Material tematic sesiune clasică/ online de coaching/ consiliere profesională/ orientare în carieră, individuală/ personalizată și/ sau de grup

„DreptCompAct- COMpetențe ACTuale pentru studenți la DREPT", Cod proiect: 312957

Competențe transversale în domeniul juridic. Comunicarea (VII)

Competențe digitale, de siguranță pe internet și securitate cibernetică. (A)

Digitalizarea este deja parte din viața noastră, a fiecăruia dintre noi, și presupune dezvoltarea unor competențe specifice. Definiția de dicționar a competențelor digitale diferă în dex față de definiția create de inteligența artificială. Competent este cel care este bine informat într-un anumit domeniu; care este capabil, care este în măsură să judece un anumit lucru.[1], iar competența este capacitate a cuiva de a se pronunța asupra unui lucru, pe temeiul unei cunoașteri adânci a problemei în discuție; (…)[2]

Digital, aparține degetelor, se referă la degete; iar digitală= Afișaj digital (definiția cibernetică) = (prin opoziție cu analogic) se spune despre sistemele sau aparatele care afișează datele în mod discontinuu, cu ajutorul unor caractere (în general cifre) mobile; iar definiția electronică (Despre aparate, dispozitive, instrumente, sisteme) Care generează, măsoară, prelucrează sau stochează semnale digitale.[3]

Competențele digitale sunt definite de inteligența artificială într-un mod accesibil, astfel: Competențele digitale înseamnă a ști să folosești în mod sigur, critic și responsabil tehnologiile digitale pentru a căuta informații, a comunica, a colabora, a crea conținut (inclusiv programare), a-ți proteja datele (securitate cibernetică), a rezolva probleme și a participa la societate, fiind vitale pentru viața personală, educație și piața muncii. Ele se bazează pe abilități precum alfabetizarea informațională, gândirea critică, crearea de conținut digital (ex: Excel, Word, Google Docs, programare), siguranța online și comunicarea prin rețele sociale.

[1] https://dexonline.ro/definitie/competenta
[2] idem 1
[3] https://dexonline.ro/definitie/digital%C4%83

Competențele digitale, inclusiv cele de siguranță pe internet și securitate cibernetică, sunt esențiale în era digitală. Acestea se referă la abilitatea de a utiliza eficient tehnologia informației și comunicațiilor, de a naviga în siguranță pe internet și de a proteja datele personale și organizaționale de amenințările cibernetice.

Competențele digitale includ:

- **Utilizarea calculatorului și a internetului** care presupune cunoașterea funcționării de bază a unui calculator, a sistemelor de operare și a aplicațiilor uzuale (Word, Excel, PowerPoint).
- **Navigarea pe internet** care include căutarea eficientă de informații, utilizarea browserelor web și a motoarelor de căutare.
- **Comunicarea online,** pe care deja o folosim cu toții, presupune utilizarea e-mailului, a platformelor de socializare și a altor instrumente de comunicare digitală.
- **Crearea și gestionarea conținutului digital,** include abilitatea de a crea documente, prezentări, foi de calcul și alte tipuri de conținut digital.
- **Marketing online** include înțelegerea elementelor de bază ale marketingului digital și utilizarea acestora pentru promovarea produselor sau serviciilor.

Pentru a înțelege importanța acestor competențe, din perspectiva absolventului de studii juridice este obligatorie analiza reglementărilor europene în materie, în evoluția acestora.

Astfel, conform sintezei prezentate chiar pe site-ul eur-lex, *'Securitatea cibernetică, cunoscută și ca tehnologia informației sau securitate informatică, implică stabilirea de măsuri care protejează sistemele și rețelele împotriva dezvăluirii de informații, furtului sau daunelor cu privire la hardware, software sau date electronice, precum și împotriva perturbării sau direcționării greșite a serviciilor pe care le oferă.*

Securitatea cibernetică a fost de mult timp o prioritate a Uniunii Europene (UE). Acest lucru se reflectă de curând în bugetul său pe termen lung (cadrul financiar multianual) pentru perioada 2021-2027, cu finanțări importante destinate sprijinirii cercetării, inovării și infrastructurii securității cibernetice, apărării cibernetice și industriei de securitate cibernetică.

Din 2004 și consolidată prin ***Regulamentul UE din 2019 privind securitatea cibernetică****,* ***Agenția Uniunii Europene pentru Securitate Cibernetică*** *(ENISA) a colaborat cu statele membre UE și alte părți relevante,*

oferind consultanță și furnizând soluții, dar și construind capacități de securitate cibernetică pentru a răspunde împreună la incidente de securitate cibernetică transfrontaliere de mare amploare.

*Cea mai recentă **strategie de securitate cibernetică** a UE, prezentată în 2020, urmărește să consolideze rezistența colectivă împotriva amenințărilor cibernetice și să ajute la asigurarea faptului că cetățenii și întreprinderile pot beneficia pe deplin de servicii și instrumente digitale fiabile și de încredere. Aceasta cuprinde propuneri pentru inițiative de reglementare, de investiții și politice în trei domenii.*

- ***Îmbunătățirea rezistenței, suveranitatea tehnologică și spiritul de conducere.** Acestea vor fi atinse prin reformarea normelor cu privire la securitatea **rețelelor și sistemelor informatice**. Aceasta include adoptarea de legislație revizuită (o nouă directivă, propusă în 2020) privind măsuri pentru un nivel ridicat comun de securitate cibernetică în întreaga UE pentru sporirea rezilienței cibernetice a **infrastructurilor critice din sectorul public și privat**.*

- ***Consolidarea capacității operaționale pentru prevenire, descurajare și răspuns.** Urmează să fie creată o nouă unitate cibernetică comună pentru consolidarea cooperării dintre organismele UE și autoritățile statelor membre responsabile pentru prevenirea, descurajarea și răspunsul la atacuri cibernetice. **Setul de instrumente UE pentru diplomația cibernetică** va fi actualizat pentru a preveni, descuraja, intimida și răspunde eficient la activități cibernetice rău intenționate, în special cele care îi afectează infrastructura critică, lanțurile de aprovizionare, instituțiile și procesele democratice.*

- ***Promovarea unui spațiu cibernetic global și deschis printr-o cooperare sporită.** Aceasta va fi realizată prin colaborarea cu parteneri și organizații la nivel internațional pentru consolidarea ordinii globale bazată pe norme, promovarea securității internaționale și stabilității în spațiul cibernetic și protejarea drepturilor omului și a libertăților fundamentale online. UE va spori eforturile de consolidare a capacităților cibernetice în țările din afara UE, împreună cu dialoguri cibernetice cu țările din afara UE, organizații regionale și internaționale, precum și cu comunitatea multilaterală a părților interesate.*[4]

[4] https://eur-lex.europa.eu/RO/legal-content/glossary/cybersecurity.html

Din cele sintetizate este lesne de observat că preocupările europene sunt confirmate de acțiuni concrete atât prin reglementările concrete, cât și prin crearea infrastructurii necesare implementării cadrului legal creat și îmbunătățit în speță Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA).

Regulamentul UE privind securitatea cibernetică[5] urmărește atingerea unui nivel ridicat de securitate cibernetică, de rezistență cibernetică și de încredere în Uniunea Europeană (UE), prin stabilirea unor obiective, sarcini și aspecte organizatorice pentru o agenție consolidată și redenumită a Uniunii Europene pentru securitate cibernetică (ENISA), cu un nou mandat permanent;

În același sens, se crează un cadru pentru sisteme europene voluntare de certificare a securității cibernetice pentru produse, servicii și procese pentru tehnologia informației și comunicațiilor (TIC), precum și pentru servicii de securitate gestionate.

Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), este creată cu scopul asigurării unui nivel comun ridicat de securitate cibernetică în întreaga UE; sprijinirii autorităților naționale și instituțiilor, organelor, oficiilor și agențiilor UE pentru a-și îmbunătăți securitatea cibernetică. Mai mult decât atât, servește drept punct de referință în privința consilierii și expertizei în materie de securitate cibernetică pentru instituțiile, organele, oficiile și agențiile UE și pentru alte părți interesate relevante. Nu este deloc de neglijat contribuția agenției la reducerea fragmentării pieței interne; acționând în mod independent, evitând dublarea activităților statelor membre și ținând seama de expertiza națională; își propune și dezvoltarea propriile resurse și capacități, a competențelor tehnice și umane, care să ofere sprijinul concret în asigurarea securității cibernetice statelor membre. [6]

Această structură instituțională importantă pentru asigurarea securității cibernetice a populațiilor europene, fiind creată pentru o **perioadă nedeterminată** începând cu 27 iunie 2019, operează în conformitate cu un singur document de programare care conține **programarea sa anuală și multianuală**. Respectând regulile de securitate ale Comisiei pentru a proteja informațiile sensibile neclasificate și informațiile clasificate ale UE, ENISA nu divulgă terților informații confidențiale pe care le prelucrează sau le primește, dar participă pe deplin la măsurile UE de combatere a fraudei, a corupției și a altor activități ilegale, prelucrând datele cu caracter personal în conformitate cu normele UE respective."[7]

[5] https://eur-lex.europa.eu/RO/legal-content/summary/the-eu-cybersecurity-act.html
[6] https://www.enisa.europa.eu/
[7] https://eur-lex.europa.eu/eli/reg/2019/881/oj/ron

Regulamnetul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 apr 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică), creează la rându-i un ***grup al părților interesate pentru certificarea securității cibernetice format din experți recunoscuți*** cu scopul, printre altele, de a acorda consiliere Comisiei cu privire la problemele strategice privind cadrul de certificare a securității cibernetice a UE și, la cerere, ENISA cu privire la problemele generale și strategice referitoare la sarcinile relevante ale agenției; și ***un grup european pentru certificarea securității cibernetice (ECCG) alcătuit din reprezentanți naționali pentru a sfătui și ajuta Comisia*** în activitatea sa de a asigura implementarea și aplicarea consecventă a Legii și ENISA în legătură cu pregătirea sistemelor de certificare a securității cibernetice.[8]

Important este să conștientizăm rolul fiecărei structuri care este bine stabilit prin cadru european de certificare a securității cibernetice din regulamentul indicat mai sus și care stabilește inclusiv atribuțiile și rolul specific astfel: Conform cadrului: ***Comisia***- publică un program de lucru continuu al UE pentru certificarea europeană de securitate cibernetică identificând priorități strategice și produse TIC, servicii TIC, procese TIC și servicii de securitate gestionate care ar putea beneficia de un sistem; și poate solicita ENISA pregătirea unui sistem de certificare a candidatului sau revizuirea unuia existent; iar ***ENISA***:

- pregătește sisteme de proiecte adecvate, în urma unei solicitări a Comisiei sau a grupului european pentru certificarea securității cibernetice;
- evaluează fiecare sistem de certificare adoptat, la fiecare cinci ani, ținând cont de feedbackul primit;
- menține un site web dedicat care oferă informații despre sisteme, certificate și declarații de conformitate.

Din perspectiva părților implicate este relevantă și cunoașterea atribuțiilor specifice pentru toate părțile implicate:

a. sistemele europene voluntare de certificare a securității cibernetice;
b. producătorii și furnizorii de produse TIC, servicii TIC, procese TIC și servicii de securitate gestionate certificate;
c. statele membre;

[8] Idem 2

d. Comisia,

a. **Sistemele europene voluntare de certificare a securității cibernetice**:

- ✓ urmăresc atingerea diverselor obiective de securitate, cum ar fi protejarea datelor stocate, transmise și procesate;
- ✓ denotă nivelul de securitate al produselor TIC, serviciilor TIC, proceselor TIC și serviciilor de securitate gestionate ca fiind de bază, substanțial sau ridicat;
- ✓ permit producătorilor și furnizorilor de produse TIC, servicii TIC, procese TIC și servicii de securitate gestionate cu risc scăzut (de exemplu, de bază) să le evalueze singuri (autoevaluarea conformității);
- ✓ trebuie să includă anumite caracteristici, cum ar fi descrieri clare ale scopului, obiectului și domeniului de aplicare și criteriile și metodele de evaluare utilizate;
- ✓ le înlocuiesc pe cele naționale similare, deși aceste certificate rămân valabile până la data de expirare.

b. **Producătorii și furnizorii de produse TIC, servicii TIC, procese TIC și servicii de securitate gestionate certificate** trebuie să pună la dispoziția publicului:

- ✓ orientări și recomandări care să le servească utilizatorilor finali la configurarea, aplicarea și întreținerea produselor sau serviciilor lor;
- ✓ Informații privind perioada în timpul căreia se oferă asistență în materie de securitate;
- ✓ coordonatele lor;
- ✓ trimitere la registrele online care conțin informații despre problemele de securitate cibernetică cunoscute care afectează produsele sau serviciile lor.

c. **Statele membre** numesc una sau mai multe **autorități naționale de certificare a securității cibernetice** cu resurse și competențe suficiente pentru monitorizarea, supravegherea și aplicarea normelor sistemelor europene de certificare a securității cibernetice.

d. **Comisia**:

- ✓ evaluează în mod regulat eficiența și utilizarea sistemelor de certificare adoptate și consideră dacă vreun sistem ar trebui să fie obligatoriu;
- ✓ a trebuit să completeze prima sa evaluare detaliată până la 31 decembrie 2023, iar celelalte la fiecare doi ani;
- ✓ a trebuit să evalueze impactul, eficacitatea și eficiența ENISA până la 28 iunie 2024 și, ulterior, la fiecare cinci ani.

Din perspectivă practică și procedurală, persoanele fizice și juridice au **dreptul de a depune o plângere la emitentul** unui certificat european de securitate cibernetică și de a solicita o **soluție judiciară eficientă**.[9]

În evoluția reglementărilor, s-au modificat serviciile de securitate gestionate, când în decembrie 2024, a fost adoptat Regulamentul (UE) 2025/37[10] de modificare a regulamentului în ceea ce privește serviciile de securitate gestionate. Modificarea specifică introduce **definiția serviciilor de securitate gestionate** și **extinde domeniul de aplicare** al cadrului european de certificare a securității cibernetice prin includerea serviciilor de securitate gestionate. În consecință, acesta extinde, de asemenea, **mandatul și sarcinile ENISA** în ceea ce privește serviciile de securitate gestionate.

Tot în decembrie 2024, prin adoptarea de către Comisie a Regulamentului de punere în aplicare (UE) 2024/3143 privind notificările în temeiul articolului 61 alineatul (5) din Regulamentul privind securitatea cibernetică, prin actele de punere în aplicare se stabilesc circumstanțele, formatele și procedurile de **notificare a organismelor de evaluare a conformității** din cadrul sistemelor europene de certificare în domeniul securității cibernetice prin intermediul sistemului de informații „organisme notificate și desemnate în conformitate cu noua abordare” (NANDO). Prin același document se clarifică și circumstanțele în care ar trebui să se aducă modificări notificării și pe baza cărora ar putea fi contestată competența organismelor de evaluare a conformității notificate.[11]

[9] Idem 5
[10] Regulamentul (UE) 2025/37 a fost publicat în Jurnalul Oficial la 15 ianuarie 2025 și se aplică de la 4 februarie 2025.
[11] Regulamentul de punere în aplicare (UE) 2024/3143 a fost publicat în Jurnalul Oficial la 19 decembrie 2024 și se aplică de la 8 ianuarie 2025.

În ianuarie 2024, Comisia a adoptat Regulamentul de punere în aplicare (UE) 2024/482 [12](a se vedea sinteza). Acest act stabilește normele de aplicare a Regulamentului (UE) 2019/881 în ceea ce privește adoptarea **sistemului european de certificare a securității cibernetice bazat pe criterii comune (EUCC)**. Acesta este primul sistem la nivelul UE și se referă la certificate la niveluri de asigurare „substanțiale" sau „ridicate" pentru produse TIC, cum ar fi hardware și software, inclusiv componente precum cipuri și carduri inteligente. Regulamentul include norme detaliate privind aspecte precum:

- ✓ standardele și cerințele pentru evaluarea și eliberarea, reînnoirea și retragerea certificatelor EUCC pentru produse și profiluri de protecție;
- ✓ organismele de evaluare a conformității acreditate să elibereze certificate sau să efectueze activități de evaluare;
- ✓ monitorizarea conformității, neconformitatea și nerespectarea;
- ✓ proceduri de gestionare și divulgare a vulnerabilităților;
- ✓ păstrarea evidențelor, divulgarea și protecția informațiilor;
- ✓ acorduri de recunoaștere reciprocă cu țări din afara UE;
- ✓ evaluarea inter pares a organismelor de certificare;
- ✓ întreținerea sistemului; și
- ✓ sistemele naționale de certificare a securității cibernetice reglementate de EUCC.

Regulamentul de punere în aplicare EUCC se aplică de la 27 februarie 2025. Regulamentul (UE) 2019/881 și regulamentul de punere în aplicare aferent nu afectează responsabilitățile statelor membre în materie de **securitate publică, apărare, securitate națională sau drept penal**. Regulamentul abrogă Regulamentul (UE) nr. 526/2013 de la 27 iunie 2019.

[12] a se vedea sinteza, https://eur-lex.europa.eu/RO/legal-content/summary/european-common-criteria-based-cybersecurity-certification-scheme-eucc.html

Abundența de reglementări și modificări succesive poate părea inutilă sau foarte complicată, dar dacă analizăm punctual efectele vizate prin măsurile impuse, realizăm că numai așa se poate proteja din perspectiva pieței unice economia fiecărui stat.

Prin certificarea produselor TIC se realizează protecția acestora prin evaluările care trebuie să respecte criteriile comune, metodologia comună de evaluare și documentele de ultimă generație aplicabile.

Certificarea la **niveluri superioare de asigurare** (nivelurile AVA_VAN 4 sau 5) trebuie efectuată, de regulă, pe baza domeniilor tehnice sau a profilurilor de protecție adoptate ca documente de ultimă generație și enumerate în anexa I a Regulamentului de punere în aplicare EUCC.

Solicitanții trebuie să furnizeze o **documentație completă**, inclusiv rezultatele evaluărilor anterioare, dacă este cazul, pentru a susține procesul de certificare.

Organismele de certificare eliberează certificate dacă sunt îndeplinite toate condițiile, iar aceste certificate includ informațiile specifice descrise în anexa VII.

Sistemele naționale de certificare a securității cibernetice trebuie să se alinieze la EUCC și să înceteze să producă efecte în termen de 12 luni de la intrarea în vigoare a regulamentului. Un proces național de certificare început în această perioadă trebuie finalizat în termen de 24 de luni de la intrarea în vigoare.

Certificatele sunt:

- **valabile pentru o perioadă de până la cinci ani**, cu posibile prelungiri după aprobare;
- **revizuite periodic** pentru a asigura conformitatea continuă cu cerințele de securitate;
- **retrase** dacă produsul certificat nu mai îndeplinește standardele impuse sau dacă există neconformități semnificative.

Certificarea profilurilor de protecție. Profilurile de protecție stabilesc cerințe de securitate pentru anumite categorii de produse TIC. Aceste profiluri sunt **evaluate în mod similar produselor TIC**, asigurându-se că acestea îndeplinesc cerințele de securitate necesare pentru anumite categorii TIC; și **certificate de autorități naționale de certificare a securității cibernetice** sau de organisme publice acreditate, sau de un organism de certificare, cu aprobarea prealabilă.

Mărcile și etichetele produselor certificate. Produsele certificate pot purta o marcă și o etichetă care indică **statutul lor de certificare**. Acestea trebuie să fie **clar vizibile** și să conțină detalii precum nivelul de asigurare, numărul unic de identificare și un cod QR care face legătura cu informațiile de certificare.

Organismele de evaluare a conformității și facilitățile de evaluare a securității tehnologiei informației (ITSEF) trebuie să fie **acreditate** în conformitate cu Regulamentul (CE) nr. 765/2008[13] și, pentru niveluri ridicate de asigurare, autorizate de autoritățile naționale de certificare a securității cibernetice.

Autoritățile naționale de certificare a securității cibernetice au atribuții concrete, respectiv monitorizează conformitatea organismelor de certificare, a ITSEF-urilor și a deținătorilor de certificate. De asemenea, acestea gestionează reclamațiile și efectuează investigații privind neconformitatea.

Produsele neconforme trebuie supuse unor **măsuri de remediere**, iar certificatele pot fi suspendate sau retrase dacă problemele nu sunt rezolvate.

Organismele de certificare care eliberează certificate de înaltă asigurare trebuie să se supună periodic unor **evaluări inter pares** pentru a asigura consecvența și standarde înalte în practicile de certificare.

Grupul european pentru certificarea securității cibernetice[14] joacă un rol crucial în menținerea sistemului, aprobând documentele de ultimă generație și asigurând relevanța și eficacitatea continue.

Gestionarea și divulgarea vulnerabilităților

Deținătorii de certificate trebuie să stabilească **proceduri de gestionare și divulgare a vulnerabilităților**, să efectueze analize ale impactului vulnerabilităților și să raporteze organismelor și autorităților de certificare vulnerabilitățile semnificative.

Certificatele retrase trebuie să fie publicate în bazele de date relevante, asigurând transparența cu privire la vulnerabilitățile cunoscute.

Păstrarea și protejarea informațiilor

[13] a se vedea sinteza https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=LEGISSUM:l33248

[14] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-group

Organismele de certificare și ITSEF trebuie să **păstreze înregistrările** evaluărilor și certificărilor timp de cel puțin cinci ani după retragerea certificatului.

Toate părțile implicate în procesul de certificare trebuie să **protejeze informațiile confidențiale** și secretele de afaceri.

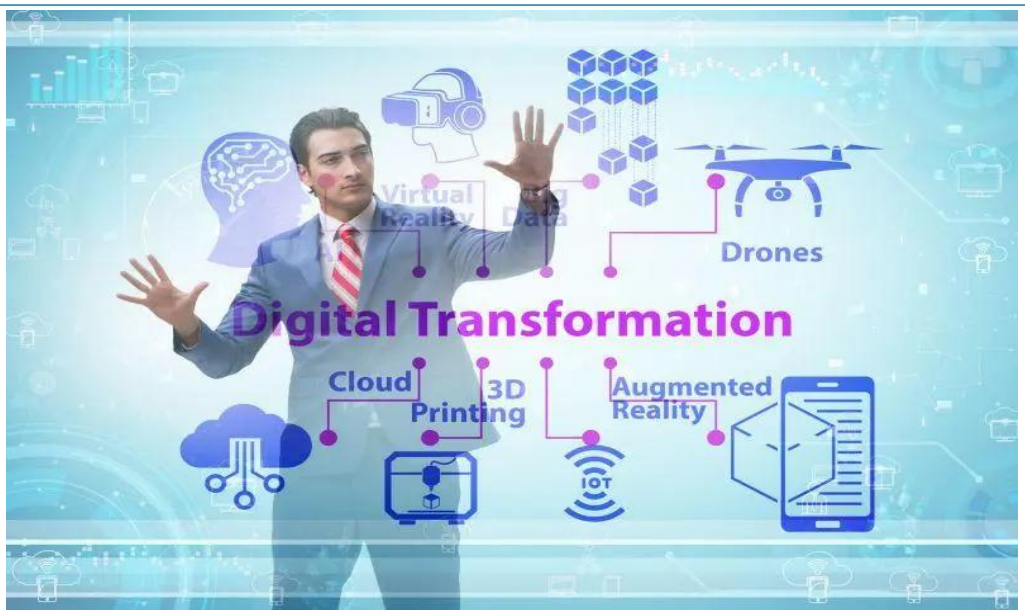
Acordurile de recunoaștere reciprocă cu statele din afara UE

Statele din afara UE pot **recunoaște certificările EUCC** prin acorduri de recunoaștere reciprocă, cu condiția să îndeplinească criteriile privind monitorizarea, supravegherea și gestionarea vulnerabilității, după modelul convențiilor dintre state pentru evitare a dublei impuneri. (impozitarea veniturilor dobândite legal în alte state decât statul de origine/naționalitate)[15] Regulamentul se aplică de la 27 februarie 2025. [16]

Concluzii: Inteligența artificială (AI) definește securitatea cibernetică (sau securitatea digitală) ca un set de măsuri, procese și tehnologii care protejează sistemele informatice, rețelele, programele și datele împotriva atacurilor digitale, furtului de informații, daunelor sau accesului neautorizat, asigurând confidențialitatea, integritatea și disponibilitatea datelor în spațiul virtual. Aceasta implică protejarea dispozitivelor personale, a conturilor online, a fișierelor și a activelor financiare, prin politici, practici de securitate și soluții tehnice.

Transformarea digitală a societății actuale, dar mai ales a societății viitorului constituie o provocare pentru fiecare dintre noi, indiferent de generația din care facem parte, iar capacitatea de a ne adapta fiecare va face diferența între salariatul performant care-și simplifică activitatea automatizată și își concentrează atenția spre creație, inovație, și cel care nu poate, nu vrea nu înțelege utilitatea etc….care se autoizolează într-un conservatorism ineficient pentru toate părțile implicate!

[15] https://www.anaf.ro/anaf/internet/ANAF/asistenta_contribuabili/acorduri_internationale/conventii
[16] Pentru informații suplimentare, consultați:
- Certificare UE privind securitatea cibernetică (Agenția Uniunii Europene pentru Securitate Cibernetică)
- Cadrul de certificare a securității cibernetice (Agenția Uniunii Europene pentru Securitate Cibernetică).


Virtual Reality
Data
Drones
Digital Transformation
Cloud
3D Printing
IOT
Augmented Reality