

Asociația pentru Libertatea Românilor,
Bacău, Str. Decebal, nr.6, sc.A, ap.11, cod 600283
<http://asociatialibertatearomanilor.com/>
Tel. 0744.590.721
E-mail: asociatialibertatearomanilor@gmail.com

Către: _____

**Memoriu cu privire la riscurile și restrângerea libertăților
exercitate de sistemul de monitorizare a accesului elevilor,
profesorilor și a personalului auxiliar
în unitățile de învățământ din România**

În calitatea sa de asociație ce are ca scop protecția drepturilor și libertăților fundamentale ale persoanei, după cum sunt prezentate acestea în Constituția României, Asociația pentru Libertatea Românilor, împreună cu asociațiile semnatare, a redactat acest memoriu privind utilizarea sistemelor de identificare și monitorizare electronică în școli. Memoriul își propune nu numai să descrie riscurile tehnologiei RFID, dar și să prezinte propunerile concrete pentru a elimina aceste riscuri.

Tehnologiile de identificare și monitorizare electronică sunt tehnologii cu implicații sociale grave și profunde.

În prezent, în unele unități de învățământ din România s-au implementat sisteme de control a accesului persoanelor utilizând sisteme bazate pe RFID (sau alte tehnologii echivalente), cartele magnetice, amprente.

Cele mai răspândite sunt sistemele de identificare și monitorizare electronică bazate pe unde electromagnetice (RFID sau alte tehnologii echivalente).

Dispozitivele RFID sunt reprezentate de microcircuite electronice cu dimensiuni de câțiva milimetri sau chiar mai mici, care stochează o anumită cantitate de informație în format digital, informație ce poate fi citită cu ajutorul unui cititor specializat, prin intermediul undelor radio, de la o distanță teoretic de câțiva centimetri, practic până la 30m.

De aici rezultă o caracteristică esențială și anume că dispozitivele RFID pot transmite date în mod insesizabil, prin aer, nestincherit de uși, perete, rucsaci, portmonee sau îmbrăcăminte.

Alte tehnologii contactless (fără contact) funcționează pe principii asemănătoare.

RFID a fost inițial conceput ca sistem de inventariere și de urmărire a obiectelor și animalelor. Sistemele RFID sunt acum comercializate în școli ca o modalitate de a extinde urmărirea și inventarierea pentru persoane fizice, umane. Aceste aplicații implică încorporarea microcircuitelor electronice RFID în carduri școlare în scopul de a urmări prezența și mișcările elevilor, profesorilor și personalului din școli.

În cazul folosirii sistemelor de acces biometrice pe bază de amprentă, pentru funcționarea sistemului, este necesar să se stocheze amprentele tuturor elevilor, profesorilor și membrilor personalului. Această aplicație biometrică pare disproportională în raport cu necesitatea de a controla accesul și de a gestiona anumite situații. Există deja un sistem eficient și mult mai simplu, și anume catalogul.

Datele colectate prin intermediul sistemului de acces în școli se stochează și sunt prelucrate în rețeaua informatică a școlii și eventual în rețelele informatiche externe.

1. Amenințarea la adresa libertăților civile și intimității (vieții private) a persoanei¹

ApLR împreună cu asociațiile aderente dorește să atragă atenția asupra folosirii neadecvate a sistemelor de a monitorizare a elevilor, profesorilor și personalului din școli. Dispozitivele electronice de control a accesului încalcă aşteptările rezonabile minime de intimitate și amenință libertățile civile ale copiilor și adulților în școlile noastre astfel:

1.1 Folosirea acestui sistem implica dezumanizare și risc de dezinscriere școlară : În timpul procesului de supraveghere și îndrumare din școli, monitorizarea comportamentelor detaliate ale persoanelor fizice poate deveni înjositoare. Se încalcă unele principii ale educației moderne, precum și drepturile copilului, care prevăd ca educația să se facă prin folosirea unor metode pozitive iar nu prin constrângere, unii copii putând astfel dezvolta un sindrom de respingere al scolii (fobia școlară), în acest ultim caz, aspect deja prezent atât în literatura de specialitate cât și în realitate, existând la momentul actual numeroase cazuri psihiatrice diagnosticate ca atare.

1.2 Încălcarea libertății de exprimare și de asociere. În cazul instalării dispozitivelor de acces în mai multe locații din interiorul școlii (de exemplu pe fiecare încăpere, pentru a demonstra astfel prezența efectivă a elevului în clasă și nu doar în cadrul școlii), software-ul de urmărire poate monitoriza cardurile de acces la portător, descurajând persoanele fizice să își exercite drepturile la libertatea de gândire, de exprimare și de asociere. De exemplu, elevii ar putea evita să solicite sfatul unui anumit profesor sau al psihologului scolii atunci când ei știu că utilizarea cardurilor vor indica prezența lor în aceste locații.

1.3 Așa cum legislația actuală respectă dreptul la obiecție pe motive de conștiință oferind posibilitatea de opțiune în privința documentelor personale electronice (pașaport, carte de identitate, etc.) tot la fel trebuie tratată și problema în discuție întrucât multe persoane manifestă opoziție față de sistemele electronice de identificare datorită proprietăților convingerii filozofice sau religioase. Școlile sunt obligate să respecte aceste convingerile ale elevilor.

1.4 Folosirea neautorizată a sistemelor de acces electronic cu vulnerabilizarea și expunerea posesorilor unor riscuri inacceptabile. În timp ce sistemele electronice de acces pot fi dezvoltate

¹ În continuare, punctele 1.4, 1.5, 1.7, 2.8.1, 2.8.5, și 2.8.4 se referă numai la sistemele de monitorizare a accesului care folosesc tehnologii pe baza undelor electromagnetice (de tip RFID sau echivalente), restul punctelor având aplicabilitate generală.

pentru a fi utilizate într-o școală, cardurile de acces la purtător pot fi citite pe ascuns de oriunde, de către oricine, cu dispozitivul de citire adecvat. Deoarece dispozitivele de citire ale cardurilor de acces (RFID sau echivalente) funcționează în ascuns, prin unde radio invizibile, utilizările neautorizate sau clandestine pot fi aproape imposibil de detectat. În plus, informațiile colectate pe aceste sisteme clandestine ar putea fi folosite, partajate sau alterate, modificate, fără știrea persoanelor fizice sau consimțământul lor. De exemplu, locația unui elev la un moment dat ar putea fi monitorizată de la distanță de către prietenul sau prietena gelos/ geloasă, de către un hărțuitor sau chiar un pedofil. Elevii vor putea fi ținți unor astfel de hărțuri oriunde vor avea asupra lor acest card, chiar și acasă.

1.5 Dispozitivele de citire ascunse, nedetectabile de către posesori. Dispozitivele electronice incorporate în cardurile de acces pot fi citite de la distanță (nu se limitează la limita de vedere, la câmpul vizual) de către dispozitive de citire care pot fi incorporate invizibil în aproape orice mediu accesibil ființelor umane. Cititoarele de carduri electronice RFID (sau echivalente) au fost deja înglobate, în cadrul programelor experimentale, în baie, gresie, țesute în covoare și carpe de podea, ascunse în uși sau incorporate în rafturi, ceea ce face practic imposibil pentru cineva să știe când sau dacă a fost "scanat".

1.6 Dezinformări periculoase. Noi riscuri în ceea ce privește securitatea. A ne baza pe sisteme electronice de acces și monitorizare pentru securitate, în locul observării umane, creează mai degrabă noi riscuri de securitate. Falsificarea și hackingul (furtul virtual) pot învinge cu ușurință aceste sisteme. De exemplu, un student ar putea fi considerat ca prezent la cursuri în temeiul cardului de acces, dar de fapt să fie la sute de km distanță, fără ca dispariția acestuia să fie observată.

1.7 Riscurile potențiale pentru sănătate. Sistemele RFID (sau echivalente) emit radiații electromagnetice și sunt foarte multe semne de întrebare cu privire la modul în care sănătatea umană ar putea fi afectată în medii în care dispozitivele de citire sunt omniprezente. Acest real motiv de îngrijorare și efectele dezumanizante ale supravegherii omniprezente pot plasa stres suplimentar asupra elevilor, părinților și profesorilor.

1.8 Condiționarea persoanei umane la urmărire și monitorizare. Tinerii învață despre lume și se pregătesc pentru viitorul lor predominant în școală. Utilizarea unor sisteme de urmărire și monitorizare a acestora pe parcursul procesului lor de dezvoltare, le va crea o stare de acceptare a acestor sisteme și de considerare a procesului de monitorizare și urmărire a persoanei ca fiind o variantă a stării de normalitate. Acest lucru ar putea inaugura o societate care acceptă acest tip de tratament ca pe o rutină, mai degrabă decât ca pe o încălcare a vieții private și a libertăților civile.

1.9 ApLR și asociațiile semnatare avertizează, de asemenea, în legătură cu riscurile implicate de utilizarea datelor biometrice în scopul identificării în cadrul unor baze de date centralizate extinse, având în vedere consecințele potențial negative asupra persoanelor vizate (a se vedea documentul anexat). Trebuie să se țină seama de impactul major al acestor sisteme asupra demnității umane a persoanelor vizate și de implicațiile utilizării lor asupra drepturilor fundamentale ale omului. În lumina Convenției Europene pentru apărarea drepturilor omului și a libertăților fundamentale, precum și a jurisprudenței Curții Europene a Drepturilor Omului privind articolul 8 din Convenție, ApLR arată că orice încălcare a dreptului la protecția datelor este permisă numai cu condiția să respecte legea și să fie necesară, într-o societate democratică, pentru protejarea unui interes public important.

Pentru a asigura respectarea acestor condiții, este necesar să se precizeze scopul urmărit de introducerea acestui sistem și să se evaluateze proporționalitatea datelor care urmează să fie introduse în sistem în raport cu scopul respectiv.

Pentru aceasta, operatorul trebuie să stabilească dacă prelucrarea, mecanismele de prelucrare, categoriile de date care urmează a fi colectate și prelucrate și transferul informațiilor din baza de date sunt necesare și indispensabile. Măsurile de securitate adoptate trebuie să fie adecvate și eficiente. Operatorul trebuie să aibă în vedere drepturile de care beneficiază persoanele ale căror date personale sunt colectate și să se asigure că aplicația conține un mecanism adecvat pentru exercitarea acestor drepturi.

2. Cadrul de lucru necesar a fi pus în aplicare

În timp ce AplR și asociațiile semnatare recunosc responsabilitatea unei școli de a asigura condiții de siguranță elevilor și cadrelor didactice și autoritățile statului trebuie să recunoască în același timp drepturile persoanelor de a își menține și apăra propria lor demnitate, intimitate și drepturile și libertățile civile așa cum sunt prevăzute de Constituția României. Pentru a reduce potențialul de consecințe dăunătoare ale implementării sistemului electronic de monitorizare și control (prin dispozitive RFID și nu numai) la persoane fizice și pentru societate, sunt absolut necesare următoarele:

2.1. Implementarea sistemului trebuie realizată doar după realizarea unei analize de evaluare a impactului, analiză realizată și sponsorizată de către o entitate neutră. Procesul trebuie să implice și părinții, dar și societatea civilă.

2.2. Implementarea tehnologiei de supraveghere din școli, campusuri, etc. trebuie realizată numai cu respectarea principiilor vizând informarea corecta și transparentă a celor direct afectați prin:

- avertismente publice;

- conștientizarea scopului și caracteristicilor sistemului, inclusiv informații despre datele inserate pe aceste carduri, potențiala utilizare neautorizată, locurile de amplasare a dispozitivelor de citire, etc.

2.3. Libera alegere/Consimțământul. Școlile trebuie să obțină consimțământul elevilor și părinților pentru a participa la un sistem de supraveghere ce utilizează sisteme electronice de control și monitorizare a accesului. Acest consimțământ trebuie înregistrat. **Școlile trebuie să prevadă dreptul persoanei de a-și revoca consimțământul.**

Prelucrarea datelor personale trebuie să se bazeze pe unul dintre temeiurile legale menționate la articolul 7 din Directiva 95/46/CE. Primul temei legal, menționat la articolul 7 litera (a), este constituit de acordarea consimțământului de către persoana vizată. Conform Directivei privind protecția datelor, articolul 2 litera (h), consimțământul trebuie să fie o manifestare de voință liberă, specifică și informată a persoanei vizate. Trebuie să fie clar că un astfel de consimțământ nu poate fi obținut în mod liber prin acceptarea obligatorie a unor termeni și condiții generale sau prin opțiunea de neparticipare. În plus, consimțământul trebuie să fie revocabil. În această privință, în avizul său privind definiția consimțământului, grupul de lucru subliniază diferite aspecte importante ale acestei noțiuni: validitatea consimțământului, dreptul persoanelor de a-și retrage consimțământul; consimțământul acordat înainte de începerea prelucrării; cerințe privind calitatea și accesibilitatea informațiilor. În multe cazuri de prelucrare a datelor personale, în lipsa unei alternative valabile, consimțământul nu poate fi considerat liber exprimat. De exemplu, un sistem a cărui utilizare ar descuraja persoanele vizate (de exemplu, deoarece necesită prea mult timp sau este prea complicat procedeul) nu poate fi considerat o alternativă valabilă și prin urmare, acesta nu ar determina un consimțământ real, valabil.

2.4. Colectarea datelor trebuie să fie limitată la strictul necesar.

2.5. Participanților trebuie să li se asigure acces la cerere la datele colectate prin aceste sisteme pentru a se asigura că acestea sunt corecte și nu sunt disproporționate în raport cu scopul. De asemenea, acestora trebuie să li se asigure mecanisme de corectare a datelor inexacte din sistem sau eliminare a celor înregisterate în mod disproporționat.

2.6. Securitatea. Școlile trebuie să implementeze programe de asigurare a conformității, securității și integrității datelor. Trebuie să existe un sistem de audit periodic, neutru, al securității sistemului informatic. Toate aceste condiționări duc la creșterea semnificativă a costurilor inițiale și a celor pentru menenanță.

2.7. Stabilirea unor prevederi concrete privind modul în care vor fi despăgubiți/ocrotiți participanții afectați de funcționarea injustă sau inexactă a sistemului.

2.8 De asemenea, trebuie stabilite în mod clar practicile interzise de școli, în cadrul acestui sistem de acces și monitorizare, cum ar fi:

- 2.8.1. Sistemele RFID (sau echivalente) nu trebuie folosite pentru a urmări persoane fizice deținătoare ale unui sistem de acces bazat pe tehnologia RFID (sau echivalent) sau persoane asociate cu deținătorii, fără a li se cere consumămantul scris sau fără a i se aduce acestora la cunoștință în mod expres acest fapt. În cazul elevilor, părinții trebuie să consimtă de asemenea la acest procedeu de urmărire.**
- 2.8.2. Nicio școală nu trebuie să constrângă o persoană să își dea acordul, prin modalități ce includ condiționarea angajării, accesul la procesul educației în școală, participarea la activități extrașcolare etc. și nicio școală nu trebuie să folosească procedee de stimulare a acceptării cardului de acces. Refuzul de a da consumămantul nu trebuie să conducă la niciun fel de sancțiune de natură disciplinară sau de altă natură.**
- 2.8.3. Persoanele care refuză să participe la sistem pe motive de libertate de conștiință sau de convingeri religioase nu trebuie ridiculizate sau discriminate pentru convingerile lor.**
- 2.8.4. Nu vor exista baze de date ascunse sau sisteme (procedee) de partajare a datelor.**
- 2.8.5. Dispozitivele de citire a cardurilor de acces (contactless sau RFID) nu trebuie să fie instalate în secret sau ascunse.**
- 2.8.6. Persoanele care refuză cardurile nu trebuie obligate să interacționeze cu dispozitivele de tip RFID (sau echivalente) sau să poarte asupra lor carduri de acces cu dispozitive de tip RFID (sau echivalente).**

3. Concluzii

3.1 Datorită seriozității acestei probleme, vă solicităm să dispuneți stoparea instalării unor astfel de sisteme de identificare și monitorizare electronică în școli, campusuri, cantine, etc. până când nu vor exista dovezi suficiente ale siguranței lor, legalității și eficienței acestor echipamente.

3.2 Dacă școlile optează pentru a continua instalarea echipamentelor, este imperios necesar a fi adoptate prevederi concrete pentru a respecta principiul informării corecte și complete și să fie respectat dreptul persoanelor de a rămâne în afara sistemului pe motiv de conștiință sau obiecții religioase față de această tehnologie de supraveghere.

Cu deosebită considerație,

Asociația Pentru Libertatea Românilor
prin Președinte
Profesor **Nicolae Livadă**



Prezentul memoriu este susținut de următoarele asociații:

1. Asociația pentru Libertatea Românilor - Bacău (inițiatorea memoriului)
2. Asociația Națională a Cadrelor Militare în Rezervă și Retragere – Filiala Vrancea „Ștefan cel Mare”
3. Asociația Pro-Vita – Filiala București
4. Asociația Umanitate Pentru Toți – Bacău

5. Asociația Culturală Valea Muntelui – Neamț
6. Asociația Bucovina Profunda
7. Alianța pentru Demnitate Națională
8. Asociația Christiana
9. Alianța Familiilor din România
10. Federația Organizațiilor Ortodoxe Pro-Vita din România
11. Asociația Prietenii Sf. Efrem cel Nou
12. Asociația pentru Apărarea Familiei și Copilului
13. Asociația ProTinerețe Alba Iulia
14. Liga Studenților din Universitatea din București
15. Liga de Utilitate Publică
16. Liga Distributistă Română „Ion Mihalache”
17. Asociația HRISDORIA
18. Fundația „Sfinții Martiri Brâncoveni” – Constanța
19. Asociația Rost
20. Asociația Predania
21. Asociația Civică a Tinerilor Creștin - Ortodocși Români
22. Asociația pentru Cultură și Educație „Sfântul Daniil Sihastrul”
23. Asociația „Ortodoxia Tinerilor”
24. Asociația „Artă și Tradiții Meșteșugărești”- Alba
25. Asociația Tinerilor Ortodocși „Orthograffiti”
26. Fundația Creștină „Părintele Arsenie Boca”
27. Fundația „Sfinții Martiri Brâncoveni” – Suceava
28. Asociația Antimis – Timișoara
29. Liga Tineretului Creștin - Ortodox Român
30. Fundația Sfinții Închisorilor
31. Asociația Dascălilor din România
32. Asociația Familia Ortodoxă
33. Asociația „Copil dorit”
34. Asociația „Triada”
35. Fundația „Sfânta Irina”
36. Asociația „Prietenii de Familie”
37. Asociația Meșterilor Populari din Moldova – Iași
38. Asociația Prologos – Timișoara
39. Asociația Prologos – Oradea
40. Asociația Prologos – Cugir
41. Asociația Enable
42. Asociația Synaxis 2010
43. Asociația Basarabii
44. Asociația "Frăția Ortodoxă Adevăr și Caritate"
45. Asociația Civic Media
46. Asociația Neagoe Basarab
47. Mișcarea pentru Rezistență Filiala Mehedinți