei care vorbesc despe IA și chiar fac acest lucru după o documentare temeinică iar asta crează confuziile despre care am vorbit creând discrepanțe între ceea ce poate face tehnologia în realitate și ceea ce cred oamenii că face *("roboții vor prelua controlul")*.

Este adevărat că, în prezent, cele mai spectaculoase utilizări ale IA sunt realizate utilizând o mare putere de procesare și hardware foarte costisitor fiind accesibilă doar unui numar foarte mic de utilizatori.

Pe lângă aceasta sau poate, în primul rând, intervine componenta etică atunci când se monitorizează activitatea altor oameni.

Când primăria unui oraș oarecare din România a anunțat că intenționează să instaleze un sistem de supraveghere video cu recunoaștere facială, anunțul a avut atât păreri pro cât și unele contra.

Oamenii ar vrea să se simtă în siguranță dar să nu fie supravegheați și mai ales identificați.

Despre cerințele legale rezultate din GDPR este o altă poveste dar amintesc doar că Autoritatea Europeană pentru Protecția Datelor (AEPD) a precizat că recunoașterea facială ar trebui interzisă în Europa, din cauza „intruziunii sale profunde și nedemocratice" în viața privată a oamenilor.

De aici lucrurile pot lua o întorsătură absolut necunoscută pentru mine și nu îmi permit, nici măcar să anticipez care vor fi consecințele.

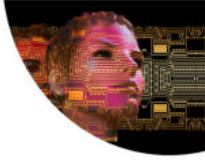
Rămâne doar o întrebare: *"Când eliminați ceea ce este practic imposibil și ce nu este etic, cu ce utilizări ale IA în securitate mai rămânem? În ultimă instanță, implicarea IA în acest domeniu nu înseamnă cu adevărat să facem lucruri pe care nu le-am mai făcut până acum, ci să facem ceea ce facem deja, dar mai bine."* [3]

Atunci când personalul din serviciile de securitate are la dispoziție o semnalare promptă a activităților suspecte din obiectivul supravegheat atunci va putea gestiona cu mult mai mare ușurință situațiile de securitate (pătrunderi neautorizate, altercații între angajați sau sustrageri de bunuri interne.).

Unul din beneficiile reale ale IA în securitatea fizică constă în modul în care învățarea automată poate eficientiza supravegherea video.

Dacă un sistem de supraveghere video clasic înregistrează doar evenimentele, supravegherea video bazată pe analize asupra imaginilor colectate poate îmbunătăți enorm, de exemplu, protecția unui mediu de afaceri.

Foto: Gerd Altmann (Pixabay)



SECȚIUNEA 3
Rolul IA în securitatea fizică

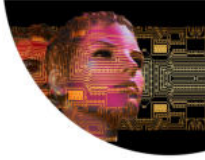
Aici intervine elementul de învățare automată necesar pentru ca un sistem de supraveghere video să fie „instruit" să recunoască potențialele amenințări oferind soluții de supraveghere video cu o precizie sporită.

"Într-o situație în care forța de muncă insuficientă nu își poate permite să petreacă timp cu evenimentele neimportante, valoarea învățării automate ca instrument care ajută la filtrarea alertelor inutile este incontestabilă. Pentru echipele de securitate, aceasta reprezintă o oportunitate de a-și optimiza resursele și de a proteja obiectivul mai eficient, reacționând la incidente reale în mod proactiv, mai degrabă decât retrospectiv." [3]

Eu personal, cunosc companii care ar dori să elimine în totalitate componenta umană din procesele de securitate și să se bazeze doar pe tehnologie și IA dar legislația actuală din România nu permite acest lucru.

Oricât de tentantă este această idee și oricât de bine ar fi realizat programul de control bazat pe IA, eliminarea procesului de luare a deciziilor umane din operațiunile de securitate fizică are un potențial ridict de a provoca incidente catastrofale, pentru indivizi și/sau companii. Tehnologia modernă și sofisticată face viața personalului de securitate mai ușoară pentru că își îndreptă imediat atenția către evenimente suspecte în timp real dar un omul va fi mereu implicat în proces prin interpretarea stării de alarmă și, de ce nu, apelând la intuiția sa pentru a provoca reacția adecvată stării de fapt.

Foto: Gerd Altmann (Pixabay)



SECȚIUNEA 4
Aplicații IA în securitatea fizică

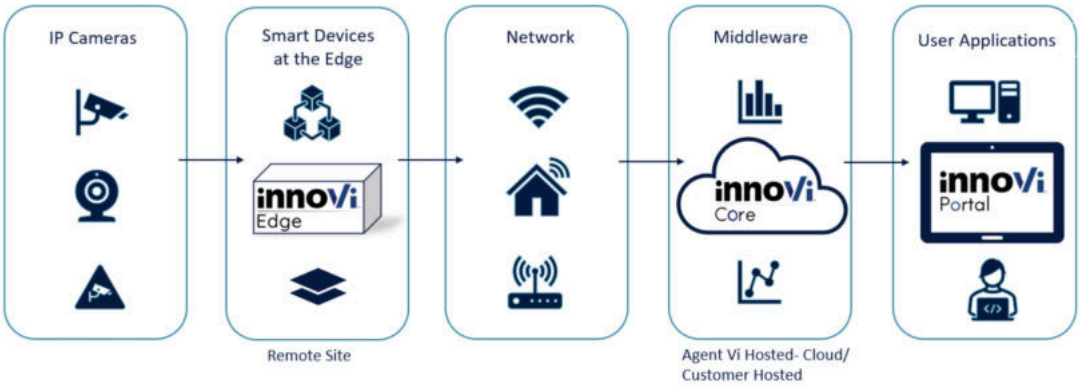
Supravegherea video

În ultimii ani, progresele tehnologice ale supraveghere video au fost spectaculoase iar utilizarea tehnologiilor bazate pe inteligența artificială în supravegherea video sunt într-o dezvoltare fără precedent datorită cercetărilor și dezvoltării în rețelele neuronale de învățare profundă (deep learning neural networks).

Rețelele neuronale de învățare profundă sunt capabile să ofere un nivel de precizie și fiabilitate în detectare și clasificare obiectelor și comportamentului semnificativ mai mare decât analiza bazată pe regulile tradiționale.

Agent Video Intelligence (innoVi™) este o platformă software de analiză video bazată pe IA, de ultimă generație (bazat pe algoritmi deep learning) care oferă un set larg de capabilități de analiză video extrem de sofisticate pentru securitate, siguranță și operațiuni comerciale sporite, cum ar fi detectarea în timp real a evenimentelor de interes, căutarea și analiza rapidă a videoclipurilor înregistrate și extragerea datelor statistice . Disponibilă ca SaaS bazat pe cloud sau ca software local, capabilitățile sale răspund nevoilor oricărei instalații de supraveghere noi sau existente.

Cum functionează?



Sursa: https://www.agentvi.com/

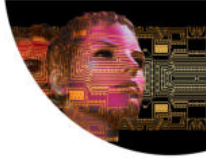
Fiind o platformă software de arhitectură deschisă, **innoVi™** se aplică oricărui sistem de supraveghere, oferind o integrare ușoară cu platforme de gestionare video terță parte, precum și cu software de recepție a alarmelor a fost concepută pentru a oferi disponibilitate ridicată serviciilor, redundanță completă, backupuri și actualizări automatizate fără întrerupere, monitorizarea stării rețelei și a camerelor 24/7 și calibrare automată, fără a fi nevoie de modificări manuale.

Agent Video Intelligence (innoVi™) susține că, folosind imagini video capturate de camerele inteligente, algoritmii au capacitatea de a separa și clasifica oameni, animale, vehicule și obiecte statice pentru a asigura o detecție exactă și rate de alarmă false foarte mici.

Compania explică faptul că datele sunt construite în modele de comportament normal. Acesta servește drept model împotriva căruia sistemul va compara comportamentul suspect.

Învățarea automată permite, de asemenea, ca aplicația să fie aplicată oricărui număr de camere, în funcție de cerințele facilităților extinse și ale orașelor inteligente.

Software-ul detectează intruziunile și recunoașterea facială pentru a permite personalului de securitate și poliției să răspundă în timp ce evenimentul este în desfășurare.



SECȚIUNEA 4
Aplicații IA în securitatea fizică

Video Management System

Compania AZITREND Distribution este prezentă pe piața din România cu platforma TRASSIR, una dintre cele mai performante platforme software de management și analiză video. TRASSIR integrează 99.9% din camerele IP de pe piata, dar si camere analogice fiind o platformă deschisă ce permite integrarea cu alte sisteme.

Utilizând cei mai noi algoritmi de calcul, TRASSIR se poate extinde si adapta la orice fel de specific, de la solutii pentru retail, pana la industrial, centre de business, depozite, paza perimetrala, mari centre comerciale, smart city, gări, autogări, stadioane si aeroporturi. Pe platforma TRASSIR rulează deja mai multe proiecte cu peste 70.000 camere si peste 10.000 de servere.

Avantajele Soluției TRASSIR:

Integrare totală

TRASSIR se poate integra cu orice sistem de control acces, cu centrale anti-efracție, de detecție fum sau foc etc. De asemenea, TRASSIR este o soluție deschisa si permite integrarea cu orice alte sisteme externe, cum ar fi: case de marcat, scannere depozite, cântare auto, sisteme de control al accesului, etc.

Analiza video

People counter, heatmap, heatmap on map, queue detector, face detection, face recognition, detecție obiecte în mișcare, detecție de fum și foc, detecție obiecte lăsate/pierdute, human detection, căutare avansata, etc.

Compatibilitate totală

TRASSIR este compatibil cu 99,9% dintre modelele de camere video, analogice sau IP.

Scalabilitate

TRASSIR are posibilități nelimitate de a se dezvolta cu module suplimentare, in funcție de necesități.

SECȚIUNEA 4
Aplicații IA în securitatea fizică

Soluție de pază perimetrală electronică cu detecție umană

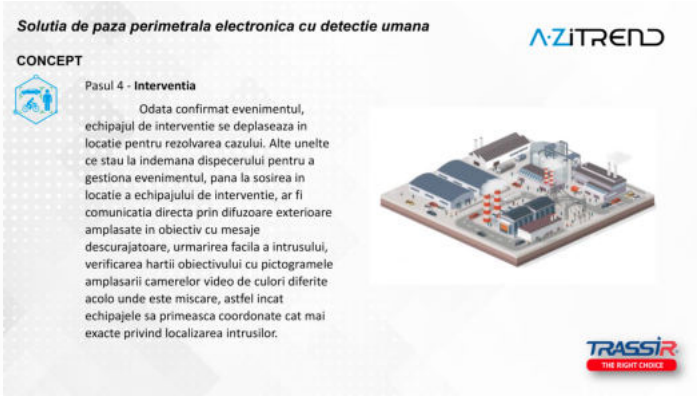
Conceptul de paza electronica are la baza Software-ul de Video Management System si analiza video Trassir.

Componenta VMS, prin facilitățile sale de utilizare:

- Reduce timpul de lucru din Dispeceratul de Monitorizare cu pana la 50%.
- Reduce timpul de căutare al evenimentelor cu pana 90%.
- Reacționează la scenarii și alerte automatizat.
- Crează și transmite rapoarte de evenimente și sau informații personalizate.
- Gestionează arhiva de înregistrări inteligent , cu pierderi minime in orice situație.
- Integrează echipamente 3rd party pentru confirmare sau căutare a evenimentelor.
- Înglobează într-o interfață unică un număr nelimitat de dispozitive, ușor de gestionat.

Componenta de analiză video, folosește pentru recunoașterea obiectelor în imagini, tehnologia Deep Learning, de învățarea prealabila a sistemului prin intermediul Rețelelor Neuronale , care sunt obiectele pe care trebuie să le recunoască.

Dacă în teorie se poate recunoaște orice obiect intr-un anumit proces, dezvoltatorii Trassir s-au axat pe recunoașterea obiectelor uzuale în această etapă, pentru a defini conceptul de paza electronica (oameni, mașini, biciclete, obținând astfel o reducere de costuri în procesul de învățare a rețelei și o acuratețe maximă a recunoașterii, cu minimum de alerte false.

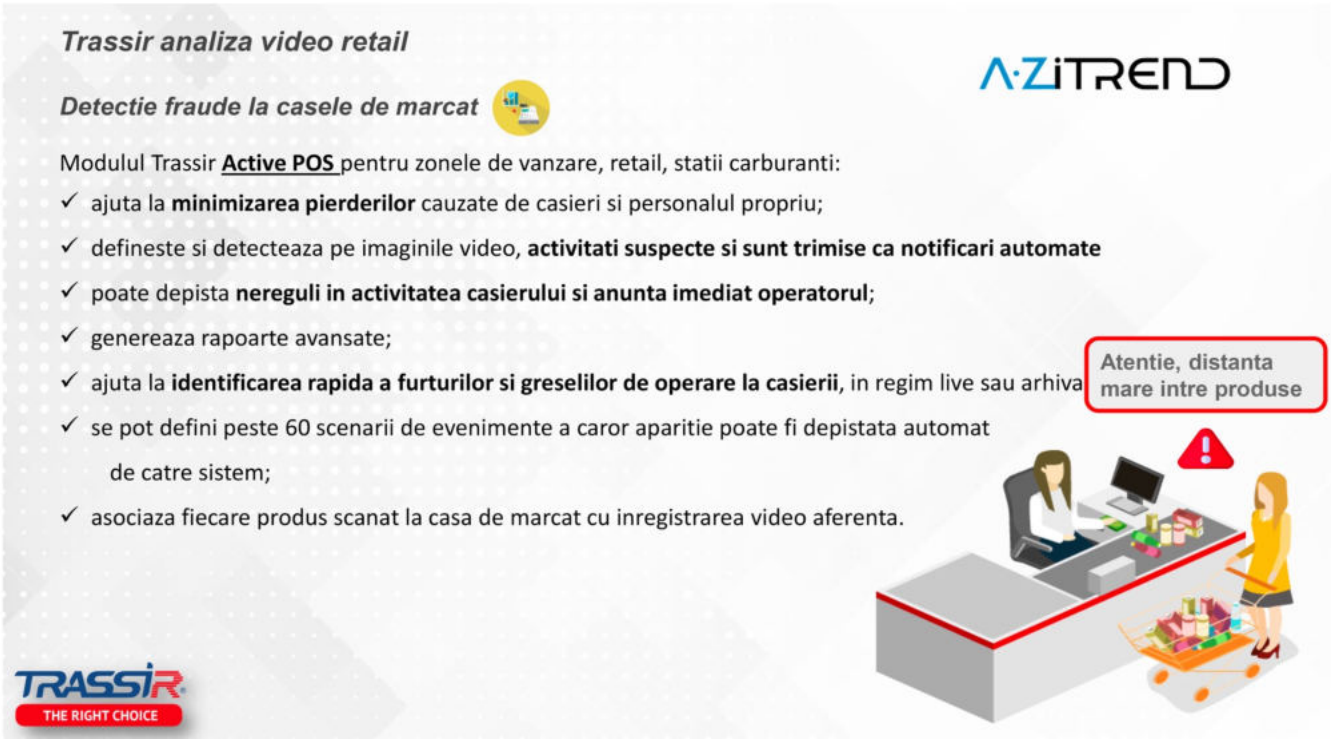


SECȚIUNEA 4
Aplicații IA în securitatea fizică

Soluții pentru comerțul cu amănuntul (Intelligence Retail)

Intelligence Retail oferă soluții de servicii de merchandising personalizate, bazate pe analiza digitală a fotografiilor din magazine.

- Se reduc costurile auditului în punctele de vânzare, specifice retail
- Conduce la creșterea vânzărilor
- Mărește profitabilitatea
- Consolidează loialitatea clienților.

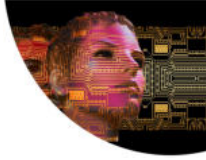


Sistemul video poate reprezenta mai mult decât un clasic tool de captare și înregistrare a imaginilor video.

Acesta poate fi un instrument important în managementul business-ului din retail , prin funcționalitățile de analiza video disponibile in acest moment in platforma Trassir.

Astfel cu ajutorul unui sistem video integrat in Trassir se pot notifica sau raporta:

- Câți clienți au vizitat magazinul, cum sunt repartizați pe departamente și care sunt cele mai vizitate rafturi.
- Dacă se petrec posibile fraude la case de marcat
- Dacă sunt suficiente case de marcat deschise sau programul casierilor trebuie optimizat
- Care este gradul de ocupare al mărfurilor la raft;
- Câți clienți au abordat vânzătorii
- Ce produse lipsesc de la raft.



SECȚIUNEA 4
Aplicații IA în securitatea fizică

Controlul mulțimilor

O caracteristică de bază a controlului mulțimilor cu IA este realizată prin instalarea de camere inteligente cu software de recunoaștere facială pentru a ajuta autoritățile locale și a identifica anumite persoane suspecte, a identifica comportamentele anormale sau violente și a avertiza autoritățile cu privire la orice activitate suspectă prin compararea videoclipurilor în timp real.

Senzorii de mișcare conectați, identifică cele mai aglomerate zone din timpul evenimentelor sportive și de divertisment, pot determina, de asemenea, când și unde se așteaptă să se deplaseze mulțimile în timp ce informează organizatorii de evenimente despre locația barierelor, sau închiderea străzilor.

Tot senzorii de mișcare conectați rezolvă probleme precum blocajele de trafic și locurile cu evenimente unde sunt aglomerări mari de oameni prin redistribuirea resurselor și crearea unor hărți în timp real a participanților.

Sistemul ideal de control al mulțimii oferă o vedere largă a locației și o perspectivă detaliată asupra punctelor de interes.

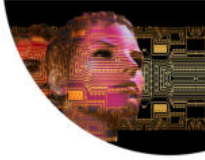
Evolv Technology oferă un sistem de securitate fizică care constă într-un dispozitiv de screening al amenințărilor personalului, Evolve Edge, care funcționează cu aplicația de recunoaștere facială automată Evolv Pinpoint eliminând blocajele și cozile lungi fără a fi nevoie ca persoanele să se oprească pentru a fi identificate.

Camera încorporată de recunoaștere facială captează imagini video pe măsură ce vizitatorii se apropie, în timp ce algoritmii Evolv Pinpoint compară fețele vizitatorilor cu cele de pe lista de urmărire încărcate în baza de date a sistemului. Dacă se descoperă că vizitatorul este o persoană potențial periculoasă, imaginea și profilul său sunt afișate pe o tabletă și evidențiate printr-o lumină roșie, persoana fiind blocată la intrare și reținută.

Sursa: https://youtu.be/e-Fh4OWiDHO

Dacă profilul vizitatorului declanșează o lumină galbenă în jurul profilului său, ceea ce înseamnă o amenințare neconfirmată, agenții de securitate pot trimite profilul unui expert uman în monitorizare centrală pentru revizuire și verificare în timp real iar acest proces durează doar câteva secunde.

Dacă identificarea este negativă, videoclipul vizitatorului este eliminat și vizitatorului i se permite să treacă.



SECȚIUNEA 5
Viitorul IA în securitatea fizică

Nu cred că există cineva capabil să anticipeze cu exactitate cum va evolua inteligența artificială în aplicațiile de securitate fizică dar acesta este un domeniu care va aduce, cu siguranță, mari schimbări în anii care vin.

În timp ce unele dintre soluțiile prezentate anterior au demonstrat impactul pozitiv al inteligenței artificiale și al tehnologiilor de securitate fizică bazate pe date, dezvoltatorii și utilizatorii discută frecvent și despre provocările și neajunsurile sale cum ar fi criminalitatea cibernetică sau problemele legate de confidențialitate.

Iată câteva capacități oferite de IA la care să ne așteptăm în viitorul apropiat așa cum le-a văzut Kayla Matthews.(7)

Consensul general este acela că, pe măsură ce aceste tehnologii se dezvoltă este necesară și o reglementare pe măsură a acestora așa cum am văzut că Uniunea Europeană a realizat deja.

Înțelegerea și reglementarea modului în care recunoașterea facială și soluțiile biometrice pot crea considerentele legate de confidențialitate a fost și este un subiect major de interes pentru toate autoritățile europene.

Concluzia: intervenția umană va fi întotdeauna necesară într-o oarecare măsură pentru a confirma acuratețea interpretării învățării automate chiar dacă aceasta și tehnologia de analiză predictivă se vor îmbunătăți în permanență.

Analize de supraveghere video - Sistemele tipice de supraveghere video pot analiza o infracțiune numai după ce a fost comisă. Este posibil să existe suficiente camere împrăștiate în zona dorită, dar nu suficient de mulți oameni pentru a viziona fluxuri video și a scana conținut. IA poate ajuta la depășirea acestei limitări. Software-ul analizează imagini și detectează anomalii (indicatori de comportament violent, de exemplu) în timp real prevenind faptele criminale și permițând o reacție rapidă a forțelor de intervenție.

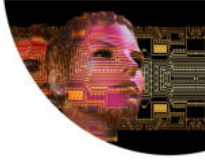
Sisteme de control/admitere acces - Sistemele inteligente de control al accesului sunt o soluție globală pentru securitatea fizică. Software-ul utilizează automatizarea pentru a monitoriza intrările și ieșirile pentru a proteja datele sensibile și a diagnostica problemele care apar recomanând soluții dacă se constată o vulnerabilitate alertând personalul uman.

Patrule cu roboți și drone - Înainte de apariția IA, securitatea fizică a implicat foarte mult personal uman de securitate care să patruleze în sau la exteriorul unui anumit perimetru căutând potențiale amenințări. Acest lucru a fost, și este în continuare o vulnerabilitate importantă dacă personalul este insuficent, prost dotat sau nepregătit profesional.

Automatizarea sarcinilor - IA ajută deja industria de securitate prin automatizarea sarcinilor repetitive, permițând organizațiilor să realoce personalul uman. De exemplu, IA poate „viziona" sute de ore de filmăare video în câteva secunde și poate face distincția între diferite înregistrări, ideal dacă căutați o anumită persoană într-o zonă aglomerată.

Monitorizarea mulțimilor - Monitorizarea unei mari mulțimi de oameni (o stradă aglomerată, o stație de metrou, o zonă comercială sau un concert) poate fi extrem de dificilă, mai ales dacă personalul uman este insuficient Sistemele de monitorizare a mulțimii utilizate de IA pot urmări fiecare persoană într-o zonă desemnată. Senzorii inteligenți pot detecta obiecte realizate cu materiale specifice și pot discerne forma acestora, chiar și atunci când sunt ascunse de vedere. Personalul uman este alertat dacă este descoperită o armă, de exemplu.

Capacitatea de luare a deciziilor - Tehnologia IA este utilizată de consumatori în fiecare zi. I-ați cerut vreodată lui Siri să formeze un număr sau să caute indicații de orientare? În curând, personalul de securitate va putea utiliza această tehnologie pentru a lua decizii într-o fracțiune de secundă putând determina care evenimente necesită un apel la forțele de intervenție și care sunt alarme false.



FORMAREA PROFESIONALĂ

În România, ocupațiile din domeniile sistemelor de securitate private și apărării împotriva incendiilor se află pe ˝Lista profesiilor și ocupațiilor pentru care există cerințe speciale la organizarea pregătirii profesionale˝ iar cursurile de formare profesională sunt organizate de către **RQM CERT**, furnizor de formare profesionala acredita de Autoritatea Națională pentru Calificări (ANC) în baza Standardelor Ocupaționale și a Programelor Cadru avizate de către Inspectoratul General al Poliției Române (I.G.P.R.) și/sau Inspectoratul General pentru Situații de Urgență (I.G.S.U.)

Certificatele de competențe profesionale, eliberate de către Ministerul Muncii și Protecției Sociale și Ministerul Educaţiei prin furnizorii de formare profesională acreditați de Autoritatea Națională pentru Calificări (ANC) fac parte din categoria actelor oficiale și sunt recunoscute la nivel național iar dacă sunt apostilate în cadrul instituției prefectului și traduse sunt recunoscute și la nivel internațional.


ROMÂNIA

MMPS ME

Seria N Nr. 0079

CERTIFICAT
DE ABSOLVIRE

Dl/Dna .....
C.N.P. .....
născut(ă) în anul ....., luna .....
ziua ..... în localitatea .....
jud./sect. ..... fiul (fiica) lui .....
..... și al (a) .....
a participat în perioada .....
la programul de inițiere/perfecționare/specializare cu durata de ..... ore,
pentru ocupația (competențe comune) .....
.....
cod COR ....., organizat de .....
cu sediul în localitatea .....
județul ..... înmatriculat în RNFFPA cu nr. ..... și a promovat examenul de absolvire în anul .....
luna ..... ziua ..... cu nota/calificativul .....

DIRECTOR*), PREȘEDINTE**),

L.Ș. Secretar,

Nr. .....
Data eliberării .....
Semnătura absolventului .....

*) Directorul furnizorului de formare
**) Președintele comisiei de examinare


Ministerul Muncii și Protecției Sociale — ROMÂNIA — Ministerul Educației

Seria N Nr. 0079

CERTIFICAT
DE ABSOLVIRE

Dl/Dna .....
C.N.P. ..... născut(ă) în anul ....., luna .....
ziua ..... în localitatea ..... județul/sectorul .....
..... fiul/fiica lui ..... și al (a) .....
..... a participat în perioada ..... la programul de inițiere/perfecționare/specializare .....
..... cu durata de ..... ore, pentru ocupația (competențe comune) .....
cod COR ....., organizat de ..... cu sediul în localitatea ..... județul ..... înmatriculat în Registrul național al furnizorilor de formare profesională a adulților cu nr. .....
și a promovat examenul de absolvire în anul ..... luna ..... ziua ..... cu nota/calificativul .....

Prezentul certificat se eliberează în conformitate cu prevederile Ordonanței Guvernului nr. 129/2000, republicată și este însoțit de suplimentul descriptiv al certificatului.

DIRECTOR, Secretar, PREȘEDINTE,

L.Ș.

Nr. ..... Data eliberării: anul ....., luna ....., ziua .....

Managementul operațiunilor de securitate

https://rqmcert.com

Manager de securitate
(Cod COR: 121306)

Certificat de absolvire eliberat Ministerul Muncii și Protecției Sociale și Ministerul Educaţiei.

Activitatea managerului de securitate cuprinde: Securitatea Fizică * Securitatea personalului * Securitatea documentelor clasificate * Securitatea Industrială * Securitatea Sistemelor Informatice și de Comunicații (INFOSEC) și Instruirea și educația preventivă a personalului.

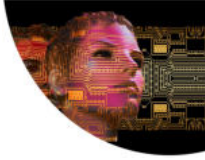
Evaluarea riscurilor la securitatea fizică

https://rqmcert.com

Evaluator de risc la securitatea fizică
(Cod COR: 242115)

Certificat de absolvire eliberat Ministerul Muncii și Protecției Sociale și Ministerul Educaţiei.

Analiza de risc la securitatea fizică constituie fundamentul adoptării măsurilor de securitate a obiectivelor, bunurilor şi valorilor prevăzute de lege, transpuse în planul de pază şi proiectul sistemului de alarmare. Obținerea certificatului de absolvire vă va permite să solicitați înscrierea în Registrul Naţional al Evaluatorilor de Risc la Securitate Fizică (RNERSF)



FORMAREA PROFESIONALĂ

RQM CERT - furnizor de formare profesionala acredita de Autoritatea Națională pentru Calificări (ANC)

https://rqmcert.com

Proiectant sisteme de securitate

(Cod COR: 215119)

Certificat de absolvire eliberat Ministerul Muncii și Protecției Sociale și Ministerul Educației.

Modului I - Proiectarea sistemelor tehnice de detecție și semnalizare la afracție și control acces, TVCI și monitorizare/Proiectarea sistemelor tehnice de detecție și alarmare la incendiu.

Modului II - Proiectarea instalațiilor pentru stingere automată a incendiului/Proiectarea sistemului de control și evacuare a fumului și gazelor fierbinți din construcții și de limitare a propagării fumului în caz de incendiu.

https://rqmcert.com

Tehnician Sisteme de Detecție, Supraveghere Video, Control Acces

(Cod COR: 352130)

Certificat de absolvire eliberat Ministerul Muncii și Protecției Sociale și Ministerul Educației.

Obținerea certificatului de absolvire este obligatorie dacă intenționați să vă licențiați/autorizați propria companie la I.G.P.R./I.G.S.U. sau să lucrați în cadrul unor companii licențiate de I.G.P.R. pentru ˝instalarea, modificarea, monitorizarea, întreținerea și utilizarea sistemelor de alarmare împotriva efracției˝ sau autorizate de I.G.S.U. pentru ˝instalarea și întreținerea sistemelor și instalațiilor de semnalizare, alarmare și alertare în caz de incendiu˝.

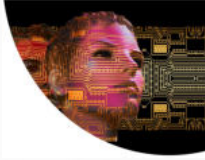
https://rqmcert.com

Tehnician sisteme și instalații de limitare și stingere a incendiilor

(Cod COR: 742106)

Certificat de absolvire eliberat Ministerul Muncii și Protecției Sociale și Ministerul Educației.

Obținerea certificatului de absolvire este obligatoriu dacă intenționați să vă autorizați propria companie la I.G.S.U. sau să lucrați în cadrul unor companii autorizate de I.G.S.U. pentru ˝instalarea si intretinere a sistemelor si instalatiilor de limitare si stingere a incendiilor, cu exceptia celor care contin anumite gaze fluorurate cu efect de sera.˝



BIBLIOGRAFIE:

(1) Norme privind IA: ce dorește Parlamentul European, https://www.europarl.europa.eu/

(2) Ce este inteligența artificială și cum este utilizată? https://www.europarl.europa.eu/

(3) The role of AI in physical security, James Moore https://www.ifsecglobal.com/physical-security/the-role-of-ai-in-physical-security/

(4) The Future of Artificial Intelligence in Physical Security, https://www.barrybros.com/

(5) AI for Physical Security – 4 Current Applications, https://emerj.com/

(6) Artificial Intelligence is Transforming Physical Security, https://www.briefcam.com/

(7) 6 Ways AI Will Change Physical Security, https://www.getkisi.com/

(8) What Is Physical Security? A Comprehensive Guide For 2021, https://www.jigsawacademy.com/

(9) AI Security https://awakesecurity.com/glossary/

(10) Artificial Intelligence (AI) Trends In Physical Security Systems, https://www.securityinformed.com/

(11) Top 5 Physical Security Trends in Retail to Watch in 2021, https://losspreventionmedia.com/

(12) Inteligența artificială depășește tendințele de securitate fizică din 2021, https://patriot1tech.com/

(13) Connecting Artificial Intelligence and Physical Security, https://emergetech.org/

(14) How AI in physical security makes public places safer, https://searchenterpriseai.techtarget.com/

(15) Noi norme și măsuri europene menite să sprijine încrederea în inteligentța artificială, https://www.haptic.ro/

(16) HOTĂRÂRE nr. 28 din 8 septembrie 2020 privind adoptarea opiniei referitoare la Cartea albă - Inteligența artificială - O abordare europeană axată pe excelență și încredere - COM (2020) 65

(17) Excelență și încredere în inteligența artificială, https://ec.europa.eu/

(18) Se schimbă totul în Europa! Uniunea Europeană a prezentat un document revoluționar privind inteligența artificială. Preiau roboții controlul? https://www.capital.ro/

(19) Cartea albă inteligența artificială - O abordare europeană axată pe excelență și încredere

(20) Propunerea de regulament de stabilire a normelor armonizate privind inteligența artificială (Legea privind inteligența artificială)

(21) Cei nouă titani tech, Amy Webb, Editura GLOBO

(22) O Europă pregătită pentru era digitală: Comisia propune noi norme și măsuri menite să sprijine încrederea în inteligența artificială și excelența în acest domeniu (comunicat de presa) https://ec.europa.eu/

(23) ANNEXES to the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - Fostering a European approach to Artificial Intelligence

(24) Supraveghere video: analize video inteligente. https://securitynewsdesk.com/

(25) Artificial Intelligence in Physical Security - An overview of market and technology opportunities, IHS Markit, https://www.securityindustry.org/

(26) AZITREND Distributionn, https://azitrend.ro/

Autori:

Ion Iordache, BEc

Consultant de Securitate,
Data Protection Officer (DPO) și Training & Development Manager la RQM Cert,
CEO și fondator la
Iordache Quality Services (iQS),
companii care oferă servicii de consultanță și cursuri de formare în managementul securității, GDPR și sisteme de management bazate pe standardele internaționale ISO.

www.ioniordache.com ion@ioniordache.com

Alexandru Mihai Caplescu, Ing.

Proiectant de Securitate și Evaluator de Risc la Securitatea Fizică la
BIWTECH SMART
companiie care oferă servicii de consultanță, proiectare sisteme de securitate și evaluări de risc la securitatea fizică.

alex@caplescu.com

DATA ȘI VERSIUNEA 15.08.2021, V.00

Copii ale celei mai recente versiuni ale acestui ghid pot fi descărcate de pe https://ioniordache.com.

Dacă aveți nevoie de informații suplimentare, asistență sau recomandări cu privire la conținutul acestui document, vă rog să mă contactați la ion@ioniordache.com.

RQM Certification

RQM Certification cu sediul în Timișoara este un furnizor de formare profesională cu o echipă excepțională de specialiști cu mare experiență în formare profesională, servicii de evaluare și audit. Compania are expertiză în domeniul sistemelor de management al calității, al mediului, al sănătății și securității la locul de muncă, al automobilelor, al securității fizice, al informațiilor și al serviciilor IT. Programele de formare sunt concepute pentru a sprijini învățarea activă în conformitate cu standardele internaționale și cerințele specifice fiecărei industrii.

www.rqmcert.com
office@rqmcert.com
+40 356 173 020