Volum coordonat de

Ciprian Ceobanu, Constantin Cucoș,
Olimpius Istrate, Ion-Ovidiu Pânișoară

EDUCAȚIA DIGITALĂ

Ediţia a II-a revăzută şi adăugită

POLIROM
2022

Cuprins

Partea a III-a

TEHNOLOGIA ÎN PROFILAREA INOVAȚIEI PEDAGOGICE

Partea a IV-a

SPECIFICITATEA PROCESULUI DIDACTIC ÎN ERA TEHNOLOGICĂ

Partea a V-a

UTILIZAREA TEHNOLOGIEI PENTRU SERVICII DE SUPORT EDUCAȚIONAL

Soluții privind problemele de prelucrare a datelor personale în cadrul educației digitale. Ipoteze, scenarii, exemple

Dreptul la viață privată și dreptul la protecția datelor sunt apărate de instanțele naționale și europene (Șandru, A.-M., 2018b, pp. 26-33). Dar până la aplicarea dreptului de instanțele judecătorești, cea mai mare parte a aplicării se realizează prin respectarea normelor de către cei care au obligații în acest sens. Respectarea drepturilor referitoare la datele personale este un proces complicat nu doar pentru că suntem în prezența unor drepturi relativ noi (legislația a apărut în anii 1990), dar și pentru că pune probleme de ierarhie a unor valori: libertatea de exprimare, dreptul la informare, libertatea de gândire și protecția datelor. În plus, în domeniul educației, o bună parte din subiecții aplicării regulilor sunt copii, persoane fără capacitate deplină de exercițiu. Și chiar și consimțământul părinților pe alocuri este superfluu și uneori chiar ilegal, în sensul că nu produce efecte juridice, iar școala sau universitatea răspund din punct de vedere juridic[1]. Probabil că primul pas în educația digitală este educația copiilor în sensul protejării și valorizării datelor personale.

Problemele de prelucrare a datelor apar în ipotezele enumerate mai jos, în care sunt menționate și principalele riscuri:

Conectivitatea în școli trebuie să înlăture decalajele existente între statele membre ale UE în ceea ce privește introducerea conexiunii în bandă largă de foarte mare capacitate în toate școlile europene. Există două elemente care trebuie abordate: introducerea 5G, cu problemele sale referitoare la riscuri privind sănătatea utilizatorilor, și siguranța datelor în privința transferului acestora în afara Uniunii Europene sau a accesului neautorizat la date. Riscurile trebuie limitate prin măsuri tehnice și organizatorice în cadrul fiecărei școli în parte. Riscurile în privința conectivității sunt generale, nu se referă doar la mediul școlar, însă tocmai din cauză că suntem în prezența unor subiecți ale căror date sunt speciale, respectiv minorii, măsurile trebuie să fie eficiente. În special, trebuie luate măsuri în privința riscurilor generate de utilizarea tehnologiei wireless. Conectarea elevilor sau a studenților la tehnologia wireless prin intermediul unui cont pe o rețea socială introduce un risc în plus și prin acest fapt școala sau universitatea dobândește calitatea de operator alături de rețeaua socială. De asemenea, în procesul de creare a conturilor pentru oaspeți trebuie respectat principiul minimizării datelor, în sensul că solicitarea datelor sensibile, precum CNP, cetățenie, telefon de acasă (noțiune învechită...), nu asigură conformitatea cu GDPR. Mai mult, operatorul (universitatea, școala) solicită propriilor angajați ori studenți completarea unui formular

1. Cu privire la consimțământ în prelucrarea datelor, Șandru D.-M. (2018b, pp. 39-48; 2017, pp. 129-135). Unele din precizările referitoare la relația angajat-angajator se pot aplica și în domeniul educațional, chiar dacă sunt în prezența unui raport student/elev-profesor. A se vedea argumentele privind lipsirea de utilitate a consimțământului în Șandru (2019a) și Macenaite & Kosta (2017).

prea încărcat cu date personale, cum ar fi numele părinților, data și locul nașterii, sexul, CNP-ul, tipul actului de identitate, seria și numărul actului de identitate, naționalitatea, cetățenia, numărul de telefon mobil, de acasă și de fax, precum și adresa completă de domiciliu. Cea mai simplă metodă de identificare a utilizatorului este adresa de e-mail instituțională. Desigur, toți operatorii trebuie să ia măsurile necesare pentru protejarea rețelelor, măsuri tehnice și organizatorice care trebuie avute în vedere de departamentul IT și de responsabilul cu protecția datelor[1]. Măsurile tehnice și organizatorice trebuie să pornească de la premisa, fundamentată empiric, că mai mult de 60% din încălcările de securitate a datelor își au originea în acțiuni umane. Cele mai multe pornesc de la accesarea e-mailului, deschiderea unor fișiere și de la parolele utilizate.

Conectivitatea se referă nu doar la surse și resurse în școală sau universitate, ci și la un acces mai rapid la informație din partea persoanelor interesate. Un proiect de lege referitor la catalogul școlar online intră în responsabilitatea unităților de învățământ preuniversitar, proiect aprobat de Parlament, asupra căruia Președinția a făcut cerere de reexaminare și care este încă în procedură parlamentară la Camera Deputaților[2].

Profilarea. Crearea de profiluri și procesul decizional automatizat sunt recunoscute de Regulamentul General privind Protecția Datelor (art. 22, dar și considerentul 24 din Preambul referitor la „monitorizarea comportamentului", precum și considerentele 70 și 71) și de *Orientările* Grupului de Lucru[3] ca niște procese care au multe riscuri referitoare la accesul la cultură, segregare, afectarea libertății de a alege, previziuni inexacte etc. Paradoxal și fără să aducă argumente, *Orientările* consideră că profilarea ar putea să aducă beneficii în educație. Ca orice proces automatizat, care în consecință este mai ieftin, profilarea prelucrează date mari și la un preț mult mai mic decât dacă ar fi angajate persoane, care oricum nu ar avea capacitatea utilizării a zeci și sute de algoritmi, și astfel *ar putea* avea *beneficii*. Dar care sunt costurile acestor beneficii? Procesul decizional automatizat, inclusiv crearea de profiluri, ar trebui să nu afecteze într-o măsură semnificativă împrejurările, comportamentul și alegerile persoanelor în cauză, să nu aibă un impact prelungit sau permanent asupra persoanei vizate sau să determine excluderea sau discriminarea persoanelor. *Orientările* arată că este greu de stabilit ce poate fi considerat suficient de semnificativ pentru a atinge pragul de afectare, dar sunt oferite exemple, iar unul dintre ele se referă la „decizii care afectează accesul unei persoane la educație" (pp. 23-24). Aceasta înseamnă nu doar admiterea la facultate, dar și participarea la anumite activități în cadrul facultății se încadrează la o profilare incorectă, pentru că ar afecta semnificativ viața privată a persoanei vizate. Cum vom observa în continuare, în prelucrarea datelor și realizarea procesului decizional automatizat,

1. Unele măsuri pot fi observate în documentele Agenției pentru Cibersecuritate a Uniunii Europene (ENISA), https://www.enisa.europa.eu/topics/data-protection
2. Detalii privind Propunerea legislativă PI-x nr. 4/2015[/2019] pentru modificarea și completarea Legii nr. 1/2011 a educației naționale disponibile la http://cameradeputatilor.ro/pls/proiecte/upl_pck.proiect?cam=2&idp=14556
3. Grupul de Lucru „Articolul 29" pentru protecția datelor, *Orientări privind procesul decizional individual automatizat și crearea de profiluri în sensul Regulamentului (UE) 2016/679*, 17/RO, WP251rev.01, adoptate la 3 octombrie 2017, așa cum au fost revizuite și adoptate ultima dată la 6 februarie 2018.

inclusiv a profilării, uneori nu este suficient consimțământul persoanei vizate de aceste procese. În orice caz, operatorul (școala, universitatea) trebuie să pună „în aplicare măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate, cel puțin dreptul acesteia de a obține intervenție umană din partea operatorului, de a-și exprima punctul de vedere și de a contesta decizia" (art. 22, alin. 3). Chiar planul Comisiei evocă pericolul profilării, constatând că: „Expunerea zilnică la date digitale create în mare parte de *algoritmi de nepătruns* creează riscuri clare și necesită mai mult decât oricând o gândire critică și capacitatea de a interacționa într-un mod pozitiv și competent în mediul digital" (Comisia Europeană, 2018, p. 4). Procesul decizional automatizat, inclusiv crearea de profiluri nu ar trebui să vizeze un copil (considerentul 71 din preambulul Regulamentului). Deși, conform *Orientărilor*, acest considerent nu ar trebui interpretat în sensul unei interdicții absolute, în niciun caz nu pot fi utilizate excepțiile prevăzute de art. 22 din Regulament, inclusiv acordul persoanei vizate.

Uneori, profilarea nu este vizibilă sau nu constituie scopul principal al profilării. *Utilizarea pontajului electronic (pentru prezența studenților)* sau a programelor de calculator (software) care să urmărească activitatea studenților, populară în Statele Unite, ar fi nejustificată și ilegală dacă o raportăm la GDPR. Un program precum SpotterEDU este utilizat în zeci de școli pentru a urmări mii de studenți prin conectarea automată a telefonului la o rețea specifică, respectiv software-ul în cauză. Unele școli nu se opresc doar la analiza prezenței, ci realizează și un scor de risc, o profilare, care cuprinde, de exemplu, numărul de vizite la bibliotecă (Harwell, 2019). Ar fi valabil consimțământul studentului pentru instalarea unei asemenea aplicații? Pentru identitate de rațiune cu domeniul relațiilor de muncă, având în vedere că studentul nu poate refuza sau consecințele ar fi nefavorabile pentru el, consimțământul dat în asemenea circumstanțe nu este valabil exprimat[1].

Utilizarea rețelelor sociale pentru diseminarea sau pentru coordonarea și realizarea activităților. Utilizarea rețelelor sociale poate fi analizată din două perspective: utilizarea rețelelor sociale prin constituirea unor „pagini" pentru diseminarea rezultatelor unei cercetări, prezentarea unei entități (școală, facultate, universitate) sau ca instrument pentru comunicare între membrii unei comunități (proiect, clasă, grupă, centru de cercetare etc.). Răspunderea pentru cele două modalități de utilizare a rețelelor sociale este diferită, dar conține un element comun: dacă sunt constituite ca pagini oficiale, entitatea care le constituie („operatorul") răspunde alături de rețeaua socială pentru prelucrarea

1. Pe larg: Documentul de lucru privind supravegherea comunicațiilor electronice la locul de muncă, GL 55, 29 mai 2002, Avizul nr. 8/2001 privind prelucrarea datelor cu caracter personal în contextul ocupării unui loc de muncă, GL 48, 13 septembrie 2001, Avizul nr. 6/2014 privind noțiunea de interese legitime ale operatorului în conformitate cu articolul 7 din Directiva 95/46/CE, GL 217, adoptat la 9 aprilie 2014. În toate aceste documente nu trebuie să ne înșelăm cu privire la sfera de aplicare și să restrângem înțelesul expresiei „loc de muncă". Avizul nr. 2/2017 privind prelucrarea datelor la locul de muncă, GL 249, adoptat la 8 iunie 2017 precizează că, „pentru cea mai mare parte a acțiunii de prelucrare a acestor date la locul de muncă, temeiul juridic nu poate și nu ar trebui să fie consimțământul angajaților, având în vedere natura relației între angajat și angajator".

datelor. Pentru că am detaliat în altă parte consecințele unei asemenea calificări[1], în acest capitol vom prezenta doar acțiunile practice obligatorii a fi întreprinse: măsuri tehnice și organizatorice (desemnarea unei persoane care să administreze discuțiile), informarea persoanelor care intră atât pe pagina web, cât și pe pagina de pe rețeaua socială cu privire la drepturile sale, prevăzute în art. 13-14, mai precis, informarea acestui utilizator. A doua perspectivă se referă la realizarea activităților prin intermediul rețelelor sociale, de exemplu, temele elevilor sau referatele studenților să fie trimise prin intermediul rețelelor sociale, fie că sunt constituite „grupuri", fie pe adresa unuia dintre utilizatori (către profesor, de exemplu). Având în vedere principiile GDPR, considerăm că în starea actuală a legislației și jurisprudenței o asemenea acțiune este la limita legalității din următoarele motive: entitatea (școală, facultate, „proiect") trebuie să aloce fonduri pentru programe (software-uri) proprii, asociate sau nu site-ului de bază, pentru a limita prelucrarea datelor de către terți, în caz contrar obligând utilizatorii (studenți, elevi) să-și creeze un cont în rețeaua socială respectivă sau să-l folosească într-un anumit scop. Uneori este esențială pentru un proiect utilizarea rețelelor sociale, pentru că, de exemplu, grupul-țintă poate fi ușor identificat pe o anumită rețea socială: în această situație este bună limitarea doar la informarea cu privire la beneficiile/oportunitățile proiectului, iar toate prelucrările de date să se desfășoare pe un site dedicat sau cu program dedicat. Orice „intermediar" care prelucrează date reprezintă un risc în plus. Minimizarea prelucrării datelor este un principiu important al GDPR, pentru nerespectarea acestui principiu fiind aplicate importante amenzi în statele membre ale Uniunii Europene.

Inteligența artificială (AI) este un element fundamental al funcționării pe scară largă a educației digitale. Laboratoare răzlețe există și acum, dar uniformizarea educației digitale va conduce la prelucrarea masivă de date, pentru care trebuie să existe o strategie specifică.

În planul Comisiei Europene se menționează necesitatea lansării „în educație, [de] proiecte-pilot legate de inteligența artificială și de analitica învățării, pentru a folosi mai bine volumul enorm de date disponibile în prezent și pentru a contribui astfel la soluționarea problemelor specifice și la îmbunătățirea punerii în aplicare și a monitorizării politicii în domeniul educației" (Comisia Europeană, 2018, p. 14). Trebuie menționat că inteligența artificială are ca ipoteză de lucru bazele mari de date (*Big Data*), așadar presupune asigurarea împotriva unor eventuale încălcări a securității datelor. În Documentul accesoriu Planului Comisiei (European Commission, 2018) se menționează că prelucrarea datelor copiilor a fost considerată intruzivă în viața privată și în ceea ce privește respectarea datelor cu caracter personal (Ferguson *et al.*, 2016). În același timp, este citat un proiect costisitor din Statele Unite care a fost abandonat după proteste ale părinților, elevilor și profesorilor pentru că a fost considerat prea intruziv (Bulger, McCormick & Pitcan, 2017). Sunt oferite și exemple de bune practici din statele membre, de exemplu, autoritatea de protecție a datelor din Franța are discuții regulate cu mediul universitar privind problemele de protecție a datelor. Inteligența artificială, ca auxiliar în educație, pune probleme de adaptabilitate a programelor

1. Pe larg despre jurisprudența Curții de Justiție în materie, Șandru (2019b).

respective și de utilizare a datelor. Însă, într-un viitor nu prea îndepărtat, s-ar putea pune și probleme de etică a muncii, de înlocuire a cadrelor didactice cu roboți[1]. În ambele situații, reglementările juridice sunt la început, Uniunea Europeană fiind în curs de formulare a primelor documente privind poziția sa față de dezvoltarea AI. Ne reține atenția un document întocmit de experți independenți, în care două din cele șapte puncte[2] se referă la protecția juridică a utilizatorilor, respectiv dreptul la viață privată și dreptul la protecția datelor, precum și transparența posibilității de urmărire a datelor în sistemele de inteligență artificială. Corolarul acestora este principiul responsabilității, prin care să se asigure răspunderea sistemelor de inteligență artificială și a acțiunilor acestora.

Menționăm la final *dreptul la ștergere* întrucât constituie o problemă declanșată de popularizarea excesivă și strâmbă a GDPR, unul dintre „noile" avantaje fiind dreptul la ștergere. Acest drept nu este nici nou și nici nu se poate exercita fără restricții. Art. 17 din GDPR este interpretabil și își va găsi justa aplicare după mai mult timp[3]. Cu toate acestea, în contextul aplicării dreptului la protecția datelor în educația digitală, trebuie menționat considerentul 65 al GDPR: „Acest drept este relevant în special în cazul în care persoana vizată și-a dat consimțământul când era copil și nu cunoștea pe deplin riscurile pe care le implică prelucrarea, iar ulterior dorește să elimine astfel de date cu caracter personal, în special de pe internet. Persoana vizată ar trebui să aibă posibilitatea de a-și exercita acest drept în pofida faptului că nu mai este copil. Cu toate acestea, păstrarea în continuare a datelor cu caracter personal ar trebui să fie legală în cazul în care este necesară pentru exercitarea dreptului la libertatea de exprimare și de informare, pentru respectarea unei obligații legale, pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul, din motive de interes public în domeniul sănătății publice, în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice sau pentru constatarea, exercitarea sau apărarea unui drept în instanță". Așadar, responsabilitatea părților și a cadrelor didactice în utilizarea datelor personale ale copiilor, inclusiv imagini publicate pe rețele sociale, este enormă.

Securitatea cibernetică în educație

Acțiune distinctă în planul Comisiei Europene, securitatea cibernetică în educație are două componente: (1) campanii de informare la nivelul UE care să se adreseze cadrelor didactice, părinților, precum și elevilor/studenților și care să stimuleze siguranța online, igiena cibernetică și alfabetizarea mediatică și (2) inițiativa predării

1. Cu privire la posibilitățile de utilizare a tehnicii în sălile de clasă, respectiv *sistemul de science of learning and development* (SoLD) (Darling-Hammond *et al.*, 2019, pp. 1 și urm.).
2. Grupul de experți la nivel înalt privind inteligența artificială, *Orientări în materie de etică în domeniul IA*, 8 aprilie 2019, disponibil la https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai
3. Cu privire la rectificarea și ștergerea datelor, în contextul identității digitale, vezi Jugastru (2018, pp. 44-50), Șchiopu (2019, pp. 47-55).

securității cibernetice pe baza Cadrului competențelor digitale pentru cetățeni (Comisia Europeană, 2018, p. 12)[1].

Etapele esențiale care trebuie urmate în situații neprevăzute de încălcare a securității datelor trebuie cunoscute de toți utilizatorii, pentru că ascunderea încălcărilor poate produce efecte dezastruoase și poate împiedica luarea unor măsuri care să limiteze efectele breșelor de securitate. Înainte de a se ajunge la încălcarea securității datelor, orice entitate (operator) trebuie să analizeze riscurile. Un „risc" reprezintă un scenariu care descrie un eveniment și consecințele acestuia, estimat în termeni de severitate și probabilitate. Pe de altă parte, „managementul riscului" poate fi definit ca fiind activitățile coordonate pentru a conduce și controla o organizație cu privire la un risc[2]. În situația în care riscul totuși s-a produs, în oricare din formele sale – distrugere, pierdere, modificare, divulgare neautorizată sau acces neautorizat –, și operatorul descoperă acest lucru (uneori încălcarea securității datelor este descoperită și după mai mulți ani), trebuie luate următoarele măsuri: informarea conducerii operatorului și în cazuri sensibile chiar a ministerului de resort (în situația unor breșe de securitate grave la o universitate), notificarea autorității de protecție a datelor, informarea persoanelor vizate de încălcarea securității datelor. Toate aceste acțiuni se fac în scopul limitării efectelor produse de încălcarea de securitate a datelor. Încălcarea securității datelor este o problemă reală – de exemplu, în cursul unui an școlar în Marea Britanie au fost notificate peste 700 de breșe de securitate[3].

Pandemia de COVID-19 în educație

Pandemia este unul dintre acele evenimente extraordinare asemănătoare calamităților naturale, care aduce nu numai frică, ci și restricții pentru cetățeni[4]. Libertatea de circulație este unul dintre principalele drepturi care au fost limitate, proporțional cu pericolul la adresa sănătății publice. Ca urmare a acestui fapt, s-a pus presiune pe continuarea activității și unele domenii de activitate au părut a fi favorizate de stadiul tehnicii și, în consecință, s-au mutat în mediul online. Întrucât problemele apărute sunt

1. „Ne confruntăm cu o nevoie în permanentă schimbare de alfabetizare mediatică, de aptitudini și competențe digitale extrem de variate, de siguranță, de securitate și de confidențialitate, dar obținerea lor rămâne o provocare pentru cea mai mare parte a populației și pentru profesiile și sectoarele mai avansate" (Comisia Europeană, 2018, p. 4).
2. *Ghid privind Evaluarea impactului asupra protecției datelor (DPIA) și stabilirea dacă o prelucrare este „susceptibilă să genereze un risc ridicat" în sensul Regulamentului 2016/679*, WP 248 rev.01, 4 octombrie 2017. Vezi și Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, *M.Of.*, nr. 21/9.01.2019, precum și https://twitter.com/CVEnew, https://www.cert.ro/
3. Pe larg, Hickie (2018). Pentru un atac recent asupra site-ului Universității din Maastricht, vezi *„Thank you!" from executive board*, 31 decembrie 2019, disponibil la https://www.maastrichtuniversity.nl/news/thank-you-executive-board
4. Pentru reguli și necesitatea respectării drepturilor persoanelor vizate în situații extreme, vezi Șandru & Șandru (2018, pp. 58-66).