IGPA
Institutul pentru Guvernare și Politici Avansate
Asociație Obștească

STUDIU DE POLITICI PUBLICE

CAPACITATEA REPUBLICII MOLDOVA DE A ASIGURA SECURITATEA CIBERNETICĂ ȘI PROTECȚIA DATELOR PERSONALE

Studiu de caz: incidentul de la Agenția de Guvernare Electronică din octombrie 2026

NOIEMBRIE 2026

AUTOR: DENIS SAVA
Director, IGPA

CHIȘINĂU
IGPA.MD

Rezumat executiv

Între 19 și 23 octombrie 2026, atacatorii au extras automat din serviciile publice digitale ale Republicii Moldova date personale asociate cu circa 750.000 de IDNP, după ce au interogat sistemele folosind aproximativ un milion de identificatori. Datele includ identitatea, fotografia, familia, informații despre asigurarea medicală, pensii, prestații și dizabilitate, bunuri, companii și unele date financiare. Registrele de stat nu au fost modificate, iar datele cardurilor bancare nu au fost afectate. Studiul evaluează, pe baza surselor publice disponibile la 3 noiembrie 2026, capacitatea statului de a asigura securitatea cibernetică și protecția datelor personale.

Constatări-cheie

1. **Incidentul a exploatat deficiențe de bază, nu o vulnerabilitate sofisticată.** Potrivit AGE, unele servicii erau accesibile fără autentificare, iar datele obținute au fost folosite pentru extrageri ulterioare. Volumul de circa 11 milioane de cereri nu a fost oprit de mecanisme de limitare și nu a fost semnalat de monitorizare.
2. **Detectarea a venit de la cetățeni.** Alarma a fost dată de persoanele care au observat în aplicația EVO accesări suspecte ale datelor lor. Activitatea atacatorilor a durat circa patru zile înainte de a fi oprită. Odată detectat, incidentul a fost izolat rapid și cuprinzător.
3. **Cadrul legal este avansat, aplicarea abia începe.** Legea nr. 195/2024 (în vigoare din august 2026) și Legea nr. 48/2023 oferă instrumentele necesare, inclusiv sancțiuni pentru autoritățile publice, dar incidentul a survenit înainte ca mecanismele de verificare a conformității să fie testate.
4. **Responsabilitățile sunt neclare și concentrate.** Administratorul serviciilor (AGE), operatorul tehnic (STISC) și deținătorul registrului populației (ASP) au același fondator, Cancelaria de Stat. Rolurile juridice pentru fiecare serviciu nu sunt delimitate public, iar ASC și STISC au competențe parțial suprapuse.
5. **Persoanele afectate nu au fost încă notificate individual.** La 3 noiembrie, notificarea individuală era în pregătire, fără termen anunțat, deși natura datelor indică un risc ridicat pentru persoane.
6. **Riscurile cele mai grave sunt fraudele personalizate și profilarea prin agregare.** Datele permit fraude credibile, în special împotriva persoanelor vulnerabile, și, combinate cu alte seturi, profilarea unei mari părți a populației. Atribuirea atacului unui actor statal a fost afirmată politic, dar nu este susținută public de probe tehnice.
7. **Clasamentele internaționale măsoară pregătirea formală.** Locul 6 în NCSI reflectă efortul normativ și instituțional real; nivelul 3 în Global Cybersecurity Index și incidentul arată decalajul față de eficacitatea operațională.

Recomandări prioritare

1. **Notificarea individuală și sprijinul victimelor (0–30 de zile).** Notificarea fiecărei persoane afectate, un instrument online de verificare, o linie gratuită de asistență și o campanie anti-fraudă pentru vârstnici.
2. **Poarta de securitate pentru repunerea serviciilor (imediat).** Niciun serviciu care atinge date personale nu revine online fără autentificare, autorizare la nivel de obiect, minimizarea datelor, limitarea ratei de cereri și un test de securitate independent.
3. **Monitorizare comportamentală și centru de operațiuni de securitate 24/7 (60 de zile – 12 luni).** Reguli care detectează interogarea unui număr anormal de persoane distincte, integrate într-un centru guvernamental de monitorizare permanentă.

4. **Anchetă independentă cu raport public (90 de zile).** O comisie de experți naționali și internaționali, după modelul Singapore, în paralel cu finalizarea investigației CNPDCP în cel mult șase luni.
5. **Coaliția anti-fraudă și blocarea creditării pe IDNP (30–90 de zile).** Măsuri comune ale BNM, CNPF, băncilor, creditorilor nebancari, operatorilor de telefonie și Poliției, plus dreptul cetățenilor de a bloca gratuit contractarea de credite pe numele lor.

Cuprins

Rezumat executiv **2**

Lista abrevierilor **6**

1. Introducere **8**

1.1. Contextul 8

1.2. Scopul și întrebările de cercetare 9

1.3. Ce nu face acest studiu 9

1.4. Structura studiului 9

2. Metodologie **10**

2.1. Tipul de cercetare și data de referință 10

2.2. Surse 10

2.3. Gradarea certitudinii 10

2.4. Metoda de analiză a riscurilor 10

2.5. Selecția cazurilor internaționale 11

2.6. Benchmarking 11

2.7. Considerente etice 11

3. Cadrul conceptual și legal **12**

3.1. Noțiuni de bază 12

3.2. Cadrul național 13

3.3. Cadrul european și internațional 17

3.4. Sinteză comparativă 19

3.5. Cine răspunde? Harta responsabilităților 19

4. Studiul de caz: incidentul AGE din octombrie 2026 ..... **21**

4.1. Ecosistemul serviciilor publice digitale 21

4.2. Cronologia incidentului 21

4.3. Ce date au fost extrase 22

4.4. Vectorul de atac, la nivel conceptual 23

4.5. Detectarea 24

4.6. Răspunsul și izolarea 25

4.7. Comunicarea publică 26

4.8. Notificarea autorității și a persoanelor vizate 27

4.9. Atribuirea 28

4.10. Răspuns la întrebarea 1: vulnerabilitățile 28

5. Analiza riscurilor **30**

5.1. Abordare 30

5.2. Registrul riscurilor 30

5.3. Matricea probabilitate × impact 31

5.4. Riscuri pentru persoane 31

5.5. Riscuri pentru stat și pentru securitatea națională 32

5.6. Riscuri sistemice 33

5.7. Riscuri reziduale 34

6. Experiențe internaționale **35**

6.1. Selecția cazurilor 35

6.2. Estonia: extragerea fotografiilor din baza documentelor de identitate (2021) 35

6.3. Australia: Optus (2022) 36

6.4. Bulgaria: Agenția Națională a Veniturilor (2019) 37

6.5. Singapore: SingHealth (2018)..... 38
6.6. Albania: atacul asupra serviciilor guvernamentale (2022)..... 38
6.7. Franța: France Travail (2024)..... 39
6.8. Statele Unite: Office of Personnel Management (2015)..... 39
6.9. Tabel comparativ..... 40
6.10. Lecții transferabile, scalate la Republica Moldova..... 41
7. Capacitatea instituțională și benchmarking..... 42
7.1. Poziția Republicii Moldova în clasamentele internaționale..... 42
7.2. Paradoxul clasamentelor..... 42
7.3. Maturitatea față de NIS2..... 43
7.4. Capacitatea umană și financiară..... 43
8. Discuție..... 45
8.1. Ce spune incidentul despre capacitatea statului..... 45
8.2. Argumentele autorităților..... 45
8.3. Răspunderea: persoane sau sistem?..... 46
8.4. Atribuirea și riscul politizării..... 46
8.5. Digitalizare și securitate: o falsă dilemă..... 46
8.6. Lentila aderării la UE..... 47
9. Recomandări..... 48
9.1. Principii..... 48
9.2. Orizontul 0–3 luni: limitarea prejudiciului și stabilizarea..... 48
9.3. Orizontul 3–12 luni: remedierea structurală..... 49
9.4. Orizontul 1–3 ani: reziliență pe termen lung..... 50
9.5. Tabelul de implementare..... 51
10. Concluzii..... 54
11. Limitele studiului..... 55
Bibliografie..... 56
Anexa 1. Cronologia detaliată..... 62
Anexa 2. Glosar..... 65
Anexa 3. Tabele suplimentare..... 67

Lista abrevierilor

Abrevieri utilizate

Abreviere	Semnificație
ACMA	Australian Communications and Media Authority (Autoritatea australiană pentru comunicații și media)
AGE	Agenția de Guvernare Electronică
API	Interfață de programare a aplicațiilor
ASC	Agenția pentru Securitate Cibernetică
ASP	Agenția Servicii Publice
BNM	Banca Națională a Moldovei
CCDCOE	Centrul de Excelență NATO pentru Apărare Cibernetică Cooperativă
CEC	Comisia Electorală Centrală
CJUE	Curtea de Justiție a Uniunii Europene
CNIL	Commission nationale de l'informatique et des libertés (Franța)
CNPDCP	Centrul Național pentru Protecția Datelor cu Caracter Personal
CNPF	Comisia Națională a Pieței Financiare
CNS	Consiliul Național de Securitate
CPDP	Comisia pentru protecția datelor cu caracter personal (Bulgaria)
eIDAS 2	Regulamentul (UE) 2024/1183 privind identitatea digitală europeană
EVO	Aplicația și portalul guvernamental de servicii și identitate digitală
GCI	Global Cybersecurity Index (ITU)
GDPR	Regulamentul general privind protecția datelor (UE) 2016/679
HG	Hotărâre de Guvern
IDNP	Numărul de identificare de stat al persoanei fizice
IHiS	Integrated Health Information Systems (Singapore)
ITU	Uniunea Internațională a Telecomunicațiilor
MA	Ministerul Apărării
MAI	Ministerul Afacerilor Interne
MDED	Ministerul Dezvoltării Economice și Digitalizării
NCSI	National Cyber Security Index (e-Governance Academy)
NIS2	Directiva (UE) 2022/2555 privind securitatea cibernetică
NIST	National Institute of Standards and Technology (SUA)
NRA	Agenția Națională a Veniturilor (Bulgaria)
OAIC	Office of the Australian Information Commissioner
OPM	Office of Personnel Management (SUA)
OWASP	Open Worldwide Application Security Project
PDPC	Personal Data Protection Commission (Singapore)
RIA	Autoritatea Sistemului Informațional (Estonia)
SIS	Serviciul de Informații și Securitate

Abreviere	Semnificație
SOC	Centru de operațiuni de securitate
STISC	Serviciul Tehnologia Informației și Securitate Cibernetică
UE	Uniunea Europeană

1. Introducere

1.1. Contextul

Între 19 și 23 octombrie 2026, serviciile publice digitale ale Republicii Moldova au fost ținta unei extrageri automate de date personale fără precedent pentru țară. Potrivit estimărilor preliminare comunicate de Agenția de Guvernare Electronică (AGE), atacatorii au interogat sistemele guvernamentale folosind aproximativ un milion de numere de identificare de stat ale persoanelor fizice (IDNP) și au reușit să obțină seturi de date pentru circa 750.000 dintre acestea.[1] Informațiile extrase acoperă identitatea persoanelor, legăturile de familie, statutul de asigurat medical, prestațiile sociale și pensiile, dizabilitatea, permisul de conducere, fotografia, bunurile și companiile deținute, precum și unele date financiare, inclusiv coduri IBAN, obligații fiscale și istoricul plăților efectuate prin serviciul guvernamental de plăți.[2]

Mărimea cifrei trebuie citită corect. Nu este vorba despre 750.000 de conturi de utilizator compromise, ci despre 750.000 de identificatori pentru care au fost obținute răspunsuri din serviciile statului, iar autoritățile au precizat că nu toate persoanele au avut expuse toate categoriile de date.[3] Totuși, raportat la populația țării, presa a descris incidentul drept cea mai mare scurgere de date din istoria Republicii Moldova, comparabilă ca amploare cu aproximativ o treime din populație.[4] Autoritățile au confirmat, la rândul lor, că nu au identificat modificări ale datelor din registrele de stat și că datele cardurilor bancare nu au fost afectate.[5]

Incidentul are loc într-un moment special. În august 2026 a intrat în vigoare Legea nr. 195/2024 privind protecția datelor cu caracter personal, construită după modelul Regulamentului general privind protecția datelor (GDPR) al Uniunii Europene.[6] Din 2025 se aplică Legea nr. 48/2023 privind securitatea cibernetică, care transpune parțial Directiva NIS2.[7] Totodată, Republica Moldova a urcat pe locul 5, iar în prezent ocupă locul 6 în lume în Indicele Național de Securitate Cibernetică (NCSI), un clasament care măsoară existența legislației, a instituțiilor și a capacităților declarate.[8,9] Iar procesul de aderare la Uniunea Europeană a intrat într-o fază în care capitolele privind justiția, drepturile fundamentale și societatea informațională cer nu doar adoptarea normelor, ci și dovada aplicării lor.

---

[1] Agenția de Guvernare Electronică (AGE), comunicat privind estimările preliminare ale incidentului cibernetic din 19–23 octombrie 2026, 27 octombrie 2026, https://egov.md/ro/node/41145.

[2] Agenția de Guvernare Electronică (AGE), comunicat privind estimările preliminare ale incidentului cibernetic din 19–23 octombrie 2026, 27 octombrie 2026.

[3] NewsMaker, „Datele a circa 750.000 de persoane din Moldova au ajuns la hackeri. Autoritățile avertizează: pot fi folosite pentru fraudă", 27 octombrie 2026, https://newsmaker.md/ro/datele-a-circa-750-000-de-persoane-din-moldova-au-ajuns-la-hackeri-autoritățile-avertizează-pot-fi-folosite-pentru-fraudă.

[4] Spotmedia, „Atac cibernetic masiv asupra Republicii Moldova", octombrie 2026, https://spotmedia.ro/stiri/eveniment/atac-cibernetic-masiv-asupra-republicii-moldova.

[5] AGE, comunicat privind restabilirea a 61 de servicii publice digitale, 30 octombrie 2026, preluat de Agenția Moldpres: https://www.moldpres.md/rom/societate/peste-60-de-servicii-publice-digitale-au-fost-restabilite-si-sunt-disponibile-pe-portalul-evo.

[6] CNPDCP, „Legea nr. 195/2024 privind protecția datelor cu caracter personal (în vigoare din 23 august 2026)", material informativ, 2026, https://datepersonale.md/wp-content/uploads/2026/03/Legea-nr.1952024.pdf.

[7] Legea nr. 48 din 16.03.2023 privind securitatea cibernetică, Monitorul Oficial 2023, nr. 151–153, art. 225, în vigoare din 01.01.2025.

[8] Logos Press, „How Moldova Managed to Rank Fifth in the World in Cybersecurity", 2026, https://logos-pres.md/en/news/how-moldova-managed-to-rank-fifth-in-the-world-in-cybersecurity/.

[9] e-Governance Academy, National Cyber Security Index, profilul Republicii Moldova (ultima actualizare a datelor: 29.01.2026), https://ncsi.ega.ee/country/md/.

Cazul AGE pune astfel la încercare întregul edificiu: arhitectura serviciilor digitale ale statului, cadrul legal recent adoptat, instituțiile create în ultimii trei ani și încrederea cetățenilor într-o administrație care a mizat pe digitalizare ca motor al reformei.

1.2. Scopul și întrebările de cercetare

Studiul evaluează capacitatea Republicii Moldova de a asigura securitatea cibernetică și protecția datelor personale, folosind incidentul AGE din octombrie 2026 ca studiu de caz central. Analiza urmărește șase întrebări de cercetare:

- **Î1. Vulnerabilități.** Ce vulnerabilități tehnice, organizaționale și de guvernanță au făcut posibil incidentul?
- **Î2. Cadrul legal și instituțional.** Este adecvat cadrul legal și instituțional (AGE, ASC, STISC, CNPDCP, Cancelaria de Stat, deținătorii registrelor) și unde există goluri sau suprapuneri de responsabilitate?
- **Î3. Riscuri.** Ce riscuri decurg din incident pentru persoane, pentru stat și pentru securitatea națională, pe termen scurt și lung?
- **Î4. Experiența altor state.** Ce cazuri străine comparabile există și ce lecții sunt transferabile?
- **Î5. Conformitatea europeană.** În ce măsură este Republica Moldova aliniată la GDPR, NIS2, eIDAS 2 și Convenția 108+, în contextul aderării la UE?
- **Î6. Măsuri.** Ce măsuri sunt necesare, cu ce prioritate, cost și responsabil?

1.3. Ce nu face acest studiu

Studiul nu reproduce și nu descrie detalii operaționale care ar permite repetarea atacului: adrese ale serviciilor, structura cererilor, instrumente sau secvențe tehnice. Vectorul de atac este analizat exclusiv la nivel conceptual, pe categoriile publice ale standardului OWASP API Security Top 10.[10] De asemenea, studiul nu atribuie atacul unui actor anume. Sunt prezentate doar declarațiile oficiale, cu nivelul de certitudine exprimat de autorități, iar acolo unde nu există confirmare, informația este marcată ca atare.

Analiza este nepartizană. Evaluarea vizează funcționarea instituțiilor și a normelor, nu partidele politice. Pentru fiecare constatare critică sunt prezentate și argumentele sau explicațiile oferite de autorități.

1.4. Structura studiului

Capitolul 2 descrie metodologia. Capitolul 3 prezintă cadrul conceptual și juridic, național și european. Capitolul 4 reconstituie incidentul și evaluează răspunsul instituțional. Capitolul 5 analizează riscurile pe baza unei matrice probabilitate × impact. Capitolul 6 examinează șapte cazuri internaționale comparabile. Capitolul 7 confruntă clasamentele internaționale cu realitatea operațională. Capitolul 8 discută constatările, iar capitolul 9 formulează recomandări pe trei orizonturi de timp, cu tabel de implementare. Urmează concluziile, limitele studiului, bibliografia și anexele (cronologie detaliată, glosar și tabele suplimentare).

[10] OWASP Foundation, OWASP API Security Top 10 – 2023, https://owasp.org/API-Security/.

2. Metodologie

2.1. Tipul de cercetare și data de referință

Studiul este o cercetare calitativă aplicată, de tip studiu de caz explicativ, completată cu analiză juridică comparată, evaluare de risc și benchmarking. Data de referință a datelor este **3 noiembrie 2026**. Faptele care s-au produs sau au devenit publice ulterior acestei date nu sunt incluse; acolo unde un eveniment era deja anunțat (de exemplu, audierile parlamentare din 4 noiembrie 2026), acesta este menționat ca eveniment programat.

2.2. Surse

Au fost utilizate exclusiv surse publice, grupate în patru categorii:

- **Acte normative și documente oficiale:** legi și hotărâri de Guvern ale Republicii Moldova, acte ale Uniunii Europene, tratate ale Consiliului Europei, jurisprudența Curții de Justiție a Uniunii Europene.
- **Comunicări instituționale:** comunicatele AGE, STISC, ASC, CNPDCP, Guvernului, Președinției, Procuraturii și Parlamentului, inclusiv cele preluate de agenția de stat Moldpres.
- **Presă:** publicații naționale și internaționale care au relatat incidentul și cazurile comparate.
- **Rapoarte, standarde și literatură de specialitate:** indici internaționali (ITU, e-Governance Academy, Comisia Europeană), standarde (NIST, ISO/IEC, OWASP), rapoarte de anchetă și analize juridice.

Toate sursele online au fost consultate între 27 octombrie și 3 noiembrie 2026.

2.3. Gradarea certitudinii

Pentru fiecare fapt relevant, studiul distinge între trei niveluri de certitudine, redate explicit în text prin formulare:

- **Fapte confirmate oficial** — enunțate într-un comunicat, act sau declarație publică a unei instituții competente (de exemplu, „potrivit comunicatului AGE din 27 octombrie”).
- **Fapte relatate de presă** — publicate de cel puțin o sursă jurnalistică, dar neconfirmate printr-un document oficial (de exemplu, „presa a relatat că…”).
- **Afirmații neconfirmate** — informații care circulă public, dar nu au putut fi verificate; ele sunt marcate ca „neconfirmate” sau „date indisponibile”.

Cifrele comunicate de autorități în perioada analizată sunt, în mare parte, **preliminare**. Studiul le folosește ca atare și semnalează când au fost revizuite.

2.4. Metoda de analiză a riscurilor

Evaluarea riscurilor urmează ghidul NIST SP 800-30 Rev. 1, compatibil cu standardul ISO/IEC 27005:2022.[11,12] Etapele sunt: identificarea surselor de amenințare și a evenimentelor de amenințare; stabilirea vulnerabilităților și a condițiilor predispozante; estimarea probabilității de materializare; estimarea impactului; determinarea nivelului de risc.

[11] NIST, Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments, septembrie 2012.

[12] ISO/IEC 27005:2022, Information security, cybersecurity and privacy protection — Guidance on managing information security risks.

Probabilitatea și impactul sunt evaluate pe scale de cinci trepte (1 – foarte scăzut, 2 – scăzut, 3 – moderat, 4 – ridicat, 5 – foarte ridicat). Nivelul de risc rezultă din produsul celor două valori și este încadrat astfel: 1–4 scăzut, 5–9 moderat, 10–16 ridicat, 20–25 critic. Evaluarea reflectă judecata experțială a autorului pe baza surselor publice. Ea nu înlocuiește o evaluare internă cu acces la jurnalele de sistem, dar oferă un cadru verificabil pentru prioritizare.

2.5. Selecția cazurilor internaționale

Cazurile comparate au fost selectate pe baza a patru criterii: (1) similitudinea vectorului de atac (acces automat la date prin interfețe insuficient protejate) sau a tipului de date (registre de stat, identitate, sănătate, date fiscale); (2) natura publică a operatorului sau rolul statului în răspuns; (3) existența unor rezultate documentate — investigații, sancțiuni, reforme; (4) relevanța pentru un stat mic sau mijlociu aflat în proces de integrare europeană. Au fost reținute șapte cazuri: Estonia (2021), Australia – Optus (2022), Bulgaria (2019), Singapore (2018), Albania (2022), Franța (2024) și Statele Unite – OPM (2015). Motivarea fiecărei alegeri este prezentată în capitolul 6.

2.6. Benchmarking

Pentru poziționarea internațională au fost folosite cele mai recente ediții disponibile ale Global Cybersecurity Index (ITU, 2024), National Cyber Security Index (e-Governance Academy, date actualizate în ianuarie 2026) și eGovernment Benchmark al Comisiei Europene (ediția 2025, publicată în 2026). Gradul de maturitate față de NIS2 a fost evaluat calitativ, pe baza obligațiilor directivei comparate cu actele normative naționale.

2.7. Considerente etice

Studiul nu prelucrează date personale ale persoanelor afectate și nu reproduce mostre din presupuse seturi de date scurse. Republicarea unor nume sau IDNP-uri dintr-o presupusă scurgere ar constitui ea însăși o prelucrare ilegală și ar valida datele pentru cei care le comercializează, avertisment formulat public și de presa de specialitate.[13] Detaliile tehnice sunt limitate la nivelul necesar pentru înțelegerea vulnerabilității și a remedierii ei.

[13] Mediacritica, „Atacul asupra datelor personale: ce știm, ce nu știm și ce pericole subestimăm”, 2026, https://mediacritica.md/atacul-asupra-datelor-personale-ce-stim-ce-nu-stim-si-ce-pericole-subestimam/.

3. Cadrul conceptual și legal

3.1. Noțiuni de bază

Date cu caracter personal și categorii speciale. Date cu caracter personal sunt orice informații privind o persoană fizică identificată sau identificabilă. Legislația europeană și, din 2026, cea națională disting categoriile speciale de date — printre care datele privind sănătatea — a căror prelucrare este, în principiu, interzisă, cu excepțiile prevăzute de lege. Datele financiare (IBAN, datorii fiscale, istoric de plăți) nu sunt categorii speciale în sens juridic, dar au un potențial ridicat de prejudiciu.

Încălcarea securității datelor. GDPR și Legea nr. 195/2024 definesc încălcarea securității datelor cu caracter personal ca o breșă de securitate care duce, accidental sau ilegal, la distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la date.[14,15] Definiția nu cere ca un sistem să fi fost „spart” în sens tehnic: extragerea de date printr-un serviciu care le furnizează fără verificarea dreptului de acces este o încălcare a securității datelor.

Operator și persoană împuternicită. Operatorul stabilește scopurile și mijloacele prelucrării și răspunde pentru conformitate. Persoana împuternicită prelucrează date în numele operatorului. Când două sau mai multe entități stabilesc împreună scopurile și mijloacele, ele sunt operatori asociați și trebuie să își distribuie responsabilitățile printr-un acord transparent (art. 26 GDPR). În arhitecturile de guvernare electronică, aceste roluri se suprapun frecvent: un registru are un deținător, platforma de interoperabilitate are un administrator, serviciul electronic are un prestator, iar infrastructura are un operator tehnic.

Interoperabilitate și interfețe de programare (API). Serviciile publice moderne nu stochează toate datele într-un singur loc. Ele interoghează la cerere registrele de stat prin interfețe de programare (API), adesea printr-o platformă centrală de interoperabilitate. Avantajul este principiul „o singură dată” — cetățeanul nu mai prezintă documente pe care statul le deține deja. Riscul este concentrarea: un serviciu care poate interoga mai multe registre devine, dacă nu este protejat, o poartă către toate.

Categoriile OWASP API Security Top 10. Standardul de facto pentru riscurile interfețelor de programare este lista OWASP API Security Top 10 (ediția 2023).[16] Patru categorii sunt relevante pentru cazul analizat:

- **Autorizarea defectuoasă la nivel de obiect** (API1) — sistemul nu verifică dacă cel care cere informații despre o anumită persoană are dreptul să le vadă; este suficient să cunoști identificatorul.
- **Autentificarea defectuoasă** (API2) — serviciul răspunde fără a stabili cine face cererea.
- **Autorizarea defectuoasă la nivel de proprietate**, cunoscută anterior ca **expunere excesivă de date** (API3) — serviciul returnează mai multe câmpuri decât sunt necesare pentru scopul declarat.
- **Consumul nerestricționat de resurse** (API4) — lipsa limitării ratei de cereri permite interogări automate în volum mare.

[14]Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 (Regulamentul general privind protecția datelor).

[15]Legea nr. 195 din 25.07.2024 privind protecția datelor cu caracter personal, Monitorul Oficial din 23.08.2024, în vigoare din 23.08.2026.

[16]OWASP Foundation, OWASP API Security Top 10 – 2023.

Acestor categorii li se adaugă fenomenul **enumerării identificatorilor**: atunci când identificatorul personal are o structură previzibilă sau poate fi obținut din alte surse, atacatorul poate genera ori colecta liste de identificatori pe care îi folosește apoi ca „chei” pentru interogări.

Agregare și profilare. Valoarea datelor extrase crește prin combinare. Un set care leagă, pentru aceeași persoană, identitatea, fotografia, familia, bunurile, starea de sănătate și situația financiară permite profilarea fină a indivizilor și a grupurilor, mai ales dacă este combinat cu alte seturi obținute anterior.

Încredere zero (Zero Trust). Modelul descris în NIST SP 800-207 renunță la ideea unui perimetru de încredere: fiecare cerere este autentificată, autorizată și evaluată în funcție de context, indiferent dacă provine din interiorul sau din exteriorul rețelei.[17] Pentru serviciile publice digitale, Zero Trust înseamnă că nicio interfață care atinge date personale nu răspunde unei cereri anonime și că fiecare acces la datele unei persoane este justificat, limitat și jurnalizat.

3.2. Cadrul național

3.2.1. Protecția datelor: de la Legea nr. 133/2011 la Legea nr. 195/2024

Până la 22 august 2026, protecția datelor în Republica Moldova era reglementată de Legea nr. 133/2011.[18] Începând cu 23 august 2026, regimul juridic este stabilit de Legea nr. 195/2024 privind protecția datelor cu caracter personal, adoptată la 25 iulie 2024 și publicată la 23 august 2024, cu o perioadă de tranziție de doi ani.[19,20] Incidentul AGE este, prin urmare, primul caz major de încălcare a securității datelor evaluat în baza noii legi.

Legea nr. 195/2024 preia arhitectura GDPR: principiile prelucrării (art. 5), inclusiv minimizarea datelor și integritatea și confidențialitatea; principiul responsabilității, potrivit căruia operatorul trebuie să implementeze măsuri tehnice și organizatorice adecvate și să poată dovedi conformitatea; protecția datelor începând cu momentul conceperii și în mod implicit; securitatea prelucrării; evaluarea impactului asupra protecției datelor pentru prelucrările cu risc ridicat; desemnarea responsabilului cu protecția datelor, obligatorie pentru autoritățile publice.[21]

Pentru incidentul analizat, două obligații sunt centrale. Prima este notificarea Centrului Național pentru Protecția Datelor cu Caracter Personal (CNPDCP) în termen de cel mult 72 de ore de la momentul în care operatorul a luat cunoștință de încălcare, cu excepția cazului în care încălcarea nu este susceptibilă să genereze un risc pentru drepturile persoanelor (art. 33). A doua este informarea persoanelor vizate, fără întârzieri nejustificate, atunci când încălcarea este susceptibilă să genereze un risc ridicat (art. 34).[22]

---

[17] NIST, Special Publication 800-207, Zero Trust Architecture, august 2020.

[18] Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal (abrogată odată cu intrarea în vigoare a Legii nr. 195/2024).

[19] CNPDCP, „Îndrumări/explicații în vederea aplicării corecte a Legii nr. 195/2024 privind protecția datelor cu caracter personal”, 2026, https://datepersonale.md/wp-content/uploads/2026/02/CONSIDERENTE_Legea_195.pdf.

[20] Legea nr. 195 din 25.07.2024 privind protecția datelor cu caracter personal, Monitorul Oficial din 23.08.2024, în vigoare din 23.08.2026.

[21] CNPDCP, „Legea nr. 195/2024 privind protecția datelor cu caracter personal (în vigoare din 23 august 2026)”, material informativ, 2026.

[22] Ecom.md, „GDPR în Moldova: legea nr. 195/2024 pentru magazinul online”, 2026, https://ecom.md/en/blog/protectia-datelor-lege-195-2024; i-Avocat.md, „Legea nr. 195/2024 privind protecția datelor cu caracter personal: prevederi aplicabile din 23 august 2026”, 2026.

Regimul sancționator a fost schimbat radical. Sub Legea nr. 133/2011, sancțiunile se aplicau prin procedură contravențională, în sume fixe modeste. Noua lege prevede amenzi aplicate de CNPDCP de până la 1.000.000 de lei sau 1% din cifra de afaceri pentru încălcarea obligațiilor operatorului (inclusiv securitatea și notificarea incidentelor) și de până la 2.000.000 de lei sau 2% din cifra de afaceri pentru încălcarea principiilor, a drepturilor persoanelor sau a prescripțiilor Centrului.[23,24] Aplicarea este eșalonată: în primul an după intrarea în vigoare se încasează 10% din cuantumul calculat, în al doilea an 40%, iar integral abia din al treilea an.[25] Încălcarea se constată și se sancționează de la intrarea în vigoare; doar cuantumul încasat este redus.

Pot fi sancționate instituțiile statului? GDPR lasă statelor membre libertatea de a decide dacă și în ce măsură pot fi aplicate amenzi autorităților publice (art. 83 alin. (7)).[26] Unele state (Bulgaria, Franța) amendează instituții publice; altele aplică un regim distinct sau doar măsuri corective. În Republica Moldova, încă din etapa de avizare a proiectului, Procuratura Generală a observat că proiectul instituie posibilitatea aplicării amenzii în privința autorităților și instituțiilor publice.[27] Din lectura legii și a analizelor publicate rezultă că CNPDCP poate, în principiu, să constate încălcări și să aplice sancțiuni și unei instituții publice precum AGE, inclusiv măsuri corective (avertismente, dispoziții de conformare, limitarea prelucrării).[28] Studiul semnalează însă două limite. Prima: o amendă plătită de o instituție bugetară se întoarce, în esență, la bugetul public, efectul disuasiv fiind redus; măsurile corective și publicitatea constatărilor contează mai mult. A doua: aplicarea concretă a acestor prevederi față de o instituție centrală nu a fost încă testată, iar interpretarea finală va aparține CNPDCP și instanțelor.

3.2.2. Securitatea cibernetică: Legea nr. 48/2023 și actele de aplicare

Legea nr. 48/2023 privind securitatea cibernetică, în vigoare din 1 ianuarie 2025, transpune parțial Directiva NIS2.[29] Ea stabilește obligații de gestionare a riscurilor și de notificare a incidentelor pentru furnizorii de servicii din sectoarele critice și instituie autoritatea competentă la nivel național. Agenția pentru Securitate Cibernetică (ASC), creată în decembrie 2023, este autoritatea competentă, echipa națională de răspuns la incidente și punctul unic de contact, în subordinea Ministerului Dezvoltării Economice și Digitalizării.[30,31]

Cadrul a fost completat în 2024–2025 prin mai multe hotărâri de Guvern: Consiliul de coordonare în domeniul securității cibernetice (HG nr. 333/2024);[32] identificarea furnizorilor de

[23]Ecom.md, „GDPR în Moldova: legea nr. 195/2024 pentru magazinul online", 2026 i-Avocat.md, „Legea nr. 195/2024 privind protecția datelor cu caracter personal: prevederi aplicabile din 23 august 2026", 2026.

[24]Logos Press, „Amenzi de până la 2 milioane de lei pentru încălcarea regulilor privind protecția datelor personale", 2026, https://logos-pres.md/noutati/amenzi-de-pana-la-2-milioane-de-lei-pentru-incalcarea-regulilor-privind-protectia-datelor-personale/.

[25]Ecom.md, „GDPR în Moldova: legea nr. 195/2024 pentru magazinul online", 2026 i-Avocat.md, „Legea nr. 195/2024 privind protecția datelor cu caracter personal: prevederi aplicabile din 23 august 2026", 2026.

[26]Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 (Regulamentul general privind protecția datelor).

[27]Procuratura Generală, aviz din 29.11.2023 la proiectul de lege privind protecția datelor cu caracter personal, https://procuratura.md/sites/default/files/2024-02/29.11.2023%20Aviz%20PG%20proiect.pdf.

[28]Ecom.md, „GDPR în Moldova: legea nr. 195/2024 pentru magazinul online", 2026 i-Avocat.md, „Legea nr. 195/2024 privind protecția datelor cu caracter personal: prevederi aplicabile din 23 august 2026", 2026.

[29]Legea nr. 48 din 16.03.2023 privind securitatea cibernetică, Monitorul Oficial 2023, nr. 151–153, art. 225, în vigoare din 01.01.2025.

[30]Hotărârea Guvernului nr. 1028/2023 privind organizarea și funcționarea Agenției pentru Securitate Cibernetică.

[31]e-Governance Academy, National Cyber Security Index, profilul Republicii Moldova (ultima actualizare a datelor: 29.01.2026).

[32]Hotărârea Guvernului nr. 333 din 08.05.2024 privind Consiliul de coordonare în domeniul securității cibernetice.

servicii (HG nr. 860/2024);[33] cerințele de securitate pentru furnizorii de servicii (HG nr. 562/2025), cu obligația furnizorilor de a prezenta ASC raportul primei evaluări a conformității în termen de 24 de luni de la intrarea în vigoare;[34] Programul național de securitate cibernetică 2026–2030 (HG nr. 821/2025);[35] planul național de gestionare a incidentelor și crizelor cibernetice (HG nr. 823/2025);[36] divulgarea coordonată a vulnerabilităților (HG nr. 824/2025).[37]

Pentru sectorul guvernamental, Serviciul Tehnologia Informației și Securitate Cibernetică (STISC) exercită rolul de operator al infrastructurii tehnologice guvernamentale și de echipă de răspuns la incidente pentru autoritățile publice.[38] Serviciul de Informații și Securitate (SIS) are competențe în contracararea amenințărilor la adresa securității statului, inclusiv a celor din spațiul cibernetic.

Un aspect esențial pentru evaluarea răspunsului este calendarul: termenul de 24 de luni pentru prima evaluare a conformității cu cerințele HG nr. 562/2025 nu expirase la data incidentului. Altfel spus, cadrul normativ exista, dar ciclul de verificare a aplicării lui nu ajunsese la primul punct de control. Nu am identificat public lista entităților desemnate ca furnizori de servicii în baza HG nr. 860/2024 și, prin urmare, nici dacă AGE ori serviciile pe care le administrează au fost încadrate formal în acest regim.

3.2.3. Interoperabilitatea: Legea nr. 142/2018 și platforma MConnect

Schimbul de date între registrele statului este reglementat de Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate.[39] Platforma de interoperabilitate MConnect funcționează în baza HG nr. 211/2019: AGE este autoritatea competentă pentru platformă, iar STISC operatorul tehnic; participarea este gratuită pentru participanții publici și contra plată pentru cei privați.[40] Legea consacră principiul că datele sunt furnizate între participanți în baza unui temei legal, pentru un scop determinat, cu jurnalizarea accesărilor. Tocmai această jurnalizare a permis cetățenilor să observe, în aplicația EVO, accesări suspecte ale datelor lor (capitolul 4).

Parlamentul a realizat o evaluare ex-post a Legii nr. 142/2018, ceea ce confirmă că legiuitorul a identificat deja nevoia de ajustare a cadrului de interoperabilitate. Lecția incidentului este că jurnalizarea fără monitorizare activă oferă transparență după fapt, dar nu și prevenție.

3.2.4. Identitatea electronică: Legea nr. 124/2022

Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere reglementează mijloacele de identificare electronică, semnătura electronică și serviciile de încredere.[41] În arhitectura națională, MPass asigură autentificarea, iar aplicația EVO funcționează ca portofel guvernamental pentru identitate digitală, oferind cetățenilor documente electronice și acces la servicii.[42] Incidentul nu a compromis, potrivit autorităților, semnătura electronică și serviciile de

[33] Hotărârea Guvernului nr. 860/2024 cu privire la identificarea furnizorilor de servicii.

[34] Hotărârea Guvernului nr. 562 din 03.09.2025, act de punere în aplicare a Legii nr. 48/2023 privind securitatea cibernetică (cerințe de securitate pentru furnizorii de servicii); nota informativă: https://www.gov.md/sites/default/files/media/documents/sedinte-de-guvern/2025-09/NU-49-MDED-2025.pdf.

[35] Hotărârea Guvernului nr. 821/2025 cu privire la aprobarea Programului național de securitate cibernetică pentru anii 2026–2030.

[36] Hotărârea Guvernului nr. 823/2025 privind planul național de gestionare a incidentelor și crizelor cibernetice.

[37] Hotărârea Guvernului nr. 824/2025 privind divulgarea coordonată a vulnerabilităților.

[38] Hotărârea Guvernului nr. 482/2020 privind Serviciul Tehnologia Informației și Securitate Cibernetică (atribuții de echipă de răspuns la incidente pentru sectorul guvernamental).

[39] Legea nr. 142 din 19.07.2018 cu privire la schimbul de date și interoperabilitate.

[40] Hotărârea Guvernului nr. 211/2019 privind platforma de interoperabilitate (MConnect).

[41] Legea nr. 124 din 19.05.2022 privind identificarea electronică și serviciile de încredere.

încredere.[43] Totuși, autoritățile au dezactivat temporar unele funcții și au impus actualizarea obligatorie a aplicației EVO, iar Comisia Electorală Centrală a renunțat la identificarea alegătorilor prin EVO la scrutinele din 1 noiembrie 2026.[44,45]

3.2.5. Statutul AGE și guvernanța instituțională

AGE este instituție publică înființată în 2010; funcțiile de fondator le exercită Cancelaria de Stat.[46] Cancelaria de Stat are calitatea de fondator și pentru STISC și pentru Agenția Servicii Publice (ASP), deținătorul principalelor registre de identitate.[47] Deciziile Consiliului AGE sunt semnate de secretarul general al Guvernului, ceea ce reflectă legătura directă a instituției cu Cancelaria de Stat.[48] Această configurație are avantaje de coordonare, dar înseamnă că administratorul platformelor (AGE), operatorul tehnic (STISC) și deținătorul registrului populației (ASP) se află sub același fondator. Supravegherea independentă a securității lor revine, în esență, unor autorități din afara acestui lanț: ASC (în sfera MDED) pentru securitatea cibernetică și CNPDCP (autoritate autonomă, care raportează Parlamentului) pentru protecția datelor.

3.2.6. Dreptul penal și contravențional

Capitolul XI al Codului penal („Infracțiuni informatice și infracțiuni în domeniul comunicațiilor electronice") incriminează accesul ilegal la informația computerizată (art. 259), producerea sau punerea la dispoziție ilegală a mijloacelor tehnice sau a produselor program (art. 260), interceptarea ilegală a unei transmisii de date informatice (art. 260^1), alterarea integrității datelor informatice (art. 260^2), perturbarea funcționării sistemului informatic (art. 260^3), precum și falsul informatic și frauda informatică (art. 260^5, art. 260^6).[49,50] Articolele noi au fost introduse prin Legea nr. 278/2008, în vederea armonizării cu Convenția de la Budapesta, ratificată prin Legea nr. 6/2009.[51,52]

Doctrina națională a semnalat deficiențe ale art. 259, în special condiționarea răspunderii de producerea unor urmări prejudiciabile (de exemplu, copierea informației cu daune în proporții mari), spre deosebire de Convenția de la Budapesta și de Directiva 2013/40/UE, care incriminează accesul ilegal ca atare.[53] Un proiect de lege aflat în consultare propune reformularea art. 259 ca „acces ilegal la un sistem informatic", inclusiv în parte, și completarea

[42] Ziar.md, „CEC renunță la identificarea digitală a alegătorilor la scrutinele din 1 noiembrie", octombrie 2026, https://ziar.md/cec-renunta-la-identificarea-digitala-a-alegatorilor-la-scrutinele-din-1-noiembrie/.

[43] STISC, comunicat privind funcționarea normală a semnăturii electronice și a serviciilor de încredere, 1 noiembrie 2026.

[44] IPN, „Utilizatorii EVO vor trebui să instaleze cea mai recentă versiune a aplicației", octombrie 2026, https://ipn.md/utilizatorii-evo-vor-trebui-sa-instaleze-cea-mai-recenta-versiune-a-aplicatiei.

[45] Ziar.md, „CEC renunță la identificarea digitală a alegătorilor la scrutinele din 1 noiembrie", octombrie 2026.

[46] Hotărârea Guvernului nr. 760 din 18.08.2010 cu privire la Instituția publică „Agenția de Guvernare Electronică" (cu modificările ulterioare), inclusiv Statutul AGE.

[47] Guvernul Republicii Moldova, „Lista structurilor organizaționale în care Cancelaria de Stat are calitatea de fondator", https://gov.md/ro/lista-structurilor-organizationale-care-cancelaria-de-stat-are-calitatea-de-fondator.

[48] Consiliul I.P. „Agenția de Guvernare Electronică", Decizia nr. 23 din 23.12.2025 (Raportul privind realizarea Planului de acțiuni al AGE pentru anul 2025), https://egov.md/sites/default/files/decizie_nr._23_din_23.12.2025_a_consiliului_i.p._age.semnat.signed_0.pdf.

[49] Codul penal al Republicii Moldova nr. 985 din 18.04.2002, Capitolul XI „Infracțiuni informatice și infracțiuni în domeniul comunicațiilor electronice" (art. 259–260^6), cu modificările ulterioare.

[50] Proiect de lege pentru modificarea Codului penal și a Codului contravențional (alinierea la Directiva 2013/40/UE), nota informativă, https://particip.gov.md/ro/download_attachment/31395.

[51] „Prevenirea și combaterea criminalității informatice prin cooperare la nivel național și internațional", articol științific, Zenodo, https://zenodo.org/records/7573428.

[52] Legea nr. 6 din 02.02.2009 pentru ratificarea Convenției Consiliului Europei privind criminalitatea informatică.

Codului contravențional.[54] Codul penal exclude răspunderea penală a autorităților publice ca persoane juridice; răspunderea instituțională se stabilește pe cale administrativă, contravențională sau civilă, iar răspunderea penală poate viza doar persoane fizice.

Potrivit informațiilor publicate la 30 octombrie 2026, Procuratura municipiului Chișinău a pornit urmărirea penală pe temeiul bănuielii rezonabile de comitere a infracțiunilor de încălcare a inviolabilității vieții private și de divulgare a datelor urmăririi penale.[55] Nu a fost comunicată public o calificare în baza articolelor din capitolul XI. Calificarea juridică poate evolua pe parcursul urmăririi penale.

3.3. Cadrul european și internațional

3.3.1. GDPR

Pentru evaluarea incidentului, următoarele prevederi ale GDPR sunt relevante, iar Legea nr. 195/2024 le preia în substanță:[56]

- **Art. 5** — principiile minimizării datelor, integrității și confidențialității, precum și principiul responsabilității.
- **Art. 25** — protecția datelor începând cu momentul conceperii și în mod implicit: un serviciu nu ar trebui, implicit, să returneze date despre o persoană unui solicitant neidentificat.
- **Art. 32** — securitatea prelucrării, inclusiv capacitatea de a asigura confidențialitatea continuă și un proces de testare și evaluare periodică a eficacității măsurilor.
- **Art. 33–34** — notificarea autorității în 72 de ore și informarea persoanelor vizate în caz de risc ridicat.
- **Art. 35** — evaluarea impactului asupra protecției datelor înaintea prelucrărilor susceptibile să genereze un risc ridicat, cum sunt prelucrările pe scară largă sau combinarea seturilor de date.
- **Art. 83** — condițiile generale de aplicare a amenzilor, inclusiv libertatea statelor de a decide asupra amenzilor pentru autoritățile publice.

Curtea de Justiție a Uniunii Europene a clarificat, într-o cauză care privea chiar o agenție de stat (Agenția Națională a Veniturilor din Bulgaria), că un acces neautorizat comis de un terț nu este suficient, prin el însuși, pentru a concluziona că măsurile operatorului nu au fost adecvate, dar că sarcina de a dovedi caracterul adecvat al măsurilor revine operatorului, iar teama persoanei vizate de o posibilă utilizare abuzivă a datelor poate constitui, prin ea însăși, un prejudiciu moral.[57] Aceeași logică o reflectă juriștii din Republica Moldova: o instituție de stat nu poate scăpa automat de răspundere doar pentru că atacul a fost comis de hackeri.[58]

---

[53] Proiect de lege pentru modificarea Codului penal și a Codului contravențional (alinierea la Directiva 2013/40/UE), nota informativă.

[54] Proiect de lege pentru modificarea Codului penal și a Codului contravențional (alinierea la Directiva 2013/40/UE), nota informativă.

[55] TVR Moldova, „Cine răspunde pentru furtul de date ale moldovenilor? Procuratura a pornit o urmărire penală”, 30 octombrie 2026, https://tvrmoldova.md/article/332627a01e45d8f2/cine-raspunde-pentru-scurgerea-de-date-ale-moldovenilor-procuratura-a-pornit-o-urmarire-penala.html.

[56] Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 (Regulamentul general privind protecția datelor).

[57] Curtea de Justiție a Uniunii Europene, Hotărârea din 14 decembrie 2023, cauza C-340/21, VB împotriva Natsionalna agentsia za prihodite.

[58] NewsMaker, „(GHID) Ce faci dacă datele tale personale au ajuns la hackeri. Ce drepturi ai și când poți cere despăgubiri”, octombrie 2026, https://newsmaker.md/ro/ghid-ce-faci-dacă-datele-tale-personale-au-ajuns-la-hackeri-ce-drepturi-ai-și-când-

3.3.2. NIS2

Directiva (UE) 2022/2555 (NIS2) extinde obligațiile de securitate cibernetică la entitățile administrației publice centrale.[59] Elementele relevante sunt: răspunderea organelor de conducere pentru aprobarea și supravegherea măsurilor de gestionare a riscurilor (art. 20); un set minim de măsuri, inclusiv politici de analiză a riscurilor, gestionarea incidentelor, securitatea lanțului de aprovizionamente, securitatea în dezvoltarea sistemelor, gestionarea vulnerabilităților, evaluarea eficacității măsurilor, controlul accesului și autentificarea multifactor (art. 21); raportarea incidentelor semnificative în trei etape — avertizare timpurie în 24 de ore, notificare în 72 de ore și raport final într-o lună (art. 23). Legea nr. 48/2023 urmează această logică, dar transpunerea este parțială, iar aplicarea efectivă în administrația publică centrală nu a fost încă verificată prin primul ciclu de evaluări.

3.3.3. eIDAS 2

Regulamentul (UE) 2024/1183 (eIDAS 2) introduce Portofelul european pentru identitate digitală.[60] Pentru un stat candidat care dezvoltă propriul portofel guvernamental (EVO), principiile eIDAS 2 sunt un reper: controlul utilizatorului asupra datelor partajate, divulgarea selectivă a atributelor, interdicția de urmărire a utilizatorului de către emitent, certificarea de securitate a portofelului și obligația de notificare a breșelor care afectează portofelul. Incidentul nu a vizat direct mecanismul de identificare, dar a atins încrederea în ecosistemul EVO, ceea ce a determinat suspendarea folosirii lui la alegeri.[61]

3.3.4. Convenția 108+ și Convenția de la Budapesta

Republica Moldova este parte la Convenția 108 a Consiliului Europei din 2008. Protocolul de amendare (CETS nr. 223), care modernizează Convenția (Convenția 108+), a fost ratificat prin Legea nr. 36 din 20 martie 2026, iar instrumentul de ratificare a fost depus la 15 mai 2026, Republica Moldova devenind al 34-lea stat care a ratificat Convenția 108+.[62,63] Convenția 108+ intră în vigoare internațional după 38 de ratificări, prag neatins la data de referință.[64,65] Ea cere, printre altele, notificarea fără întârziere a autorității de supraveghere în cazul încălcărilor de securitate care pot afecta grav drepturile persoanelor și o autoritate de supraveghere care acționează cu independență deplină.

Convenția de la Budapesta privind criminalitatea informatică, ratificată de Republica Moldova în 2009, oferă baza pentru incriminarea faptelor și pentru cooperarea internațională — conservarea rapidă a datelor, asistența judiciară reciprocă, rețeaua de puncte de contact

poți-cere-despăgubiri.

[59] Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (NIS2).

[60] Regulamentul (UE) 2024/1183 al Parlamentului European și al Consiliului din 11 aprilie 2024 de modificare a Regulamentului (UE) nr. 910/2014 în ceea ce privește instituirea cadrului european privind identitatea digitală (eIDAS 2).

[61] Ziar.md, „CEC renunță la identificarea digitală a alegătorilor la scrutinele din 1 noiembrie", octombrie 2026.

[62] CNPDCP, comunicat privind ratificarea prin Legea nr. 36 din 20.03.2026 a Protocolului de amendare a Convenției 108 (CETS nr. 223), https://datepersonale.md/en/protocol-amending-convention-for-the-protection-of-individuals-with-regard-to-automatic-processing-of-personal-data-published-in-the-official-gazette/.

[63] Consiliul Europei, „Republic of Moldova Becomes the 34th State to Ratify the Convention 108+", 15 mai 2026, https://www.coe.int/en/web/data-protection/-/republic-of-moldova-becomes-the-34th-state-to-ratify-the-convention-108-.

[64] Consiliul Europei, „Republic of Moldova Becomes the 34th State to Ratify the Convention 108+", 15 mai 2026.

[65] Consiliul Europei, Biroul Comitetului Convenției 108 (T-PD-BUR), raport de reuniune, 2026, https://rm.coe.int/t-pd-bur-2026-66rapabr-en/48802dc789.

24/7.[66,67] Pentru un atac care, foarte probabil, a folosit infrastructură din mai multe jurisdicții, aceste mecanisme sunt indispensabile anchetei.

3.4. Sinteză comparativă

Tabelul 1 rezumă gradul de aliniere al cadrului național la principalele standarde europene, așa cum rezultă din analiza de mai sus.

Tabelul 1. Alinierea cadrului național la standardele europene (evaluare calitativă a autorului)

Standard / cerință	Reglementare națională	Grad de aliniere	Observații
GDPR – principii, securitate, notificare 72 h	Legea nr. 195/2024	Ridicat (formal)	În vigoare din 23.08.2026; aplicarea practică abia începe
GDPR – amenzi pentru autorități publice (art. 83 alin. 7)	Legea nr. 195/2024	Opțiune exercitată	Posibile în principiu; cuantum eșalonat; netestat
GDPR – evaluarea impactului (art. 35)	Legea nr. 195/2024	Ridicat (formal)	Nu există dovezi publice că serviciile AGE au trecut prin evaluări de impact
NIS2 – măsuri de gestionare a riscurilor (art. 21)	Legea nr. 48/2023, HG nr. 562/2025	Parțial	Prima evaluare a conformității nu era scadentă la data incidentului
NIS2 – raportare 24 h / 72 h / 1 lună (art. 23)	Legea nr. 48/2023	Parțial	Termenele naționale și aplicarea lor la AGE nu sunt clarificate public
NIS2 – răspunderea conducerii (art. 20)	Neclar	Scăzut	Lipsește o normă explicită de răspundere a conducerii în sectorul public
eIDAS 2 – portofel de identitate digitală	Legea nr. 124/2022, EVO	Parțial	Fără certificare publică de securitate a portofelului
Convenția 108+	Ratificată (Legea nr. 36/2026)	Ridicat	Convenția nu e încă în vigoare internațional
Convenția de la Budapesta / Directiva 2013/40/UE	Codul penal, art. 259–260[6]	Parțial	Art. 259 condiționat de urmări; proiect de modificare în curs

3.5. Cine răspunde? Harta responsabilităților

Incidentul pune în evidență o problemă clasică a guvernării electronice: lanțul de responsabilitate este lung, iar fiecare verigă poate invoca, cu temei parțial, că vina se află în altă parte.

- **Deținătorii registrelor** (de exemplu, ASP pentru Registrul de stat al populației, instituțiile de asigurări sociale și medicale, Serviciul Fiscal de Stat) sunt operatori ai datelor din registrele lor. Ei autorizează furnizarea datelor către servicii, în baza legii.
- **AGE** administrează platformele guvernamentale și, potrivit conducerii sale, gestionează circa 220 dintre cele peste 400 de servicii publice electronice.[68] În calitate de prestator sau administrator al serviciilor prin care datele au fost extrase, AGE este, cel puțin pentru stratul de servicii, operator sau operator asociat. Faptul că AGE a

[66] Consiliul Europei, Convenția privind criminalitatea informatică (STE nr. 185), Budapesta, 23.11.2001.

[67] Legea nr. 6 din 02.02.2009 pentru ratificarea Convenției Consiliului Europei privind criminalitatea informatică.

[68] Unimedia, interviu cu Nicoleta Colomeeț, directoarea AGE, 31 octombrie 2026.

notificat CNPDCP indică faptul că instituția și-a asumat calitatea de operator pentru incident.[69]

- **STISC** este operatorul tehnic al infrastructurii și al platformei de interoperabilitate și echipa de răspuns la incidente pentru sectorul guvernamental — rol apropiat de cel al unei persoane împuternicite pentru componenta de infrastructură.[70,71]
- **ASC** este autoritatea competentă în materie de securitate cibernetică și coordonator național al răspunsului la incidente.[72]
- **CNPDCP** supraveghează conformitatea cu Legea nr. 195/2024. Centrul a precizat public că nu gestionează bazele de date vizate și nu răspunde de securitatea lor, responsabilitatea revenind instituțiilor care le dețin și le administrează.[73] Pe 31 octombrie 2026, CNPDCP a anunțat inițierea unei investigații pentru a stabili circumstanțele și dacă instituțiile implicate și-au respectat obligațiile legale.[74]
- **Cancelaria de Stat** este fondatorul AGE, STISC și ASP și, prin Consiliul AGE, exercită supravegherea strategică.[75,76]

Golurile principale de responsabilitate identificate sunt trei. Primul este **lipsa unei delimitări publice și formale a rolurilor** de operator, operator asociat și persoană împuternicită între deținătorii registrelor, AGE și STISC pentru fiecare serviciu electronic. Al doilea este **absența unei funcții independente de asigurare a securității înainte de lansare**: nu există dovezi publice că serviciile care interoghează registre ar fi fost supuse obligatoriu unor teste de securitate sau unei evaluări de impact înainte de a fi expuse pe internet. Al treilea este **suprapunerea dintre ASC și STISC** în răspunsul la incidente din sectorul guvernamental, în condițiile în care cele două instituții se află în sfere de subordonare diferite (MDED, respectiv Cancelaria de Stat). În practică, comunicările din octombrie 2026 au fost comune, ceea ce sugerează o cooperare funcțională; dar baza normativă a acestei cooperări și ierarhia deciziilor în criză merită clarificate.

[69]Telegraph.md și Pivot.md, relatări privind notificarea Centrului Național pentru Protecția Datelor cu Caracter Personal de către AGE, octombrie 2026.

[70]Hotărârea Guvernului nr. 211/2019 privind platforma de interoperabilitate (MConnect).

[71]Hotărârea Guvernului nr. 482/2020 privind Serviciul Tehnologia Informației și Securitate Cibernetică (atribuții de echipă de răspuns la incidente pentru sectorul guvernamental).

[72]Hotărârea Guvernului nr. 1028/2023 privind organizarea și funcționarea Agenției pentru Securitate Cibernetică.

[73]NewsMaker, „Ce pot face moldovenii după scurgerea datelor personale? Centrul pentru Protecția Datelor cu Caracter Personal explică”, 29 octombrie 2026, https://newsmaker.md/ro/ce-pot-face-moldovenii-dupa-scurgerea-datelor-personale-centrul-pentru-protectia-datelor-cu-caracter-personal-explica.

[74]Timpul.md, „CNPDCP investighează extragerea neautorizată a datelor asociate cu aproximativ 750.000 de IDNP-uri”, 31 octombrie 2026, https://timpul.md/articol/cnpdcp-investigheaza-extragerea-neautorizata-a-datelor-asociate-cu-aproximativ-750000-de-idnp-uri-b12f4b8c.html.

[75]Guvernul Republicii Moldova, „Lista structurilor organizaționale în care Cancelaria de Stat are calitatea de fondator”.

[76]Consiliul I.P. „Agenția de Guvernare Electronică”, Decizia nr. 23 din 23.12.2025 (Raportul privind realizarea Planului de acțiuni al AGE pentru anul 2025).

4. Studiul de caz: incidentul AGE din octombrie 2026

4.1. Ecosistemul serviciilor publice digitale

Pentru a înțelege incidentul, trebuie înțeleasă arhitectura în care s-a produs. Serviciile publice digitale ale Republicii Moldova sunt construite din componente partajate, dezvoltate în mare parte de AGE începând cu 2010:

- **EVO** — aplicația și portalul guvernamental prin care cetățenii accesează servicii și documente electronice și care funcționează ca portofel guvernamental pentru identitate digitală.[77] EVO afișează utilizatorului și istoricul accesărilor datelor sale de către instituții.
- **MPass** — serviciul guvernamental de autentificare și control al accesului.
- **MSign** — serviciul de semnătură electronică.
- **MPay** — serviciul guvernamental de plăți electronice; istoricul plăților prin acest serviciu se numără printre datele extrase.[78]
- **MConnect** — platforma de interoperabilitate prin care serviciile și instituțiile interoghează registrele de stat.[79]
- **MLog** — serviciul de jurnalizare a evenimentelor, care înregistrează accesările.
- **Registrele de stat** — Registrul de stat al populației, registrele de asigurări sociale și medicale, registrul transporturilor, registrul persoanelor juridice, datele fiscale și altele, deținute de instituții diferite.

Potrivit conducerii AGE, din cele peste 400 de servicii publice electronice, circa 220 sunt gestionate de AGE, restul fiind administrate de alți prestatori.[80] Această fragmentare se reflectă și în restabilirea serviciilor: AGE a precizat că serviciile rămase indisponibile după 30 octombrie sunt gestionate de mai mulți prestatori.[81]

Arhitectura are o logică clară și beneficii reale: cetățeanul nu mai aduce acte pe care statul le deține deja, iar fiecare acces la date lasă o urmă vizibilă pentru persoana vizată. Același model creează însă un punct de concentrare: serviciile electronice care, pentru a funcționa, pot interoga mai multe registre au devenit — în lipsa unor controale adecvate — o interfață prin care date din mai multe surse puteau fi obținute pe baza unui singur identificator.

4.2. Cronologia incidentului

Tabelul 2 prezintă principalele momente, în ordine cronologică. O cronologie detaliată, cu ore și surse, se află în Anexa 1.

Tabelul 2. Cronologia sintetică a incidentului (19 octombrie – 3 noiembrie 2026)

Data	Eveniment	Nivel de certitudine
19–23 oct.	Interogări automate folosind circa 1 milion de IDNP; date extrase pentru circa 750.000	Confirmat oficial (preliminar)

[77] Ziar.md, „CEC renunță la identificarea digitală a alegătorilor la scrutinele din 1 noiembrie”, octombrie 2026.

[78] Agenția de Guvernare Electronică (AGE), comunicat privind estimările preliminare ale incidentului cibernetic din 19–23 octombrie 2026, 27 octombrie 2026.

[79] Hotărârea Guvernului nr. 211/2019 privind platforma de interoperabilitate (MConnect).

[80] Unimedia, interviu cu Nicoleta Colomeeț, directoarea AGE, 31 octombrie 2026.

[81] IPN, „Utilizatorii EVO vor trebui să instaleze cea mai recentă versiune a aplicației”, octombrie 2026.

Data	Eveniment	Nivel de certitudine
22 oct., seara	Cetățeni observă în EVO accesări suspecte ale datelor proprii și semnalează public	Relatat de presă
23 oct., 11:20	Incidentul este înregistrat formal	Declarat de conducerea AGE
23 oct., 11:30	Extragerea este oprită; 82 de servicii și peste 30 de sisteme și panouri de administrare sunt deconectate preventiv	Confirmat oficial
24 oct.	Comunicat comun AGE, STISC și ASC	Confirmat oficial
25 oct., ~02:00	Tentativă de acces forțat, blocată	Confirmat oficial
27 oct., ~07:00	Noi tentative de extragere, fără succes; AGE publică estimările preliminare	Confirmat oficial
28 oct.	Premierul anunță retragerea directoarei AGE; Președinta convoacă Consiliul Național de Securitate	Confirmat oficial
29 oct.	CNPDCP publică îndrumări pentru cetățeni; STISC explică riscurile privind IBAN	Confirmat oficial
30 oct.	61 de servicii restabilite, 21 indisponibile; Procuratura anunță pornirea urmăririi penale; predarea interimatului la AGE	Confirmat oficial / relatat de presă
31 oct.	CNPDCP anunță investigație proprie	Relatat de presă
1 nov.	Alegeri desfășurate fără identificarea alegătorilor prin EVO; STISC: semnătura electronică funcționează normal	Confirmat oficial
4 nov. (programat)	Audieri parlamentare cu ușile închise	Anunțat oficial

O observație metodologică se impune. Primul comunicat comun al AGE, STISC și ASC a plasat incidentul „în noaptea de 22 octombrie”.[82] Comunicatul AGE din 27 octombrie a extins perioada la 19–23 octombrie.[83] Revizuirea este firească într-o investigație în desfășurare și arată că activitatea atacatorilor a început cu cel puțin trei zile înainte de a fi observată.

4.3. Ce date au fost extrase

AGE și CNPDCP au descris categoriile de date extrase. Ele sunt grupate în Tabelul 3, împreună cu evaluarea autorului privind potențialul de prejudiciu.

Tabelul 3. Categoriile de date extrase și potențialul de prejudiciu

Categorie	Exemple (conform comunicărilor oficiale)	Potențial de prejudiciu
Identificare	Nume, prenume, IDNP, data și locul nașterii, fotografie	Ridicat – baza furtului de identitate și a documentelor false
Familie	Părinți și copii (rude de gradul întâi)	Ridicat – inginerie socială, presiuni, localizarea minorilor
Sănătate și protecție socială	Statut de asigurat, medic de familie, prestații sociale, pensii, dizabilitate	Foarte ridicat – categorie specială; risc de discriminare și de țintire a persoanelor vulnerabile

[82] AGE, Serviciul Tehnologia Informației și Securitate Cibernetică (STISC) și Agenția pentru Securitate Cibernetică (ASC), comunicat comun privind incidentul de securitate cibernetică asupra serviciilor publice digitale, 24 octombrie 2026, egov.md.

[83] Agenția de Guvernare Electronică (AGE), comunicat privind estimările preliminare ale incidentului cibernetic din 19–23 octombrie 2026, 27 octombrie 2026.

Categorie	Exemple (conform comunicărilor oficiale)	Potențial de prejudiciu
Documente și bunuri	Permis de conducere, vehicule, companii deținute sau administrate	Moderat–ridicat – profilare patrimonială, fraude
Financiare	Coduri IBAN, obligații fiscale, istoric de plăți prin MPay	Ridicat – fraude credibile, șantaj, deși IBAN-ul singur nu permite accesul la cont

Sursa: AGE, CNPDCP, STISC;[84,85,86] evaluarea potențialului de prejudiciu aparține autorului.

Două precizări ale autorităților sunt importante pentru proporționalitatea analizei. Prima: nu toate persoanele au avut expuse toate categoriile de date.[87] A doua: nu au fost identificate modificări neautorizate ale datelor din registre, iar accesarea informațiilor despre un bun sau o companie nu echivalează cu transferul dreptului de proprietate.[88] STISC a precizat, de asemenea, că un cod IBAN nu permite, singur, accesul la contul bancar.[89]

La 29 octombrie nu exista nicio confirmare publică privind punerea în circulație a datelor extrase.[90] La data de referință a studiului, nu am identificat o confirmare oficială că setul a fost publicat sau comercializat. Această informație rămâne **neconfirmată**.

4.4. Vectorul de atac, la nivel conceptual

Potrivit AGE, atacatorii au folosit servicii accesibile fără autentificare și, ulterior, datele obținute pentru extrageri suplimentare.[91] Prim-ministrul Vasile Tofan a declarat că atacatorii au exploatat vulnerabilități ale unor servicii digitale și au automatizat extragerea, iar unele vulnerabilități ar fi putut fi identificate cu ajutorul inteligenței artificiale.[92] Cetățenii care și-au verificat istoricul în EVO au observat accesări atribuite unor solicitări de documente de stare civilă sau de perfectare a permisului de conducere.[93]

Pe baza acestor elemente publice, incidentul poate fi încadrat conceptual în categoriile OWASP API Security Top 10. Încadrarea de mai jos este **o interpretare analitică a autorului**, nu o constatare oficială a anchetei.

[84]Agenția de Guvernare Electronică (AGE), comunicat privind estimările preliminare ale incidentului cibernetic din 19–23 octombrie 2026, 27 octombrie 2026.

[85]NewsMaker, „Ce pot face moldovenii după scurgerea datelor personale? Centrul pentru Protecția Datelor cu Caracter Personal explică”, 29 octombrie 2026.

[86]Agerpres și Moldpres, relatări privind declarațiile STISC despre riscurile asociate codurilor IBAN extrase și data audierilor parlamentare, 29 octombrie 2026.

[87]NewsMaker, „Datele a circa 750.000 de persoane din Moldova au ajuns la hackeri. Autoritățile avertizează: pot fi folosite pentru fraudă”, 27 octombrie 2026.

[88]NewsMaker, „Datele a circa 750.000 de persoane din Moldova au ajuns la hackeri. Autoritățile avertizează: pot fi folosite pentru fraudă”, 27 octombrie 2026.

[89]Agerpres și Moldpres, relatări privind declarațiile STISC despre riscurile asociate codurilor IBAN extrase și data audierilor parlamentare, 29 octombrie 2026.

[90]Mediacritica, „Atacul asupra datelor personale: ce știm, ce nu știm și ce pericole subestimăm”, 2026.

[91]Agenția de Guvernare Electronică (AGE), comunicat privind estimările preliminare ale incidentului cibernetic din 19–23 octombrie 2026, 27 octombrie 2026.

[92]TVR Moldova, „Cine răspunde pentru furtul de date ale moldovenilor? Procuratura a pornit o urmărire penală”, 30 octombrie 2026.

[93]Gândul, „Cel mai puternic atac cibernetic asupra Republicii Moldova a fost anunțat în ziua vizitei premierului Niculescu la Chișinău”, 27 octombrie 2026, https://www.gandul.ro/actualitate/atac-cibernetic-republica-moldova-date-personale-21046430.

- **Autentificare absentă sau insuficientă (API2).** Faptul confirmat oficial că unele servicii erau accesibile fără autentificare este elementul central. Un serviciu care returnează date personale unui solicitant neidentificat încalcă principiul protecției datelor în mod implicit.
- **Autorizare defectuoasă la nivel de obiect (API1).** Dacă un serviciu returnează datele persoanei X oricui furnizează identificatorul lui X, atunci identificatorul joacă rolul de cheie de acces. IDNP-ul nu este un secret: apare pe documente, în contracte și în baze de date scurse anterior.
- **Expunere excesivă de date (API3).** Diversitatea categoriilor extrase sugerează că unele servicii returnau mai multe câmpuri decât erau strict necesare scopului lor. Ipoteza este compatibilă cu observația că accesările apăreau sub denumirea unor servicii cu scop limitat.
- **Lipsa limitării ratei de cereri (API4).** Presa a relatat, iar conducerea AGE a confirmat, un volum de aproximativ 11 milioane de solicitări.[94,95,96] Raportat la circa patru zile și jumătate, rezultă o medie de ordinul a câteva zeci de cereri pe secundă — un volum care ar fi trebuit să fie blocat de mecanisme de limitare a ratei sau semnalat de sistemele de monitorizare.
- **Înlănțuirea serviciilor.** Formula oficială — datele obținute au fost folosite pentru extrageri ulterioare — descrie un atac în care rezultatul unui serviciu devine intrarea pentru altul. Raportul de circa 11 cereri pentru fiecare IDNP interogat este compatibil cu interogarea mai multor servicii pentru aceeași persoană, în scopul agregării. Și această observație este o estimare a autorului.

Studiul nu are acces la jurnalele tehnice și nu descrie serviciile concrete, structura cererilor sau instrumentele utilizate. Remedierile corespunzătoare sunt însă generice și cunoscute: autentificare obligatorie pentru orice serviciu care returnează date personale; verificarea, la fiecare cerere, a dreptului solicitantului asupra datelor cerute; minimizarea câmpurilor returnate; limitarea ratei de cereri; detectarea anomaliilor (capitolul 9).

4.5. Detectarea

Detectarea este, probabil, cea mai importantă lecție a incidentului. Activitatea atacatorilor a durat circa patru zile (19–23 octombrie) până la oprire. Cazul a devenit public după ce mai mulți cetățeni au observat în EVO înregistrări suspecte privind accesarea datelor lor în noaptea de 22 octombrie.[97] Unii au cerut public explicații, inclusiv pe rețelele sociale, întrebând AGE de ce le-au fost accesate datele la ore târzii.[98] Fosta directoare a AGE a declarat că primele semnale au venit prin rapoartele cetățenilor către serviciul de suport, că incidentul a fost înregistrat formal vineri, 23 octombrie, la 11:20, și că sistemele de monitorizare nu au semnalat traficul.[99]

Aceste date indică faptul că **detectarea a fost externă și reactivă**: transparența oferită cetățenilor prin jurnalul de accesări din EVO a funcționat ca sistem de alarmă, nu monitorizarea instituțională. Prin comparație, în cazul RIA din Estonia (2021), un partener privat a semnalat

[94]The Record (Recorded Future News), relatare privind atacul asupra serviciilor publice digitale ale Republicii Moldova și cele aproximativ 11 milioane de solicitări, octombrie 2026.

[95]Jurnal.md, relatare privind volumul de aproximativ 11 milioane de solicitări înregistrate în timpul atacului, octombrie 2026.

[96]Radio Moldova, „Datele personale a 750.000 de cetățeni, extrase în urma atacului cibernetic asupra sistemelor guvernamentale”, octombrie 2026, https://radiomoldova.md/p/88297.

[97]NewsMaker, „(GHID) Ce faci dacă datele tale personale au ajuns la hackeri. Ce drepturi ai și când poți cere despăgubiri”, octombrie 2026.

[98]Gândul, „Cel mai puternic atac cibernetic asupra Republicii Moldova a fost anunțat în ziua vizitei premierului Niculescu la Chișinău”, 27 octombrie 2026.

[99]Unimedia, interviu cu Nicoleta Colomeeț, directoarea AGE, 31 octombrie 2026.

un volum anormal de interogări după patru zile, iar agenția a închis serviciul după nouă zile de activitate a atacatorului;[100,101] în cazul Optus, vulnerabilitatea a rămas nedetectată ani la rând.[102] Durata de patru zile nu este, așadar, excepțională în comparație internațională, dar faptul că alarma a venit din partea cetățenilor și nu din partea sistemelor de securitate indică o lacună de capacitate de monitorizare.

Explicația oferită de AGE trebuie, de asemenea, consemnată. Conducerea instituției a arătat că în aproape doi ani au fost gestionate circa 40 de incidente, niciunul critic, ceea ce sugerează o capacitate operațională existentă.[103] Un trafic care imită cereri legitime către servicii publice, distribuit în timp, este mai greu de distins decât un atac de tip blocare a serviciului. Această dificultate este reală; ea argumentează însă în favoarea unor reguli de detectare bazate pe comportament (de exemplu, numărul de persoane distincte interogate de același solicitant), nu doar pe volum sau pe semnături.

4.6. Răspunsul și izolarea

Odată detectat incidentul, răspunsul a fost rapid. Extragerea a fost oprită în aproximativ zece minute de la înregistrarea formală, iar AGE a deconectat preventiv 82 de servicii publice și peste 30 de sisteme informaționale și panouri de administrare.[104] Deconectarea panourilor de administrare indică faptul că echipa a tratat incidentul ca potențial mai amplu decât o simplă expunere a unor servicii, ceea ce este o practică prudentă.

Tentativele ulterioare din 25 octombrie (în jurul orei 02:00) și din 27 octombrie (în jurul orei 07:00) au fost blocate, iar verificările nu au identificat noi extrageri.[105,106] La 30 octombrie, 61 de servicii fuseseră restabilite, iar 21 rămâneau indisponibile; reluarea celorlalte urma să aibă loc treptat, după verificări de securitate.[107] Ulterior au fost restabilite încă 11 servicii, inclusiv mai multe extrase din Registrul de stat al populației și din Registrul de stat al persoanelor juridice.[108] Serviciile pentru actele permisive au fost, de asemenea, repuse în funcțiune, iar serviciul „e-Traversare” al Poliției de Frontieră a fost limitat temporar.[109]

Alte măsuri de răspuns au inclus actualizarea obligatorie a aplicației EVO, prezentată de AGE drept măsură de consolidare a securității,[110] dezactivarea temporară a unor funcții de autentificare și renunțarea, de către Comisia Electorală Centrală, la identificarea alegătorilor prin EVO la scrutinele din 1 noiembrie, „după finalizarea tuturor verificărilor de securitate”

[100] Postimees, „Hacker gains access to hundreds of thousands of document photos”, iulie 2021, https://news.postimees.ee/7303667/hacker-gains-access-to-hundreds-of-thousands-of-document-photos.

[101] The Record, „Estonia says a hacker downloaded 286,000 ID photos from government database”, iulie 2021, https://therecord.media/estonia-says-a-hacker-downloaded-286000-id-photos-from-government-database.

[102] CSO Online, „Optus breach occurred due to a coding error, alleges ACMA”, 2024, https://www.csoonline.com/article/2492520/optus-breach-occurred-due-to-a-coding-error-alleges-acma.html.

[103] Unimedia, interviu cu Nicoleta Colomeeț, directoarea AGE, 31 octombrie 2026.

[104] Agenția de Guvernare Electronică (AGE), comunicat privind estimările preliminare ale incidentului cibernetic din 19–23 octombrie 2026, 27 octombrie 2026.

[105] Agenția de Guvernare Electronică (AGE), comunicat privind estimările preliminare ale incidentului cibernetic din 19–23 octombrie 2026, 27 octombrie 2026.

[106] AGE, comunicat privind restabilirea a 61 de servicii publice digitale, 30 octombrie 2026.

[107] AGE, comunicat privind restabilirea a 61 de servicii publice digitale, 30 octombrie 2026.

[108] Ziar.md, „Alte 11 servicii publice digitale au devenit disponibile după atacurile cibernetice”, noiembrie 2026, https://ziar.md/alte-11-servicii-publice-digitale-au-devenit-disponibile-dupa-atacurile-cibernetice/.

[109] Radio Chișinău, „Agenția de Guvernare Electronică a activat actualizarea obligatorie a aplicației EVO”, 30 octombrie 2026, https://radiochisinau.md/agentia-de-guvernare-electronica-a-activat-actualizarea-obligatorie-a-aplicatiei-evo---230480.html.

[110] IPN, „Utilizatorii EVO vor trebui să instaleze cea mai recentă versiune a aplicației”, octombrie 2026.

urmând a se relua dialogul.[111] STISC a comunicat la 1 noiembrie că semnătura electronică și serviciile de încredere funcționează normal.[112]

Pe plan instituțional, prim-ministrul a anunțat la 28 octombrie retragerea directoarei AGE; interimatul a fost preluat de Artiom Cociu.[113] Președinta Maia Sandu a convocat Consiliul Național de Securitate.[114] La data de referință nu am identificat decizii publice ale Consiliului privind acest incident. Comisia parlamentară pentru securitate națională, apărare și ordine publică a decis, în unanimitate, organizarea de audieri, programate pentru 4 noiembrie, cu ușile închise.[115,116] Procuratura a anunțat la 30 octombrie pornirea urmăririi penale,[117] iar CNPDCP a inițiat o investigație proprie.[118]

Evaluare. Izolarea a fost rapidă și cuprinzătoare, iar restabilirea graduală, condiționată de verificări, este conformă bunelor practici. Deconectarea a 82 de servicii a avut un cost real pentru cetățeni și firme, dar a fost proporțională cu incertitudinea din primele zile. Punctul slab al răspunsului nu este izolarea, ci etapa care a precedat-o (detectarea) și cea care a urmat-o (informarea individuală a persoanelor afectate).

4.7. Comunicarea publică

Comunicarea a avut câteva puncte forte. Incidentul a fost anunțat public la circa o zi după înregistrarea formală, printr-un comunicat comun al celor trei instituții tehnice.[119] Estimările preliminare au fost publicate la patru zile de la oprirea extragerii, cu precizarea explicită că sunt preliminare și că nu toți cei afectați au avut expuse toate categoriile.[120] Autoritățile au formulat consecvent mesajul de prevenție: riscul principal este folosirea datelor în tentative de fraudă și manipulare online, iar persoane rău intenționate se pot prezenta drept reprezentanți ai băncilor sau ai instituțiilor publice pentru a cere bani, parole sau coduri.[121] STISC a corectat o temere larg răspândită, explicând că IBAN-ul singur nu permite accesul la cont.[122] CNPDCP a explicat

[111] Ziar.md, „CEC renunță la identificarea digitală a alegătorilor la scrutinele din 1 noiembrie”, octombrie 2026.

[112] STISC, comunicat privind funcționarea normală a semnăturii electronice și a serviciilor de încredere, 1 noiembrie 2026.

[113] TVR Moldova, „Cine răspunde pentru furtul de date ale moldovenilor? Procuratura a pornit o urmărire penală”, 30 octombrie 2026.

[114] Digi24, „Consiliul de Securitate al R. Moldova, convocat după un atac cibernetic în care au fost furate datele personale a 750.000 de cetățeni”, 28 octombrie 2026, https://www.digi24.ro/stiri/externe/moldova/consiliul-de-securitate-al-r-moldova-convocat-dupa-un-atac-cibernetic-in-care-au-fost-furate-datele-personale-a-750-000-de-cetateni-4013145.

[115] Realitatea.md, „Cine răspunde pentru scurgerea datelor a sute de mii de moldoveni? Igor Grosu: Vor fi organizate audieri”, octombrie 2026, https://realitatea.md/video-cine-raspunde-pentru-scurgerea-datelor-a-sute-de-mii-de-moldoveni-igor-grosu-vor-fi-organizate-audieri/.

[116] TVR Moldova, „Cine răspunde pentru furtul de date ale moldovenilor? Procuratura a pornit o urmărire penală”, 30 octombrie 2026.

[117] TVR Moldova, „Cine răspunde pentru furtul de date ale moldovenilor? Procuratura a pornit o urmărire penală”, 30 octombrie 2026.

[118] Timpul.md, „CNPDCP investighează extragerea neautorizată a datelor asociate cu aproximativ 750.000 de IDNP-uri”, 31 octombrie 2026.

[119] AGE, Serviciul Tehnologia Informației și Securitate Cibernetică (STISC) și Agenția pentru Securitate Cibernetică (ASC), comunicat comun privind incidentul de securitate cibernetică asupra serviciilor publice digitale, 24 octombrie 2026, egov.md.

[120] Agenția de Guvernare Electronică (AGE), comunicat privind estimările preliminare ale incidentului cibernetic din 19–23 octombrie 2026, 27 octombrie 2026.

[121] NewsMaker, „Datele a circa 750.000 de persoane din Moldova au ajuns la hackeri. Autoritățile avertizează: pot fi folosite pentru fraudă”, 27 octombrie 2026.

[122] Agerpres și Moldpres, relatări privind declarațiile STISC despre riscurile asociate codurilor IBAN extrase și data audierilor parlamentare, 29 octombrie 2026.

drepturile persoanelor și căile de sesizare.[123] Cetățenii au fost informați că pot cere AGE informații despre accesările datelor lor, instituțiile care le-au efectuat și temeiurile invocate.[124]

Comunicarea a avut și limite. Prima: în primele zile, presa și publicul au pus întrebarea greșită — „ne golesc conturile?" —, iar riscurile de durată (furt de identitate, profilare, șantaj) au fost mai puțin explicate.[125] A doua: cifrele au fost transmise fragmentat, prin comunicate, interviuri și declarații politice; de exemplu, cifra de 11 milioane de cereri a apărut întâi în presă și a fost confirmată de conducerea AGE într-un interviu, nu într-un comunicat.[126,127] A treia: mesajele politice privind o „campanie mai largă" cu implicarea unor actori statali străini au precedat orice prezentare publică a probelor tehnice (secțiunea 4.9). A patra: un singur punct de informare pentru cetățeni — o pagină dedicată, actualizată, cu întrebări frecvente și un instrument de verificare individuală — nu a fost disponibil în primele zece zile.

4.8. Notificarea autorității și a persoanelor vizate

Notificarea CNPDCP. Presa a relatat că AGE a notificat CNPDCP.[128] Data și conținutul notificării nu au fost făcute publice, astfel încât respectarea termenului de 72 de ore prevăzut de art. 33 al Legii nr. 195/2024 nu poate fi verificată independent. Având în vedere că incidentul a fost înregistrat la 23 octombrie, termenul expira la 26 octombrie. Este un aspect pe care investigația CNPDCP îl poate clarifica.

Informarea persoanelor vizate. Potrivit art. 34, atunci când încălcarea este susceptibilă să genereze un risc ridicat pentru drepturile persoanelor, operatorul le informează fără întârzieri nejustificate. Combinația de date de identitate, fotografie, date de sănătate și date financiare face greu de susținut că riscul nu ar fi ridicat. La 30 octombrie, AGE a anunțat că pregătește un mecanism de notificare individuală, întocmind liste pe categorii de informații, verificate pentru eliminarea duplicatelor și a neconcordanțelor.[129] La data de referință (3 noiembrie), notificarea individuală nu fusese realizată și nu fusese anunțat un termen.

Legea permite înlocuirea informării individuale cu o comunicare publică atunci când informarea individuală ar necesita un efort disproporționat. Autoritățile au făcut comunicări publice ample. Însă AGE are mijloace de contact pentru o parte importantă a persoanelor (utilizatorii EVO) și și-a asumat public notificarea individuală. Din această perspectivă, întârzierea — explicabilă prin nevoia de a stabili cu precizie cine a fost afectat și ce date — riscă să depășească ceea ce poate fi considerat „fără întârzieri nejustificate". Experiența internațională arată că informarea individuală poate fi făcută în etape: un prim mesaj generic tuturor celor potențial afectați, urmat de detalii pe categorii de date. Singapore a început notificarea pacienților chiar în ziua anunțării publice a incidentului (capitolul 6).[130]

---

[123] NewsMaker, „Ce pot face moldovenii după scurgerea datelor personale? Centrul pentru Protecția Datelor cu Caracter Personal explică", 29 octombrie 2026.

[124] Timpul.md, „CNPDCP investighează extragerea neautorizată a datelor asociate cu aproximativ 750.000 de IDNP-uri", 31 octombrie 2026.

[125] Mediacritica, „Atacul asupra datelor personale: ce știm, ce nu știm și ce pericole subestimăm", 2026.

[126] The Record (Recorded Future News), relatare privind atacul asupra serviciilor publice digitale ale Republicii Moldova și cele aproximativ 11 milioane de solicitări, octombrie 2026.

[127] Unimedia, interviu cu Nicoleta Colomeeț, directoarea AGE, 31 octombrie 2026.

[128] Telegraph.md și Pivot.md, relatări privind notificarea Centrului Național pentru Protecția Datelor cu Caracter Personal de către AGE, octombrie 2026.

[129] Ziar.md, „Noi informații despre atacul cibernetic: 61 de servicii publice au fost restabilite, iar 21 rămân temporar indisponibile", 30 octombrie 2026, https://ziar.md/noi-informatii-despre-atacul-cibernetic-61-de-servicii-publice-au-fost-restabilite-2/.

[130] Wiki.sg, „SingHealth data breach (2018)", https://wiki.sg/p/SingHealth_data_breach_(2018).

4.9. Atribuirea

Studiul prezintă doar ce au declarat autoritățile, cu nivelul de certitudine exprimat de acestea:

- Prim-ministrul a vorbit despre o campanie mai largă, cu implicarea unor actori statali străini, fără a numi un stat și fără a prezenta public probe tehnice.[131]
- Potrivit relatărilor presei, purtătorul de cuvânt al Guvernului a încadrat incidentul într-o campanie hibridă.[132]
- Președinția a afirmat că atacul a fost, cel mai probabil, facilitat de inteligența artificială.[133]
- Investigația este condusă de STISC, ASC, SIS, AGE și structurile specializate ale Poliției.[134]

Contextul relevant, care nu echivalează cu o atribuire, include avertismentul public al SIS din 17 iunie 2026 privind colectarea coordonată de către serviciile speciale ruse a datelor personale ale cetățenilor Republicii Moldova, prin baze de date vândute ilegal, prin spargerea unor servere și prin baze de date colectate de o grupare criminală organizată, pentru a le folosi în fraude și escrocherii.[135] Directorul SIS a reiterat ulterior că aceste date pot fi folosite și în acțiuni de recrutare.[136]

Concluzia privind atribuirea: la data de referință, nu există o atribuire tehnică publică a incidentului unui actor anume. Ipoteza implicării unui actor statal este formulată de autorități, dar nu este susținută public de probe. Ipoteza unei operațiuni criminale cu scop financiar nu poate fi exclusă. Cele două nu se exclud reciproc: datele obținute de grupări criminale pot ajunge la servicii de informații și invers. Studiul tratează, prin urmare, atribuirea ca **neconfirmată** și recomandă publicarea unui raport tehnic de anchetă, cu nivelurile de încredere asociate.

4.10. Răspuns la întrebarea 1: vulnerabilitățile

Pe baza informațiilor publice, vulnerabilitățile care au făcut posibil incidentul pot fi grupate pe trei niveluri.

Tehnice:

- servicii care returnau date personale fără autentificare (confirmat oficial);
- lipsa verificării dreptului solicitantului asupra datelor cerute, cu IDNP folosit de facto drept cheie de acces (interpretare analitică);
- returnarea unor câmpuri care depășeau scopul serviciului (interpretare analitică);

[131] NewsMaker, relatare privind declarațiile prim-ministrului Vasile Tofan în ședința Guvernului din 28 octombrie 2026.

[132] NewsMaker, relatare privind declarațiile prim-ministrului Vasile Tofan în ședința Guvernului din 28 octombrie 2026.

[133] Digi24, „Consiliul de Securitate al R. Moldova, convocat după un atac cibernetic în care au fost furate datele personale a 750.000 de cetățeni”, 28 octombrie 2026.

[134] Agenția de Guvernare Electronică (AGE), comunicat privind estimările preliminare ale incidentului cibernetic din 19–23 octombrie 2026, 27 octombrie 2026.

[135] Digi24, „Serviciile secrete ale Rusiei colectează datele personale ale moldovenilor, avertizează SIS de la Chișinău”, iunie 2026, https://www.digi24.ro/stiri/externe/moldova/serviciile-secrete-ale-rusiei-colecteaza-datele-personale-ale-moldovenilor-avertizeaza-sis-de-la-chisinau-3819279; comunicatul SIS din 17 iunie 2026.

[136] Agerpres, „Directorul SIS avertizează că Rusia se pregătește deja de următoarele alegeri din Republica Moldova”, 2026, https://agerpres.ro/politic-extern/2026/07/09/directorul-sis-avertizeaza-ca-rusia-se-pregateste-deja-de-urmatoarele-alegeri-din-republica-moldova--1574709.

- lipsa limitării eficiente a ratei de cereri și a detectării comportamentului anormal (dedus din volumul de 11 milioane de cereri și din faptul că monitorizarea nu a semnalat traficul);
- posibilitatea înlănțuirii serviciilor pentru agregarea datelor (confirmat oficial în formula „datele obținute au fost folosite pentru extrageri ulterioare”).

Organizaționale:

- detectarea a depins de cetățeni, nu de un centru de monitorizare (confirmat de conducerea AGE);
- un portofoliu de peste 400 de servicii, administrate de prestatori diferiți, fără un inventar public și fără dovezi ale unor teste de securitate obligatorii înainte de lansare;
- absența unui program de raportare a vulnerabilităților cu recompensă (bug bounty) și a unor teste de penetrare publice și periodice ale serviciilor expuse;
- lipsa unui mecanism pregătit de notificare individuală a persoanelor afectate.

De guvernanță:

- concentrarea sub același fondator a administratorului de servicii, a operatorului tehnic și a deținătorului principalelor registre;
- neclaritatea rolurilor juridice (operator, operator asociat, persoană împuternicită) pentru fiecare serviciu;
- suprapunerea parțială dintre ASC și STISC în răspunsul la incidentele din sectorul guvernamental;
- un ciclu de verificare a conformității cu Legea nr. 48/2023 care nu ajunsese la primul punct de control;
- o autoritate de protecție a datelor cu sarcini noi și extinse din august 2026, a cărei capacitate de investigare a unui incident de această amploare nu a fost încă testată.

5. Analiza riscurilor

5.1. Abordare

Analiza aplică metoda descrisă în secțiunea 2.4 (NIST SP 800-30 Rev. 1, compatibilă cu ISO/IEC 27005:2022).[137,138] Obiectul evaluării nu este riscul ca incidentul să se producă — el s-a produs —, ci riscurile care decurg din faptul că un set amplu de date personale a ieșit de sub controlul statului. Pentru fiecare risc au fost estimate probabilitatea de materializare în următoarele 24 de luni și impactul, pe scale de la 1 la 5.

Câteva ipoteze de lucru stau la baza evaluării:

- datele extrase sunt considerate compromise permanent; chiar dacă nu au fost publicate până la data de referință, nu există un mecanism prin care ele să fie „recuperate”;
- o parte din date (IDNP, data nașterii, fotografia, relațiile de familie) nu pot fi schimbate de persoana vizată, spre deosebire de o parolă;
- setul poate fi combinat cu alte seturi de date despre cetățenii Republicii Moldova aflate deja în circulație, în special cu cele menționate de SIS în iunie 2026;[139]
- există actori motivați atât financiar (grupări de fraudă telefonică), cât și politic (operațiuni de influență), conform evaluărilor publice ale autorităților.[140,141]

5.2. Registrul riscurilor

Tabelul 4. Registrul riscurilor (P – probabilitate, I – impact, S – scor = P × I)

Cod	Risc	Sursa amenințării	P	I	S	Nivel
R1	Fraude telefonice și online personalizate (impersonarea băncii, poliției, instituțiilor)	Grupări de fraudă	5	4	20	Critic
R2	Furt de identitate și documente false folosind fotografia și datele de identificare	Grupări criminale	3	4	12	Ridicat
R3	Credite contractate fraudulos pe numele victimei	Grupări de fraudă	3	4	12	Ridicat
R4	Țintirea grupurilor vulnerabile (pensionari, persoane cu dizabilități, beneficiari de prestații)	Grupări de fraudă	4	4	16	Ridicat
R5	Expunerea datelor de sănătate și dizabilitate; stigmatizare, discriminare	Diverși	3	3	9	Moderat
R6	Șantaj și presiuni asupra unor categorii-cheie (funcționari, polițiști, militari, magistrați)	Actori statali, crimă organizată	3	4	12	Ridicat
R7	Doxxing și hărțuire a jurnaliștilor, activiștilor și politicienilor	Actori politici, grupuri organizate	3	4	12	Ridicat

[137]NIST, Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments, septembrie 2012.

[138]ISO/IEC 27005:2022, Information security, cybersecurity and privacy protection — Guidance on managing information security risks.

[139]Digi24, „Serviciile secrete ale Rusiei colectează datele personale ale moldovenilor, avertizează SIS de la Chișinău”, iunie 2026 comunicatul SIS din 17 iunie 2026.

[140]NewsMaker, „Datele a circa 750.000 de persoane din Moldova au ajuns la hackeri. Autoritățile avertizează: pot fi folosite pentru fraudă”, 27 octombrie 2026.

[141]Digi24, „Serviciile secrete ale Rusiei colectează datele personale ale moldovenilor, avertizează SIS de la Chișinău”, iunie 2026 comunicatul SIS din 17 iunie 2026.

Cod	Risc	Sursa amenințării	P	I	S	Nivel
R8	Presiuni asupra diasporei prin datele rudelor rămase în țară	Actori statali, fraudatori	3	3	9	Moderat
R9	Riscuri pentru siguranța minorilor (date despre copii legate de părinți)	Infractori	2	5	10	Ridicat
R10	Operațiuni hibride și dezinformare personalizată	Actori statali	4	4	16	Ridicat
R11	Manipulare electorală prin micro-țintire, intimidare sau mesaje false	Actori statali, actori politici	3	4	12	Ridicat
R12	Profilare la scară națională prin agregare cu scurgeri anterioare	Actori statali	4	5	20	Critic
R13	Identificarea și recrutarea persoanelor cu acces la informații sensibile	Servicii de informații străine	3	5	15	Ridicat
R14	Erodarea încrederii în serviciile digitale și revenirea la ghișeu	Efect sistemic	4	3	12	Ridicat
R15	Impact asupra evaluării progresului în negocierile de aderare la UE	Efect sistemic	3	3	9	Moderat
R16	Repetarea atacului prin servicii nerevizuite, inclusiv ale altor prestatori	Aceiași sau alți atacatori	3	5	15	Ridicat
R17	Ocolirea verificărilor de identitate la distanță (KYC), inclusiv cu imagini sintetice	Grupări de fraudă	3	4	12	Ridicat
R18	Contagiune în sectorul privat prin inginerie socială (bănci, operatori de telefonie)	Grupări de fraudă	4	3	12	Ridicat
R19	Suprasolicitarea Poliției, CNPDCP și a liniilor de suport	Efect sistemic	4	2	8	Moderat

Evaluarea aparține autorului, pe baza surselor publice citate în acest capitol.

5.3. Matricea probabilitate × impact

Tabelul 5. Matricea riscurilor (rânduri: probabilitate; coloane: impact)

Probabilitate \ Impact	1 – Foarte scăzut	2 – Scăzut	3 – Moderat	4 – Ridicat	5 – Foarte ridicat
5 – Foarte ridicată	—	—	—	R1	—
4 – Ridicată	—	R19	R14, R18	R4, R10	R12
3 – Moderată	—	—	R5, R8, R15	R2, R3, R6, R7, R11, R17	R13, R16
2 – Scăzută	—	—	—	—	R9
1 – Foarte scăzută	—	—	—	—	—

Distribuția este concentrată în zona superioară dreaptă: din 19 riscuri, două sunt critice, treisprezece ridicate și patru moderate. Niciun risc nu este scăzut, ceea ce reflectă natura datelor (multe imuabile) și contextul de securitate al țării.

5.4. Riscuri pentru persoane

Fraudele personalizate (R1) sunt riscul cu probabilitatea cea mai mare. Fraudele telefonice erau deja o problemă majoră înainte de incident; SIS a semnalat că multe dintre ele sunt

comise prin call-centre aflate peste hotare.[142] Ceea ce schimbă incidentul este credibilitatea: un apelant care cunoaște numele complet, data nașterii, numele copiilor, banca la care persoana are cont, pensia sau datoria fiscală exactă poate convinge mult mai ușor. Autoritățile au anticipat corect acest risc, avertizând că persoane rău intenționate se pot prezenta drept reprezentanți ai băncilor sau ai instituțiilor publice.[143] Impactul individual poate fi sever — pierderea economiilor —, iar la scară, efectul cumulat este semnificativ.

Grupurile vulnerabile (R4) sunt expuse disproporționat. Setul conține informații despre pensii, prestații sociale și dizabilitate. Aceste informații permit atacatorilor să selecteze exact persoanele care primesc plăți regulate de la stat și care sunt, statistic, mai puțin familiarizate cu tehnicile de inginerie socială. Un apel de tipul „sunteți beneficiar al prestației X, trebuie să confirmați datele pentru recalculare" devine extrem de credibil.

Furtul de identitate și creditele frauduloase (R2, R3) depind de calitatea verificărilor din sectorul financiar. Combinația dintre fotografie, IDNP, data și locul nașterii și numele părinților acoperă o mare parte din datele cerute la deschiderea unui cont sau la contractarea unui credit online. Riscul este mai mare în segmentul creditării nebancare la distanță. El poate fi redus prin întărirea verificărilor și prin instrumente la îndemâna cetățeanului, precum blocarea voluntară a creditării pe IDNP (capitolul 9).

Datele de sănătate (R5) sunt, în acest caz, limitate: statutul de asigurat, medicul de familie și informații despre dizabilitate, nu dosare medicale. Impactul este deci moderat, dar nu neglijabil: informația despre dizabilitate poate duce la stigmatizare sau discriminare, iar faptul că o persoană nu este asigurată medical poate fi folosit în scheme de fraudă („vă putem restabili asigurarea contra unei taxe").

Șantajul, doxxing-ul și hărțuirea (R6, R7) privesc mai puțini oameni, dar cu efecte individuale grave. Pentru jurnaliști, activiști, magistrați sau polițiști, datele despre familie, adresele asociate bunurilor și vehiculele reprezintă materie primă pentru intimidare. **Diaspora (R8)** este vulnerabilă prin datele rudelor rămase în țară. **Minorii (R9)** apar în set prin legătura cu părinții; probabilitatea unui abuz direct este scăzută, dar impactul potențial justifică încadrarea în categoria „ridicat".

5.5. Riscuri pentru stat și pentru securitatea națională

Profilarea prin agregare (R12) este riscul strategic principal. Luat izolat, setul AGE este grav; combinat cu alte seturi — date de contact din baze vândute ilegal, liste de persoane colectate de grupări organizate, date din servere private compromise —, el permite construirea unui profil detaliat pentru o mare parte a populației adulte. SIS a avertizat public, cu patru luni înainte de incident, că serviciile speciale ruse colectează în mod coordonat datele personale ale cetățenilor Republicii Moldova din astfel de surse, inclusiv o bază de date de circa 145.000 de persoane colectată, potrivit SIS, de o grupare criminală organizată.[144] În acest context, setul AGE ar reprezenta, pentru un actor ostil, o „coloană vertebrală" verificată, provenită din registrele statului, la care pot fi atașate celelalte surse. Studiul nu afirmă că datele au ajuns la un astfel de actor — acest lucru nu este confirmat —, ci că riscul ca acest lucru să se întâmple este ridicat, iar impactul ar fi foarte ridicat și de lungă durată.

Operațiunile hibride și manipularea electorală (R10, R11) decurg din profilare. Datele despre vârstă, localitate, familie, prestații și bunuri permit segmentarea mesajelor de

[142] Agerpres, „Directorul SIS avertizează că Rusia se pregătește deja de următoarele alegeri din Republica Moldova", 2026.

[143] NewsMaker, „Datele a circa 750.000 de persoane din Moldova au ajuns la hackeri. Autoritățile avertizează: pot fi folosite pentru fraudă", 27 octombrie 2026.

[144] Digi24, „Serviciile secrete ale Rusiei colectează datele personale ale moldovenilor, avertizează SIS de la Chișinău", iunie 2026 comunicatul SIS din 17 iunie 2026.

dezinformare și țintirea unor grupuri precise (de exemplu, pensionarii dintr-o anumită regiune, cu mesaje false despre pensii). Decizia Comisiei Electorale Centrale de a nu folosi EVO pentru identificarea alegătorilor la 1 noiembrie arată că instituțiile au luat în serios riscul electoral imediat.[145] Riscul pe termen mediu privește ciclurile electorale viitoare.

Recrutarea și contrainformațiile (R13) reprezintă dimensiunea cea mai puțin vizibilă. Datele despre companiile administrate, bunuri, datorii fiscale și familie pot ajuta la identificarea unor persoane cu acces la informații sensibile și a unor posibile vulnerabilități (datorii, situații familiale). Directorul SIS a menționat explicit folosirea datelor personale colectate în acțiuni de recrutare.[146] Cazul OPM din Statele Unite (capitolul 6) arată că efectele unei astfel de expuneri asupra contrainformațiilor se pot întinde pe decenii.

Încrederea (R14) este, poate, costul cel mai greu de cuantificat. Digitalizarea serviciilor publice a fost una dintre reformele de succes ale Republicii Moldova. Dacă cetățenii asociază digitalizarea cu riscul, ei pot reveni la ghișeu, iar câștigurile de eficiență și de integritate (mai puține interacțiuni directe, mai puține ocazii de corupție) se pot pierde. Pe de altă parte, faptul că alarma a fost dată de cetățeni prin jurnalul de accesări din EVO arată că transparența sistemului a funcționat și poate fi un argument pentru încredere, dacă răspunsul statului este credibil.

Aderarea la UE (R15). Incidentul nu blochează negocierile, dar va fi un test pentru evaluarea capacității administrative în domeniile protecției datelor și societății informaționale. Comisia Europeană evaluează nu doar adoptarea legislației, ci și aplicarea ei efectivă.[147] O investigație credibilă a CNPDCP, măsuri corective vizibile și transparență vor conta mai mult decât incidentul în sine.

5.6. Riscuri sistemice

Repetarea (R16). Atacatorii au încercat să revină la 25 și 27 octombrie.[148] Portofoliul de servicii include sute de servicii, administrate de prestatori diferiți; 21 de servicii erau încă indisponibile la 30 octombrie.[149] Riscul ca o vulnerabilitate similară să existe în alt serviciu, nerevizuit, nu poate fi exclus fără un inventar complet și teste independente.

Ocolirea verificărilor de identitate la distanță (R17). Combinația de fotografie oficială și date de identificare poate fi folosită pentru a încerca ocolirea procedurilor de verificare la distanță, inclusiv cu imagini sau înregistrări generate artificial. Riscul crește odată cu răspândirea instrumentelor de generare a imaginilor.

Contagiunea în sectorul privat (R18). Băncile, operatorii de telefonie și furnizorii de servicii de plată vor fi ținta unor tentative de inginerie socială în care atacatorii se prezintă drept clienți reali, cunoscând datele acestora. Fără o coordonare cu Banca Națională, Comisia Națională a Pieței Financiare și autoritatea de reglementare în comunicații, fiecare entitate își va gestiona riscul separat.

Suprasolicitarea instituțiilor (R19). Un număr mare de sesizări către Poliție, CNPDCP și liniile de suport poate depăși capacitatea acestora. Riscul este moderat, dar efectul asupra încrederii poate fi amplificat dacă cetățenii nu primesc răspuns.

[145] Ziar.md, „CEC renunță la identificarea digitală a alegătorilor la scrutinele din 1 noiembrie”, octombrie 2026.

[146] Agerpres, „Directorul SIS avertizează că Rusia se pregătește deja de următoarele alegeri din Republica Moldova”, 2026.

[147] Moldpres, „Moldova - leader among EU expansion candidate states”, noiembrie 2025, https://www.moldpres.md/eng/eu-1/moldova-leader-among-eu-expansion-candidate-states.

[148] Agenția de Guvernare Electronică (AGE), comunicat privind estimările preliminare ale incidentului cibernetic din 19–23 octombrie 2026, 27 octombrie 2026.

[149] AGE, comunicat privind restabilirea a 61 de servicii publice digitale, 30 octombrie 2026.

5.7. Riscuri reziduale

Chiar și în ipoteza implementării integrale a recomandărilor din capitolul 9, unele riscuri vor rămâne ridicate pe termen lung:

- **Riscurile legate de identitate (R2, R12, R13, R17)** rămân ridicate pentru că datele de identificare, fotografia și relațiile de familie nu pot fi schimbate. Măsurile pot reduce probabilitatea exploatării (verificări mai bune, blocarea creditării, monitorizare), dar nu și existența datelor.
- **Riscul de fraudă (R1, R4)** poate scădea la nivel moderat în 12–24 de luni, prin educație publică, alerte bancare și cooperare între instituții, dar nu va dispărea.
- **Riscul de repetare (R16)** poate fi redus la nivel moderat prin autentificare obligatorie, autorizare la nivel de obiect, limitarea ratei de cereri și monitorizare, cu condiția verificării independente.
- **Riscul de încredere (R14)** depinde aproape integral de calitatea răspunsului instituțional: o anchetă transparentă și măsuri vizibile îl pot reduce semnificativ.

Tabelul A3 din Anexa 3 prezintă estimarea autorului privind nivelul rezidual al fiecărui risc după implementarea măsurilor recomandate.

6. Experiențe internaționale

6.1. Selecția cazurilor

Din lista de cazuri candidate au fost reținute șapte, după criteriile din secțiunea 2.5. Fiecare aduce o lecție diferită:

- **Estonia, 2021 (RIA)** — cel mai apropiat vector de cazul AGE: extragerea în masă, prin interogări, a fotografiilor de pe documentele de identitate dintr-un serviciu de stat.
- **Australia, 2022 (Optus)** — o interfață expusă pe internet fără verificarea credențialelor; consecințe juridice pe termen lung.
- **Bulgaria, 2019 (NRA)** — scurgerea datelor fiscale ale majorității populației dintr-o agenție de stat; amendă aplicată unei autorități publice și jurisprudență a CJUE.
- **Singapore, 2018 (SingHealth)** — date de sănătate, actor statal sofisticat, comisie independentă de anchetă cu raport public.
- **Albania, 2022** — atac al unui actor statal asupra portalului de servicii publice; atribuire publică și reacție diplomatică.
- **Franța, 2024 (France Travail)** — cea mai mare scurgere din sectorul public francez; amendă aplicată unei instituții publice.
- **Statele Unite, 2015 (OPM)** — date ale persoanelor verificate pentru acces la informații secrete; consecințe de contrainformații.

Alte cazuri candidate au fost luate în considerare, dar nu au fost analizate separat. Atacurile asupra Estoniei din 2007 și vulnerabilitatea criptografică ROCA din 2017 sunt menționate ca context al cazului estonian. Atacul de tip ransomware asupra Costa Ricăi (2022) și atacurile asupra spitalelor din România (2024) vizează în principal disponibilitatea serviciilor, nu extragerea de date prin interfețe, astfel că lecțiile lor sunt mai puțin transferabile. Afirmațiile repetate privind scurgeri din aplicația ucraineană Diia sunt relevante pentru dimensiunea de dezinformare, dar nu au putut fi verificate pe baza unor surse oficiale suficiente.

6.2. Estonia: extragerea fotografiilor din baza documentelor de identitate (2021)

Context. Estonia este considerată un etalon al guvernării electronice. Atacurile cibernetice din 2007 au precedat acreditarea, în 2008, a Centrului de Excelență NATO pentru Apărare Cibernetică Cooperativă (CCDCOE) de la Tallinn.[150] În 2017, vulnerabilitatea ROCA a afectat cipurile a sute de mii de cărți de identitate, iar statul a revocat și actualizat certificatele.

Vectorul. În iulie 2021, un atacator a descărcat fotografiile de pe documentele de identitate ale 286.438 de persoane, prin interogări repetate la un serviciu de fotografii administrat de Autoritatea Sistemului Informațional (RIA). Atacatorul nu a pătruns în baza de date, ci a abuzat de o vulnerabilitate care permitea obținerea fotografiei unei persoane prin interogări.[151] RIA a explicat că suspectul a găsit o vulnerabilitate într-una dintre aplicații, care nu verifica suficient validitatea interogării; pentru exploatare, atacatorul trebuia să cunoască numele și codul personal al persoanei — date pe care le obținuse anterior.[152] Au fost folosite circa 9.000 de adrese IP din Estonia și din străinătate.[153]

[150] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), informații instituționale, https://ccdcoe.org.

[151] The Baltic Times, „Hundreds of thousands of ID photos illegally downloaded in Estonia", 28 iulie 2021, https://www.baltictimes.com/hundreds_of_thousands_of_id_photos_illegally_downloaded_in_estonia.

[152] The Record, „Estonia says a hacker downloaded 286,000 ID photos from government database", iulie 2021.

[153] Postimees, „Hacker gains access to hundreds of thousands of document photos", iulie 2021.

Detectare și răspuns. Primele descărcări au avut loc pe 12 iulie, iar activitatea a fost oprită nouă zile mai târziu.[154] Un furnizor privat de servicii de identitate a semnalat un volum neobișnuit de interogări, iar RIA a detectat descărcarea în masă și a închis serviciul la 21 iulie.[155] Un suspect a fost arestat la 23 iulie, într-o anchetă comună a poliției și RIA. Toate persoanele afectate au fost notificate prin e-mail de Poliție și Poliția de Frontieră, iar autoritățile au precizat că documentele rămân valabile și că trio-ul fotografie–cod personal–nume nu permite accesul la serviciile electronice ale statului.[156,157]

Sancțiuni și rezultat. Presa estoniană a relatat că era puțin probabil ca RIA să fie amendată sau ca victimele să fie despăgubite.[158] Incidentul nu a compromis infrastructura centrală de identitate.

Lecția pentru Republica Moldova. Cazul este aproape identic conceptual: un serviciu legitim, care răspundea la interogări pe baza unui identificator personal, fără control suficient al dreptului solicitantului și fără limitarea volumului. Diferențele sunt de amploare (o categorie de date în Estonia, peste zece categorii în Republica Moldova) și de răspuns: Estonia a notificat individual toate persoanele în câteva zile și a identificat rapid un suspect. Lecția principală este că nici sistemele cele mai mature nu sunt imune la erori de autorizare în servicii periferice, dar că notificarea rapidă și transparentă limitează pierderea încrederii.

6.3. Australia: Optus (2022)

Context și vector. Optus, al doilea operator de telecomunicații din Australia, a suferit în septembrie 2022 o scurgere a datelor a circa 9,5 milioane de clienți actuali și foști (aproximativ 9,8 milioane de înregistrări, potrivit unor relatări).[159,160] O interfață de programare inactivă era accesibilă de pe internet, iar controalele de acces fuseseră anulate de o eroare de cod introdusă în 2018; interfața devenise accesibilă public în 2020.[161] Atacatorul a declarat că a găsit o interfață neprotejată prin autentificare.[162]

Scara. Au fost expuse nume, date de naștere, numere de telefon, adrese de e-mail și, pentru o parte a clienților, numere de pașaport, permise de conducere și numere de asigurare medicală.[163]

Răspuns și sancțiuni. Autoritatea australiană pentru comunicații și media (ACMA) a deschis în mai 2024 o acțiune în instanța federală, susținând că Optus nu a protejat confidențialitatea datelor și că eroarea a rămas nedetectată ani la rând.[164] În august 2025, Comisarul australian pentru informații a deschis o a doua acțiune, alegând câte o încălcare pentru fiecare dintre cele

[154] Postimees, „Hacker gains access to hundreds of thousands of document photos", iulie 2021.

[155] The Record, „Estonia says a hacker downloaded 286,000 ID photos from government database", iulie 2021.

[156] Security Affairs, „Estonia's police arrested a Tallin resident who stole 286K ID scans from a government DB", 30 iulie 2021, https://securityaffairs.com/120684/cyber-crime/estonia-s-police-hacker-id-scans.html.

[157] ERR News, „AK: RIA unlikely to be fined over mass photo hack, victims not compensated", 2021, https://news.err.ee/1608294000/ak-ria-unlikely-to-be-fined-over-mass-photo-hack-victims-not-compensated.

[158] ERR News, „AK: RIA unlikely to be fined over mass photo hack, victims not compensated", 2021.

[159] CSO Online, „Optus breach occurred due to a coding error, alleges ACMA", 2024.

[160] BankInfoSecurity, „Australian Telecom Watchdog Sues Optus Over 2022 Data Breach", 2024, https://www.bankinfosecurity.com/australian-telecom-watchdog-sues-optus-over-2022-data-breach-a-25321.

[161] ISMS.online, „As Optus Is Sued, What Went Wrong and What Lessons Can We Learn?", 2025, https://www.isms.online/data-protection/as-optus-is-sued-what-went-wrong-and-what-lessons-can-we-learn/.

[162] CPO Magazine, „Optus Sued by Australian Privacy Regulator Over 2022 Data Breach", 2025, https://www.cpomagazine.com/data-protection/optus-sued-by-australian-privacy-regulator-over-2022-data-breach/.

[163] BankInfoSecurity, „Australian Telecom Watchdog Sues Optus Over 2022 Data Breach", 2024.

[164] CSO Online, „Optus breach occurred due to a coding error, alleges ACMA", 2024.

circa 9,5 milioane de persoane; pedeapsa maximă teoretică este de 2,22 milioane de dolari australieni pentru fiecare încălcare, iar suma efectivă rămâne la aprecierea instanței.[165] Optus a fost, în general, considerat cooperant.[166]

Reforme. La sfârșitul anului 2022, după incident, Australia a majorat plafonul amenzilor pentru încălcări grave ale vieții private la 50 de milioane de dolari australieni per încălcare; noul plafon nu se aplică retroactiv cazului Optus.[167]

Lecția. Optus arată că o singură interfață uitată, fără autentificare, poate expune o treime din populația unui stat. Lecția directă pentru Republica Moldova este nevoia unui inventar complet al interfețelor expuse (categoria OWASP „gestionarea inadecvată a inventarului") și a testării lor periodice. Lecția indirectă privește durata consecințelor juridice: la patru ani după incident, procesele erau încă în desfășurare.

6.4. Bulgaria: Agenția Națională a Veniturilor (2019)

Context și scară. În iulie 2019, datele personale ale circa 6 milioane de persoane — majoritatea populației Bulgariei —, deținute de Agenția Națională a Veniturilor (NRA), au fost accesate și diseminate ilegal.[168]

Sancțiuni. Comisia bulgară pentru protecția datelor (CPDP) a aplicat NRA, în august 2019, o amendă de 5,1 milioane de leva (aproximativ 2,55 milioane de euro) pentru neaplicarea unor măsuri tehnice și organizatorice adecvate. Este cea mai mare amendă aplicată vreodată în Bulgaria în baza GDPR și confirmă că legea bulgară permite amendarea autorităților publice.[169] NRA a contestat decizia, iar instanța administrativă a închis definitiv cazul ca urmare a împlinirii termenului absolut de prescripție.[170]

Jurisprudență. Persoanele afectate au cerut despăgubiri statului. Curtea Supremă Administrativă a Bulgariei a sesizat Curtea de Justiție a UE, care a stabilit în decembrie 2023 (cauza C-340/21) că accesul neautorizat al unui terț nu dovedește, prin el însuși, caracterul inadecvat al măsurilor, dar că operatorul poartă sarcina probei, iar teama de utilizare abuzivă poate constitui prejudiciu moral.[171,172]

Lecția. Cazul NRA este important pentru Republica Moldova din trei motive. Arată că o autoritate de supraveghere poate amenda o agenție fiscală de stat; arată și limitele procedurale ale acestei căi (prescripția a anulat efectul practic al amenzii); și, mai ales, a produs o jurisprudență care va fi relevantă pentru instanțele moldovenești în interpretarea Legii nr. 195/2024 în acțiunile în despăgubire.

[165] TechPartner News, „OAIC takes Optus to court over 2022 data breach", 8 august 2025, https://www.techpartner.news/news/oaic-takes-optus-to-court-over-2022-data-breach-619433.

[166] CPO Magazine, „Optus Sued by Australian Privacy Regulator Over 2022 Data Breach", 2025.

[167] CPO Magazine, „Optus Sued by Australian Privacy Regulator Over 2022 Data Breach", 2025.

[168] CMS, GDPR Enforcement Tracker Report – Bulgaria, 21 mai 2026, https://cms.law/en/bgr/publication/gdpr-enforcement-tracker-report/bulgaria.

[169] CMS, GDPR Enforcement Tracker Report – Bulgaria, 21 mai 2026.

[170] CMS, GDPR Enforcement Tracker Report – Bulgaria, 21 mai 2026.

[171] Curtea de Justiție a Uniunii Europene, Hotărârea din 14 decembrie 2023, cauza C-340/21, VB împotriva Natsionalna agentsia za prihodite.

[172] CMS, GDPR Enforcement Tracker Report – Bulgaria, 21 mai 2026.

6.5. Singapore: SingHealth (2018)

Context și vector. Între 27 iunie și 4 iulie 2018, atacatorii au extras datele personale a 1,5 milioane de pacienți ai SingHealth, cel mai mare grup de instituții medicale din Singapore, precum și evidența medicamentelor eliberate în ambulatoriu pentru 160.000 de pacienți, inclusiv ale prim-ministrului.[173,174] Comisia de anchetă a descris atacul ca fiind opera unui actor sofisticat, de tip amenințare persistentă avansată.[175]

Răspuns. SingHealth a depus plângere la poliție pe 12 iulie; incidentul a fost anunțat public pe 20 iulie printr-o declarație comună a Ministerului Sănătății și a Ministerului Comunicațiilor, iar din aceeași zi au început notificările individuale ale pacienților.[176]

Ancheta independentă. Guvernul a instituit un Comitet de Anchetă (Committee of Inquiry), care a publicat la 10 ianuarie 2019 un raport public de 454 de pagini, cu constatări și recomandări; toate recomandările au fost acceptate.[177,178] Raportul a constatat, printre altele, că personalul nu era suficient instruit în securitate cibernetică.

Sancțiuni. Comisia pentru protecția datelor personale (PDPC) a aplicat amenzi de 750.000 de dolari singaporezi furnizorului IT al sectorului medical public (IHiS) și de 250.000 de dolari singaporezi SingHealth, ca proprietar al sistemului — cele mai mari amenzi aplicate până atunci.[179,180] PDPC a ținut cont de cooperarea celor două entități și de măsurile de remediere imediate.[181] Mai mulți angajați IHiS au fost sancționați disciplinar.

Lecția. Modelul singaporez — comisie de anchetă independentă, cu mandat clar, termen și raport public — este transferabil direct. El separă stabilirea faptelor de răspunderea politică și oferă publicului o versiune unică și verificabilă a evenimentelor. Totodată, cazul arată că pot fi amendate atât instituția care deține datele, cât și furnizorul tehnic, ceea ce este relevant pentru relația AGE–STISC–deținătorii registrelor.

6.6. Albania: atacul asupra serviciilor guvernamentale (2022)

Context și vector. La 15 iulie 2022, sistemele guvernamentale ale Albaniei, inclusiv portalul de servicii e-Albania, au fost ținta unui atac distructiv. Echipa de răspuns la incidente a Microsoft a evaluat cu încredere ridicată că atacul a fost comis de actori sponsorizați de guvernul iranian.[182] Analizele publice arată că atacatorii obținuseră acces cu mult înainte și exfiltraseră date între octombrie 2021 și ianuarie 2022, înainte de faza de ransomware și ștergere a datelor; datele au fost ulterior publicate de grupul „Homeland Justice”.[183]

---

[173] Computer Weekly, „SingHealth and IT supplier fined S$1m for data breach”, ianuarie 2019, https://www.computerweekly.com/news/252455861/SingHealth-and-IT-supplier-fined-S1m-for-data-breach.

[174] Wiki.sg, „SingHealth data breach (2018)”.

[175] Committee of Inquiry into the Cyber Attack on SingHealth Patient Database System, Public Report, Singapore, 10 ianuarie 2019.

[176] Wiki.sg, „SingHealth data breach (2018)”.

[177] Wiki.sg, „SingHealth data breach (2018)”.

[178] Society for Computers & Law, „Singapore's worst cyber attack: the outcome of the investigation”, 2019, https://www.scl.org/10405-singapore-s-worst-cyber-attack-the-outcome-of-the-investigation/.

[179] Computer Weekly, „SingHealth and IT supplier fined S$1m for data breach”, ianuarie 2019.

[180] Society for Computers & Law, „Singapore's worst cyber attack: the outcome of the investigation”, 2019.

[181] Computer Weekly, „SingHealth and IT supplier fined S$1m for data breach”, ianuarie 2019.

[182] Cyber Security Hub, „Albania hit with cyber attack after severing ties with Iran”, septembrie 2022, https://cshub.com/attacks/news/iotw-albania-hit-with-cyber-attack-after-severing-ties-with-iran.

[183] SOCRadar, „Diplomatic Crisis: Cyber Attack from Iran to Albania”, 19 septembrie 2022, https://socradar.io/diplomatic-crisis-cyber-attack-from-iran-to-albania/.

Răspuns. Albania a rupt relațiile diplomatice cu Iranul în septembrie 2022 — primul caz cunoscut de rupere a relațiilor diplomatice din cauza unui atac cibernetic. Statele Unite au impus sancțiuni Ministerului iranian al Informațiilor, iar NATO și Uniunea Europeană au condamnat atacul.[184] Statele Unite, NATO și Regatul Unit au atribuit formal atacul guvernului iranian; Iranul a negat.[185] Un al doilea atac, în septembrie, a vizat sistemul de evidență a trecerii frontierei, care a fost scos temporar din funcțiune.[186]

Lecția. Albania arată cum poate fi construită o atribuire credibilă: probe tehnice, analize independente (inclusiv ale unor companii private) și confirmarea aliaților, urmate de măsuri politice proporționale. Pentru Republica Moldova, cazul sugerează că atribuirea către un actor statal trebuie susținută de probe prezentate cel puțin partenerilor și, în măsura posibilului, publicului, pentru a avea efect diplomatic și pentru a nu fi percepută ca o explicație politică a unui eșec tehnic.

6.7. Franța: France Travail (2024)

Context și vector. Între 6 februarie și 5 martie 2024, atacatori au accesat sistemele agenției publice franceze pentru ocuparea forței de muncă, France Travail, obținând datele a până la 43 de milioane de persoane înregistrate în ultimii 20 de ani: nume, date de naștere, numere de securitate socială, adrese de e-mail și poștale, numere de telefon.[187,188] Accesul s-a bazat pe inginerie socială și pe controale interne slabe.

Răspuns și sancțiuni. Agenția a notificat autoritatea franceză de protecție a datelor (CNIL) la 8 martie 2024. La 22 ianuarie 2026, CNIL a aplicat France Travail o amendă de 5 milioane de euro pentru neasigurarea securității datelor (art. 32 GDPR).[189,190] Era a doua mare scurgere în mai puțin de un an: în 2023, un incident la un subcontractor afectase circa 10 milioane de persoane.[191]

Lecția. Cazul arată că și o instituție publică dintr-un stat membru cu tradiție în protecția datelor poate fi amendată semnificativ pentru lipsa măsurilor de securitate. Arată și că ancheta autorității de supraveghere poate dura aproape doi ani; pentru CNPDCP, un calendar realist și comunicarea etapelor sunt importante pentru menținerea încrederii.

6.8. Statele Unite: Office of Personnel Management (2015)

Context și scară. Biroul de Management al Personalului (OPM) din SUA a anunțat în iunie–iulie 2015 două incidente: unul a afectat dosarele de personal a 4,2 milioane de angajați federali, iar al doilea, dosarele de verificare de securitate a 21,5 milioane de persoane — 19,7 milioane de solicitanți și 1,8 milioane de non-solicitanți, în special soți sau parteneri.[192] În total,

[184] Arab News (AP), „Albania reports 2nd cyberattack by Iran, on border systems”, 10 septembrie 2022, https://arabnews.pk/node/2159936.

[185] Security Affairs, „Albania was hit by a new cyberattack and blames Iran”, 11 septembrie 2022, https://securityaffairs.com/?p=135602.

[186] Arab News (AP), „Albania reports 2nd cyberattack by Iran, on border systems”, 10 septembrie 2022.

[187] Security Affairs, „France Travail data breach impacted 43 Million people”, 16 martie 2024, https://securityaffairs.com/160556/data-breach/france-travail-data-breach-34m-people.html.

[188] BleepingComputer, „France fines unemployment agency €5 million over data breach”, ianuarie 2026, https://www.bleepingcomputer.com/news/security/france-fines-unemployment-agency-5-million-over-data-breach/.

[189] CNIL, „Data breach: 5 million euro fine for France Travail”, 22 ianuarie 2026, https://www.cnil.fr/en/data-breach-5million-fine-france-travail.

[190] BleepingComputer, „France fines unemployment agency €5 million over data breach”, ianuarie 2026.

[191] BleepingComputer, „France fines unemployment agency €5 million over data breach”, ianuarie 2026.

circa 22,1 milioane de persoane unice au fost afectate.[193] Au fost furate și amprentele a 5,6 milioane de persoane, cifră revizuită de la 1,1 milioane estimate inițial.[194]

Răspuns. Directoarea OPM a demisionat la 10 iulie 2015, la o zi după anunțarea amplorii incidentului; directoarea pentru tehnologia informației a demisionat ulterior.[195,196] Persoanelor afectate li s-au oferit servicii de monitorizare a creditului și asigurare împotriva pierderilor cauzate de furtul de identitate.[197] Raportul Comisiei pentru supraveghere a Camerei Reprezentanților (2016) a constatat că OPM ignorase ani la rând avertismentele privind vulnerabilitățile și a recomandat, printre altele, trecerea la modelul „încredere zero" și întărirea rolului directorilor pentru tehnologia informației.[198,199] Raportul a sugerat că atacatorii erau actori statali, iar suspiciunile publice au vizat China, fără o atribuire formală publică.

Lecția. OPM este cazul de referință pentru riscul de contrainformații: datele despre persoane cu acces la informații secrete, familiile și vulnerabilitățile lor au o valoare de lungă durată pentru serviciile de informații străine. Lecțiile pentru Republica Moldova sunt două: evaluarea specifică a riscului pentru categoriile sensibile (funcționari cu acces la informații secrete, militari, polițiști, magistrați) și oferirea de servicii de monitorizare pentru persoanele afectate.

6.9. Tabel comparativ

Tabelul 6. Sinteza cazurilor internaționale comparate

Caz	An	Persoane afectate	Vector principal	Detectare	Notificare individuală	Sancțiune / consecință	Reformă
Estonia – RIA	2021	286.438	Interogări la un serviciu cu validare insuficientă	9 zile; semnal extern	Da, prin e-mail	Suspect arestat; fără amendă	Revizuirea serviciilor similare
Australia – Optus	2022	~9,5 mil.	Interfață expusă, fără autentificare	Ani (eroare din 2018)	Da	Două acțiuni în instanță (ACMA, OAIC)	Plafon de amendă majorat
Bulgaria – NRA	2019	~6 mil.	Acces neautorizat la sisteme fiscale	Date indisponibile	Date indisponibile	Amendă 5,1 mil. leva; anulată prin prescripție	Jurisprudența CJUE C-340/21
Singapore – SingHealth	2018	1,5 mil.	Actor statal sofisticat (APT)	~1 săptămână (faza de extragere)	Da, din ziua anunțului	Amenzi 1 mil. SGD; sancțiuni disciplinare	Comisie de anchetă; recomandări acceptate integral

[192]Threatpost, „OPM Hack Expands to Include Data of 21.5 Million People; Director Archuleta Resigns", iulie 2015, https://threatpost.com/opm-hack-expands-to-include-data-of-21-5-million-people/113717.

[193]Washington Examiner, „Government hacks hit 22.1 million", iulie 2015, https://www.washingtonexaminer.com/politics/2004691/government-hacks-hit-22-1-million/.

[194]iTnews, „US OPM CIO quits", 2016, https://www.itnews.com.au/news/us-opm-cio-quits-415496.

[195]Threatpost, „OPM Hack Expands to Include Data of 21.5 Million People; Director Archuleta Resigns", iulie 2015.

[196]iTnews, „US OPM CIO quits", 2016.

[197]Washington Examiner, „Government hacks hit 22.1 million", iulie 2015.

[198]U.S. House of Representatives, Committee on Oversight and Government Reform, The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation, raport al majorității, septembrie 2016.

[199]Biometric Update, „House oversight committee OPM breach report calls for zero trust model, empowered CIOs", septembrie 2016, https://www.biometricupdate.com/201609/house-oversight-committee-opm-breach-report-calls-for-zero-trust-model-empowered-cios.

Caz	An	Persoane afectate	Vector principal	Detectare	Notificare individuală	Sancțiune / consecință	Reformă
Albania	2022	Date indisponibile	Actor statal; acces îndelungat, apoi distrugere	Luni	Date indisponibile	Ruperea relațiilor diplomatice; sancțiuni aliate	Cooperare consolidată cu aliații
Franța – France Travail	2024	până la 43 mil.	Inginerie socială, controale interne slabe	~1 lună	Da	Amendă CNIL 5 mil. euro	Măsuri corective dispuse de CNIL
SUA – OPM	2015	22,1 mil.	Actor statal; intruziune îndelungată	Peste 1 an	Da, cu monitorizare	Demisii; raport parlamentar	Zero Trust; rol consolidat pentru directorii IT
Republica Moldova – AGE	**2026**	**~750.000 IDNP (preliminar)**	**Servicii fără autentificare; extragere automată**	**~4 zile; semnal de la cetățeni**	**Nu, la 3 nov. 2026 (în pregătire)**	**Demisia conducerii; dosar penal; investigație CNPDCP**	**În curs**

Sursele sunt citate în secțiunile 6.2–6.8 și în capitolul 4.

6.10. Lecții transferabile, scalate la Republica Moldova

Cazurile comparate converg către opt lecții. Ele sunt adaptate la dimensiunea și resursele Republicii Moldova — un stat mic, cu buget limitat, dar cu o arhitectură digitală centralizată, ceea ce face ca unele măsuri să fie mai ușor de aplicat decât în state mari.

1. **Interfețele periferice sunt punctul slab** (Estonia, Optus). Nu sistemele centrale, ci serviciile auxiliare, uitate sau insuficient testate, au cedat. Republica Moldova are avantajul unei platforme centrale (MConnect) prin care pot fi impuse reguli comune tuturor serviciilor.
2. **Detectarea trebuie să fie comportamentală** (Estonia, OPM). Volumul total poate părea normal; anomalia este numărul de persoane distincte interogate de același solicitant. O regulă simplă de acest tip ar fi semnalat incidentul AGE în primele ore.
3. **Notificarea individuală rapidă protejează încrederea** (Estonia, Singapore). Ambele state au notificat persoanele în câteva zile. Republica Moldova are canalul EVO, ceea ce face notificarea tehnic accesibilă.
4. **Ancheta independentă și publică separă faptele de politică** (Singapore, OPM). O comisie cu mandat de 60–90 de zile și raport public este fezabilă și la scara Republicii Moldova, cu sprijin tehnic din partea partenerilor.
5. **Instituțiile publice pot și trebuie să răspundă** (Bulgaria, Franța, Singapore). Răspunderea instituțională nu are ca scop principal amenda, ci măsurile corective și precedentul.
6. **Termenele procedurale contează** (Bulgaria). CNPDCP trebuie să conducă investigația astfel încât să nu fie compromisă de prescripție.
7. **Atribuirea credibilă cere probe și aliați** (Albania). Declarațiile politice fără probe pot fi contraproductive.
8. **Categoriile sensibile cer o evaluare separată** (OPM). Persoanele cu funcții de securitate trebuie identificate și protejate specific.

7. Capacitatea instituțională și benchmarking

7.1. Poziția Republicii Moldova în clasamentele internaționale

Global Cybersecurity Index (ITU, 2024). Ediția a cincea a indicelui ITU, publicată în septembrie 2024, a evaluat angajamentele statelor pe cinci piloni: juridic, tehnic, organizațional, dezvoltarea capacităților și cooperare.[200] Ediția 2024 a introdus un sistem pe cinci niveluri, de la nivelul 1 („model de urmat", 95–100 de puncte) la nivelul 5 („în construcție", 0–20 de puncte). Republica Moldova este încadrată la nivelul 3 („în consolidare", 55–85 de puncte), cu un scor de 65,25.[201,202] Pentru comparație, 46 de state au fost plasate la nivelul 1.[203]

National Cyber Security Index (e-Governance Academy). În NCSI, Republica Moldova ocupă locul 6 în lume, cu un grad de îndeplinire de 94,17%, pe baza datelor actualizate la 29 ianuarie 2026.[204] În 2026, presa a relatat clasarea pe locul 5, înaintea unor state cu tradiție îndelungată în domeniu.[205] Același profil indică locul 70 în Indicele de dezvoltare a guvernării electronice al ONU și locul 70 în Network Readiness Index.[206]

eGovernment Benchmark (Comisia Europeană). Ediția 2025, publicată în 2026, evaluează serviciile publice digitale din statele membre și din mai multe state candidate pe patru dimensiuni: orientarea spre utilizator, transparența, facilitatorii-cheie (identitate electronică, documente electronice, surse autentice de date) și serviciile transfrontaliere.[207] Nu am putut confirma, pe baza surselor publice consultate, includerea Republicii Moldova în ediția 2025, astfel că pentru acest indice **datele sunt indisponibile**. Dimensiunea „facilitatori-cheie" este însă relevantă conceptual: ea recompensează reutilizarea surselor autentice de date — exact mecanismul care, neprotejat, a devenit vector de atac în cazul AGE.

7.2. Paradoxul clasamentelor

Cum poate un stat clasat pe locul 6 în lume într-un indice de securitate cibernetică să sufere cea mai mare scurgere de date din istoria sa? Răspunsul ține de ceea ce măsoară indicii.

NCSI evaluează existența unor capacități documentate: legislație, instituții, strategii, echipe de răspuns, exerciții, cooperare internațională. Dovezile sunt furnizate în principal de oficialii guvernamentali și verificate documentar.[208] Republica Moldova a construit rapid, între 2023 și 2025, exact aceste elemente: Legea nr. 48/2023, ASC, Consiliul de coordonare, Programul

[200] Uniunea Internațională a Telecomunicațiilor (ITU), Global Cybersecurity Index 2024, ediția a 5-a, 2024, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf.

[201] e-Governance Academy, National Cyber Security Index, profilul Republicii Moldova (ultima actualizare a datelor: 29.01.2026).

[202] Internet Society Pulse, profilul Republicii Moldova, https://pulse.internetsociety.org/en/reports/md.

[203] Uniunea Internațională a Telecomunicațiilor (ITU), Global Cybersecurity Index 2024, ediția a 5-a, 2024.

[204] e-Governance Academy, National Cyber Security Index, profilul Republicii Moldova (ultima actualizare a datelor: 29.01.2026).

[205] Logos Press, „How Moldova Managed to Rank Fifth in the World in Cybersecurity", 2026.

[206] e-Governance Academy, National Cyber Security Index, profilul Republicii Moldova (ultima actualizare a datelor: 29.01.2026).

[207] Comisia Europeană (Capgemini și parteneri), eGovernment Benchmark 2025, publicat în 2026, https://www.capgemini.com/insights/research-library/results-of-the-egov-benchmark/.

[208] e-Governance Academy, National Cyber Security Index, profilul Republicii Moldova (ultima actualizare a datelor: 29.01.2026).

2026–2030, planul de gestionare a crizelor, cadrul de divulgare coordonată a vulnerabilităților. Clasarea reflectă corect acest efort normativ și instituțional.

Ceea ce indicii nu măsoară este eficacitatea operațională: dacă fiecare serviciu public are autentificare și autorizare corecte, dacă monitorizarea detectează un comportament anormal, dacă cerințele legale sunt aplicate în fiecare instituție. GCI, care cuprinde mai mulți indicatori de implementare, plasează Republica Moldova la un nivel intermediar, mai apropiat de realitatea dezvăluită de incident.

Concluzia nu este că indicii sunt greșiți, ci că ei descriu pregătirea formală. Incidentul AGE arată decalajul dintre arhitectura normativă (avansată) și igiena tehnică de bază a serviciilor (insuficientă). Aceeași lecție o oferă Estonia, aflată constant în fruntea clasamentelor și totuși vulnerabilă în 2021 printr-un serviciu periferic.[209]

7.3. Maturitatea față de NIS2

Tabelul 7 prezintă o evaluare calitativă a maturității Republicii Moldova față de principalele cerințe ale NIS2, distingând între adoptarea normativă și implementarea demonstrată.

Tabelul 7. Maturitatea față de cerințele NIS2 (evaluare calitativă a autorului)

Cerință NIS2	Instrument național	Adoptare normativă	Implementare demonstrată public
Strategie națională (art. 7)	Programul 2026–2030 (HG nr. 821/2025)	Ridicată	În curs
Autoritate competentă și punct unic de contact (art. 8)	ASC (HG nr. 1028/2023)	Ridicată	Medie
Echipe de răspuns la incidente (art. 10–11)	ASC; STISC pentru sectorul guvernamental	Ridicată	Medie
Gestionarea crizelor cibernetice (art. 9)	HG nr. 823/2025	Ridicată	Testată în octombrie 2026; rezultat mixt
Divulgarea coordonată a vulnerabilităților (art. 12)	HG nr. 824/2025	Ridicată	Scăzută (fără program public de raportare)
Răspunderea organelor de conducere (art. 20)	Neclar	Scăzută	Scăzută
Măsuri de gestionare a riscurilor (art. 21)	Legea nr. 48/2023, HG nr. 562/2025	Medie–ridicată	Scăzută (prima evaluare nescadentă)
Raportarea incidentelor (art. 23)	Legea nr. 48/2023	Medie	Neverificabilă public
Supraveghere și sancțiuni (art. 31–36)	Legea nr. 48/2023	Medie	Scăzută
Administrația publică centrală inclusă în domeniu	Legea nr. 48/2023, HG nr. 860/2024	Neclară	Neclară

7.4. Capacitatea umană și financiară

Nu am identificat date publice consolidate privind numărul de specialiști în securitate cibernetică din AGE, STISC, ASC și CNPDCP, nici privind bugetele alocate securității serviciilor publice digitale. Pentru acest aspect, **datele sunt indisponibile**. Lipsa transparenței nu este, în sine, o problemă de securitate — anumite detalii operaționale trebuie protejate —,

[209] The Record, „Estonia says a hacker downloaded 286,000 ID photos from government database", iulie 2021.

dar indicatori agregați (număr de posturi, posturi vacante, buget anual pentru securitate, număr de teste de penetrare efectuate) ar permite Parlamentului și publicului să evalueze dacă resursele corespund ambițiilor.

Indicii disponibili sugerează constrângeri. Instituțiile publice din domeniul tehnologiei concurează pentru specialiști cu un sector IT privat dinamic și cu piața muncii din UE. Conducerea AGE a indicat un volum de circa 40 de incidente gestionate în aproape doi ani,[210] ceea ce arată existența unei capacități de răspuns, dar nu și a unei funcții dedicate de detectare 24/7 pentru stratul de servicii.

[210] Unimedia, interviu cu Nicoleta Colomeeț, directoarea AGE, 31 octombrie 2026.

8. Discuție

8.1. Ce spune incidentul despre capacitatea statului

Incidentul AGE nu dezvăluie absența capacităților, ci un decalaj între straturi. Stratul strategic și normativ este avansat: Republica Moldova are o lege a protecției datelor aliniată la GDPR, o lege a securității cibernetice inspirată de NIS2, o agenție de securitate cibernetică, un program național și a ratificat Convenția 108+. Stratul de răspuns la criză a funcționat: izolarea a fost rapidă, instituțiile au comunicat comun, au fost luate decizii prudente (inclusiv privind alegerile). Stratul care a cedat este cel al ingineriei de securitate a serviciilor — autentificare, autorizare, minimizare, limitarea ratei de cereri, monitorizare — și al guvernanței care ar fi trebuit să garanteze aceste elemente înaintea lansării fiecărui serviciu.

Acest tip de decalaj este frecvent în statele care au digitalizat rapid. Prioritatea politică a fost, legitim, să ofere cât mai multe servicii online, cât mai simplu. Securitatea a fost tratată adesea ca o proprietate a infrastructurii (rețea, centre de date), nu a fiecărei funcționalități. Cazurile Optus și Estonia arată că aceeași eroare apare și în organizații cu resurse mult mai mari.

8.2. Argumentele autorităților

O evaluare echilibrată trebuie să consemneze argumentele instituțiilor implicate.

- **Răspunsul a fost rapid odată ce incidentul a fost cunoscut.** Extragerea a fost oprită în minute, iar sute de servicii și sisteme au fost verificate în câteva zile.[211,212]
- **Transparența sistemului a permis detectarea.** Jurnalul de accesări din EVO, construit tocmai pentru a da cetățenilor control asupra datelor lor, a funcționat ca mecanism de alertă.[213]
- **Mediul de amenințare este excepțional.** Republica Moldova se confruntă cu operațiuni hibride documentate, iar instrumentele de inteligență artificială accelerează descoperirea vulnerabilităților.[214,215] În 2026, după cum a remarcat un expert citat de presă, nicio bază de date nu este complet sigură.[216]
- **Registrele nu au fost alterate și datele bancare nu au fost compromise.**[217] Un atac asupra integrității registrelor ar fi avut consecințe mult mai grave.

[211]Agenția de Guvernare Electronică (AGE), comunicat privind estimările preliminare ale incidentului cibernetic din 19–23 octombrie 2026, 27 octombrie 2026.

[212]Unimedia, interviu cu Nicoleta Colomeeț, directoarea AGE, 31 octombrie 2026.

[213]NewsMaker, „(GHID) Ce faci dacă datele tale personale au ajuns la hackeri. Ce drepturi ai și când poți cere despăgubiri”, octombrie 2026.

[214]Digi24, „Consiliul de Securitate al R. Moldova, convocat după un atac cibernetic în care au fost furate datele personale a 750.000 de cetățeni”, 28 octombrie 2026.

[215]Digi24, „Serviciile secrete ale Rusiei colectează datele personale ale moldovenilor, avertizează SIS de la Chișinău”, iunie 2026 comunicatul SIS din 17 iunie 2026.

[216]Radio Moldova, „Datele personale a 750.000 de cetățeni, extrase în urma atacului cibernetic asupra sistemelor guvernamentale”, octombrie 2026.

[217]AGE, comunicat privind restabilirea a 61 de servicii publice digitale, 30 octombrie 2026.

- **Răspunderea a fost asumată.** Conducerea AGE a fost schimbată, a fost pornită urmărirea penală, iar CNPDCP și Parlamentul au deschis proceduri proprii.[218,219,220]
- **Portofoliul este moștenit și eterogen.** Multe servicii au fost dezvoltate în ani diferiți, de prestatori diferiți, iar AGE gestionează doar o parte dintre ele.[221]

Aceste argumente sunt, în mare parte, întemeiate. Ele nu schimbă însă două constatări: existența, în 2026, a unor servicii care returnau date personale fără autentificare reprezintă o deficiență de bază, nu un atac sofisticat; iar detectarea de către cetățeni, nu de către sisteme, indică o lacună de monitorizare.

8.3. Răspunderea: persoane sau sistem?

Schimbarea conducerii AGE a fost un semnal politic de asumare a răspunderii. Experiența OPM arată că astfel de demisii sunt frecvente după incidente majore.[222] Ea mai arată însă că, fără o anchetă care să identifice cauzele sistemice, demisiile pot crea impresia că problema a fost rezolvată prin schimbarea unor persoane. Vulnerabilitățile identificate în acest studiu — lipsa testelor obligatorii înainte de lansare, neclaritatea rolurilor, monitorizarea insuficientă — sunt sistemice și depășesc mandatul unei singure conduceri.

Tot aici se plasează întrebarea despre transparența procedurilor. Audierile parlamentare cu ușile închise sunt justificabile pentru detaliile tehnice care ar putea ajuta atacatorii. Însă un rezumat public al constatărilor, după modelul raportului public al comisiei de anchetă din Singapore,[223] ar consolida încrederea și ar face posibilă supravegherea publică a remedierilor.

8.4. Atribuirea și riscul politizării

Declarațiile privind implicarea unor actori statali străini sunt plauzibile în contextul avertismentelor SIS din iunie 2026.[224] Totuși, în absența unor probe prezentate public, ele riscă două efecte nedorite. Pot fi percepute ca o explicație care mută atenția de la deficiențele tehnice. Și pot fi contestate de actori politici interni, transformând un incident de securitate într-un subiect de polarizare. Cazul Albaniei arată că atribuirea are greutate atunci când este susținută de analize tehnice și confirmată de aliați.[225,226] Recomandarea studiului este separarea clară, în comunicare, între ceea ce se știe tehnic (cum s-a produs incidentul) și ceea ce se evaluează strategic (cine ar putea fi în spate).

8.5. Digitalizare și securitate: o falsă dilemă

Incidentul nu trebuie citit ca un argument împotriva digitalizării. Ghișeele fizice și arhivele pe hârtie au propriile vulnerabilități — corupție, pierderea dosarelor, acces neautorizat greu de urmărit. Avantajul sistemelor digitale este că fiecare acces poate fi jurnalizat, controlat și

[218]TVR Moldova, „Cine răspunde pentru furtul de date ale moldovenilor? Procuratura a pornit o urmărire penală”, 30 octombrie 2026.

[219]Timpul.md, „CNPDCP investighează extragerea neautorizată a datelor asociate cu aproximativ 750.000 de IDNP-uri”, 31 octombrie 2026.

[220]Realitatea.md, „Cine răspunde pentru scurgerea datelor a sute de mii de moldoveni? Igor Grosu: Vor fi organizate audieri”, octombrie 2026.

[221]Unimedia, interviu cu Nicoleta Colomeeț, directoarea AGE, 31 octombrie 2026.

[222]Threatpost, „OPM Hack Expands to Include Data of 21.5 Million People; Director Archuleta Resigns”, iulie 2015.

[223]Society for Computers & Law, „Singapore's worst cyber attack: the outcome of the investigation”, 2019.

[224]Digi24, „Serviciile secrete ale Rusiei colectează datele personale ale moldovenilor, avertizează SIS de la Chișinău”, iunie 2026 comunicatul SIS din 17 iunie 2026.

[225]Cyber Security Hub, „Albania hit with cyber attack after severing ties with Iran”, septembrie 2022.

[226]Security Affairs, „Albania was hit by a new cyberattack and blames Iran”, 11 septembrie 2022.

auditat; incidentul a fost descoperit tocmai datorită acestui lucru. Dilema reală nu este „digital sau nu”, ci „digital cu ce garanții”. Principiul „o singură dată” trebuie însoțit de principiul „doar cine are dreptul, doar cât e necesar, doar cu urmă verificabilă”.

8.6. Lentila aderării la UE

Pentru negocierile de aderare, incidentul este simultan un risc și o oportunitate. Riscul este ca evaluatorii să constate un decalaj între legislație și aplicare în domeniile protecției datelor și securității cibernetice. Oportunitatea este ca Republica Moldova să demonstreze, pe un caz real, funcționarea instituțiilor nou create: o investigație CNPDCP independentă și finalizată în termen, măsuri corective verificabile, notificarea persoanelor afectate și remedieri tehnice auditate extern. Comisia Europeană a apreciat, în raportul privind extinderea din 2025, progresul Republicii Moldova tocmai prin prisma implementării efective, nu doar a adoptării normelor.[227]

[227] Moldpres, „Moldova - leader among EU expansion candidate states”, noiembrie 2025.

9. Recomandări

9.1. Principii

Recomandările urmează cinci principii. **Întâi persoanele afectate:** măsurile care reduc prejudiciul imediat au prioritate. **Nicio revenire fără verificare:** niciun serviciu care atinge date personale nu ar trebui repus în funcțiune fără controale minime verificate independent. **Sistem, nu persoane:** remedierile vizează cauzele structurale. **Transparență proporțională:** detaliile tehnice sensibile se protejează, constatările și remedierile se publică. **Realism bugetar:** sunt preferate măsurile cu cost redus și efect mare, iar investițiile majore sunt eșalonate.

Costurile sunt exprimate ca ordin de mărime estimat de autor, pe baza unor proiecte comparabile, și trebuie rafinate prin calcule bugetare: **S** – scăzut (sub 1 milion de lei), **M** – mediu (1–10 milioane de lei), **R** – ridicat (10–50 de milioane de lei), **FR** – foarte ridicat (peste 50 de milioane de lei). Prioritatea este notată P1 (urgentă), P2 (importantă) și P3 (structurală, pe termen lung).

9.2. Orizontul 0–3 luni: limitarea prejudiciului și stabilizarea

Sprijin pentru persoanele afectate

Notificarea individuală (A1). Fiecare persoană al cărei IDNP a fost folosit în extragere trebuie informată individual, cu indicarea categoriilor de date expuse în cazul său și a pașilor de protecție. Notificarea poate fi făcută în etape: un prim mesaj prin EVO, SMS sau e-mail tuturor celor potențial afectați, în cel mult 30 de zile, urmat de detalii personalizate. Pentru persoanele fără canal digital — în special vârstnicii — sunt necesare scrisori sau informare prin primării, oficii poștale și casele teritoriale de asigurări sociale.

Instrumentul de verificare (A2). Un serviciu online, accesibil după autentificare, prin care orice persoană poate verifica dacă datele sale au fost extrase și ce categorii au fost afectate, completat de istoricul accesărilor din EVO.

Linia de asistență (A3). O linie telefonică gratuită, cu operatori instruiți, cu scenarii specifice pentru persoanele vârstnice și cu dizabilități, conectată direct la Poliție pentru semnalarea tentativelor de fraudă.

Coaliția anti-fraudă (A7). Banca Națională a Moldovei, Comisia Națională a Pieței Financiare, băncile, organizațiile de creditare nebancară, operatorii de telefonie și Poliția ar trebui să convină, sub coordonarea Guvernului, asupra unor măsuri comune: verificări suplimentare pentru operațiuni neobișnuite, alerte către clienți, schimb rapid de informații privind numerele de telefon folosite în fraude.

Blocarea voluntară a creditării pe IDNP (A8). Persoanele afectate ar trebui să poată cere, gratuit și simplu, blocarea contractării de credite pe numele lor până la deblocarea voluntară. Pe termen scurt, mecanismul poate fi implementat prin birourile istoriilor de credit și prin obligația creditorilor de a le consulta; pe termen mediu, el trebuie consacrat prin lege, cu supravegherea BNM și CNPF.

Măsuri tehnice

Poarta de securitate pentru repunerea serviciilor (A4). Niciun serviciu care returnează date personale nu revine online fără cinci condiții verificate independent: (a) autentificare obligatorie a solicitantului; (b) verificarea, la fiecare cerere, a dreptului solicitantului asupra datelor persoanei vizate (autorizare la nivel de obiect); (c) returnarea doar a câmpurilor necesare

scopului; (d) limitarea ratei de cereri pe solicitant și pe persoană vizată; (e) un test de securitate independent, cu raport remis ASC.

Inventarul interfețelor (A5). Un inventar complet al tuturor serviciilor și interfețelor care expun date personale, inclusiv ale celorlalți prestatori conectați la MConnect, cu responsabil desemnat pentru fiecare.

Detectarea comportamentală (A6). Reguli de monitorizare care semnalează nu doar volumul total, ci comportamentele atipice: numărul de persoane distincte interogate de același solicitant, interogări în afara programului obișnuit al unui serviciu, combinații neobișnuite de servicii pentru aceeași persoană.

Guvernanță și anchetă

Comisia independentă de anchetă (A9). O comisie formată din experți naționali independenți și experți ai partenerilor internaționali, cu mandat de 90 de zile, acces deplin la informații și obligația de a publica un raport public (cu o anexă clasificată pentru detaliile sensibile). Modelul este cel al comisiei de anchetă din Singapore.[228]

Investigația CNPDCP (A10). Finalizarea investigației în cel mult șase luni, cu decizie publică privind respectarea obligațiilor de securitate (art. 32), de notificare (art. 33–34) și de evaluare a impactului (art. 35), precum și cu măsuri corective. Calendarul trebuie gestionat astfel încât procedura să nu fie compromisă de termene de prescripție, lecție a cazului bulgar.[229]

Evaluarea categoriilor sensibile (A12). O evaluare specială, coordonată de SIS, a expunerii persoanelor cu acces la informații secrete și a celor din sistemul de securitate, justiție și apărare, cu măsuri de informare și protecție.

Comunicare de criză

Comunicarea unificată (A11). O pagină unică de informare, actualizată săptămânal, cu întrebări frecvente, cifre consolidate și termene; un purtător de cuvânt tehnic unic; separarea clară dintre informațiile tehnice confirmate și evaluările strategice privind atribuirea. O campanie anti-fraudă adresată special vârstnicilor, prin televiziune, radio și rețeaua de asistență socială.

Cooperare internațională

Asistența partenerilor (A13). Folosirea mecanismelor Convenției de la Budapesta (rețeaua de contact 24/7, conservarea rapidă a datelor) pentru anchetă și solicitarea de asistență tehnică de la partenerii din UE și NATO, inclusiv expertiza Centrului de Excelență NATO de la Tallinn.[230,231]

9.3. Orizontul 3–12 luni: remedierea structurală

Testarea obligatorie (B1). O hotărâre de Guvern care obligă testarea de securitate independentă a fiecărui serviciu public electronic înainte de lansare și cel puțin anual după aceea, cu rapoarte remise ASC.

[228] Society for Computers & Law, „Singapore's worst cyber attack: the outcome of the investigation”, 2019.

[229] CMS, GDPR Enforcement Tracker Report – Bulgaria, 21 mai 2026.

[230] Consiliul Europei, Convenția privind criminalitatea informatică (STE nr. 185), Budapesta, 23.11.2001.

[231] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), informații instituționale.

Programul public de raportare a vulnerabilităților (B2). Operaționalizarea cadrului de divulgare coordonată a vulnerabilităților (HG nr. 824/2025),[232] cu un program public, eventual cu recompense, prin care cercetătorii pot raporta legal vulnerabilități în serviciile statului.

Minimizarea datelor în MConnect (B3). Revizuirea fiecărui flux de date din platforma de interoperabilitate, cu definirea unor profiluri de date pe scop: fiecare serviciu primește doar câmpurile strict necesare. CNPDCP avizează metodologia.

Evaluările de impact (B4). Evaluări de impact asupra protecției datelor pentru toate serviciile care prelucrează date la scară largă sau combină date din mai multe registre.

Clarificarea rolurilor (B5). Acorduri publice care stabilesc, pentru fiecare serviciu, operatorul, operatorii asociați și persoanele împuternicite; modificarea corespunzătoare a HG nr. 211/2019 și, la nevoie, a Legii nr. 142/2018.

Centrul guvernamental de operațiuni de securitate (B6). Un centru de monitorizare 24/7, cu jurnalizare centralizată, retenție adecvată și reguli de detectare pentru stratul de servicii, nu doar pentru infrastructură.

Consolidarea CNPDCP (B7). Buget și personal suficient, inclusiv auditori IT, pentru a investiga incidente complexe; garanții de independență financiară, conform Convenției 108+.

Cooperarea ASC–STISC (B8). Un protocol care clarifică rolurile și ierarhia deciziilor în criza cibernetică din sectorul guvernamental.

Răspunderea conducerii (B9). Includerea explicită a administrației publice centrale în regimul Legii nr. 48/2023 și introducerea răspunderii conducătorilor pentru aprobarea și supravegherea măsurilor de securitate, după modelul art. 20 din NIS2.

Exercițiul de criză (B11). Un exercițiu național cu scenariu de exfiltrare de date din servicii publice, cu participarea ASC, STISC, SIS, CNPDCP, Poliției și a sectorului financiar.

Capacitatea umană (B12). Formarea dezvoltatorilor din instituții și de la furnizori în dezvoltarea sigură a serviciilor; clauze contractuale standard de securitate în achizițiile publice IT.

Modificarea Codului penal (B10). Finalizarea proiectului de aliniere a art. 259 la Directiva 2013/40/UE și la Convenția de la Budapesta.[233]

9.4. Orizontul 1–3 ani: reziliență pe termen lung

Arhitectura „încredere zero” (C1). Migrarea graduală a serviciilor publice către o arhitectură în care fiecare cerere este autentificată, autorizată și evaluată contextual.[234]

Separarea identificatorilor (C2). Studiul unei soluții prin care serviciile și registrele folosesc identificatori derivați, specifici fiecărui sector, în locul IDNP-ului, astfel încât cunoașterea IDNP să nu mai fie suficientă pentru a interoga mai multe registre.

[232] Hotărârea Guvernului nr. 824/2025 privind divulgarea coordonată a vulnerabilităților.

[233] Proiect de lege pentru modificarea Codului penal și a Codului contravențional (alinierea la Directiva 2013/40/UE), nota informativă.

[234] NIST, Special Publication 800-207, Zero Trust Architecture, august 2020.

Certificarea EVO (C3). Certificarea de securitate a portofelului guvernamental de identitate digitală, în linie cu cerințele eIDAS 2, ca pregătire pentru interoperabilitatea cu Portofelul european.[235]

Transpunerea completă a NIS2 (C4). Completarea Legii nr. 48/2023 pentru acoperirea integrală a cerințelor NIS2, inclusiv supravegherea și sancțiunile.

Strategia de resurse umane (C5). O grilă de salarizare specială pentru specialiștii în securitate cibernetică din sectorul public, burse și programe de rezerviști cibernetici, în cooperare cu universitățile.

Raportul anual public (C6). Un raport anual comun ASC–CNPDCP privind starea securității serviciilor publice digitale, cu indicatori agregați.

Mecanism de reparare a prejudiciului (C7). Evaluarea unui mecanism extrajudiciar, simplificat, de compensare a prejudiciilor dovedite cauzate de incidente în sistemele statului, care să reducă presiunea asupra instanțelor, ținând seama de jurisprudența CJUE privind prejudiciul moral.[236]

9.5. Tabelul de implementare

Tabelul 8. Planul de implementare a recomandărilor

Cod	Acțiune	Responsabil	Termen	Cost	Indicator de rezultat	Prioritate
A1	Notificarea individuală a persoanelor afectate	AGE, deținătorii registrelor	30 de zile	M	100% din persoanele identificate notificate	P1
A2	Instrument online de verificare	AGE	30 de zile	S	Instrument funcțional; număr de verificări	P1
A3	Linie gratuită de asistență	Cancelaria de Stat, AGE, Poliția	15 zile	S	Timp mediu de răspuns sub 3 minute	P1
A4	Poarta de securitate pentru repunerea serviciilor	AGE, STISC, ASC	Imediat	M	100% din serviciile repuse au test independent	P1
A5	Inventarul complet al interfețelor	AGE, STISC, prestatorii	60 de zile	S	Inventar aprobat, cu responsabil pe serviciu	P1
A6	Detectarea comportamentală	STISC, ASC	60 de zile	M	Timp de detectare sub 1 oră în exerciții	P1
A7	Coaliția anti-fraudă	BNM, CNPF, bănci, operatori, Poliția	30 de zile	S	Număr de tentative blocate, raportat lunar	P1
A8	Blocarea voluntară a creditării pe IDNP	BNM, CNPF, Parlamentul	90 de zile (interimar)	S–M	Număr de persoane înscrise	P1
A9	Comisia independentă de anchetă	Guvernul / Parlamentul	Constituire în 30 de zile; raport în 90	S–M	Raport public publicat	P1
A10	Finalizarea investigației CNPDCP	CNPDCP	6 luni	S	Decizie publică cu măsuri corective	P1

[235]Regulamentul (UE) 2024/1183 al Parlamentului European și al Consiliului din 11 aprilie 2024 de modificare a Regulamentului (UE) nr. 910/2014 în ceea ce privește instituirea cadrului european privind identitatea digitală (eIDAS 2).

[236]Curtea de Justiție a Uniunii Europene, Hotărârea din 14 decembrie 2023, cauza C-340/21, VB împotriva Natsionalna agentsia za prihodite.

Cod	Acțiune	Responsabil	Termen	Cost	Indicator de rezultat	Prioritate
A11	Comunicarea unificată și campania anti-fraudă	Cancelaria de Stat, AGE, Poliția	Imediat	S	Pagină unică actualizată săptămânal	P1
A12	Evaluarea categoriilor sensibile	SIS, MAI, MA	60 de zile	S	Evaluare finalizată; măsuri aplicate	P1
A13	Cooperarea internațională pentru anchetă	Procuratura, Poliția, ASC	30 de zile	S	Cereri de asistență transmise	P2
B1	Testarea obligatorie a serviciilor	Guvernul (HG), ASC, AGE	6 luni	M	% servicii testate anual	P1
B2	Program public de raportare a vulnerabilităților	ASC, AGE	6 luni	S–M	Număr de raportări valide remediate	P2
B3	Minimizarea datelor în MConnect	AGE, deținătorii registrelor, CNPDCP	12 luni	M	% fluxuri revizuite	P1
B4	Evaluări de impact pentru serviciile la scară largă	Operatorii; aviz CNPDCP	12 luni	S–M	Număr de evaluări finalizate	P2
B5	Clarificarea rolurilor juridice	Cancelaria de Stat, MDED, Parlamentul	9 luni	S	Acorduri publicate pentru toate serviciile	P2
B6	Centrul guvernamental de operațiuni de securitate 24/7	STISC, ASC	12 luni	R	Funcționare 24/7; acoperirea serviciilor	P1
B7	Consolidarea CNPDCP	Parlamentul, Ministerul Finanțelor	Bugetul 2027	M	Număr de auditori IT; investigații finalizate	P2
B8	Protocolul ASC–STISC	Guvernul	6 luni	S	Protocol aprobat și testat	P2
B9	Răspunderea conducerii și includerea administrației centrale în Legea nr. 48/2023	MDED, Parlamentul	12 luni	S	Lege modificată	P2
B10	Modificarea art. 259 Cod penal	Ministerul Justiției, Parlamentul	12 luni	S	Lege adoptată	P3
B11	Exercițiu național de criză	ASC, STISC, SIS, CNPDCP	9 luni	S	Exercițiu realizat; raport de lecții învățate	P2
B12	Formare și clauze contractuale de securitate	AGE, Agenția Achiziții Publice	12 luni	S–M	Clauze standard aplicate în contracte noi	P2
C1	Arhitectură „încredere zero”	Cancelaria de Stat, STISC, AGE	36 de luni	FR	% servicii migrate	P2
C2	Identificatori derivați pe sectoare	AGE, ASP, Parlamentul	36 de luni	R	Studiu de fezabilitate; pilot	P3
C3	Certificarea de securitate a EVO	AGE, ASC	24 de luni	M	Certificare obținută	P2
C4	Transpunerea completă a NIS2	MDED, Parlamentul	24 de luni	S	Lege adoptată	P2
C5	Strategia de resurse umane în securitate cibernetică	Guvernul, Ministerul Educației	24 de luni	R	Rata de ocupare a posturilor	P2
C6	Raport anual public ASC–CNPDCP	ASC, CNPDCP	Anual	S	Raport publicat	P3

Cod	Acțiune	Responsabil	Termen	Cost	Indicator de rezultat	Prioritate
C7	Mecanism extrajudiciar de compensare	Parlamentul, Guvernul	24 de luni	M	Studiu și proiect de lege	P3

10. Concluzii

Incidentul din octombrie 2026 este cea mai gravă scurgere de date personale din istoria Republicii Moldova. Pe baza informațiilor publice disponibile la 3 noiembrie 2026, studiul ajunge la următoarele concluzii, structurate pe întrebările de cercetare.

Vulnerabilitățile (Î1). Incidentul nu a fost rezultatul unui atac de o sofisticare excepțională asupra infrastructurii centrale, ci al unor deficiențe de bază în stratul de servicii: servicii care returnau date personale fără autentificare, lipsa unor controale eficiente asupra volumului și a tiparelor de interogare și posibilitatea înlănțuirii serviciilor pentru agregarea datelor. Detectarea a venit de la cetățeni, nu de la sistemele de monitorizare. La nivel de guvernanță, rolurile juridice sunt neclare, iar verificarea obligatorie a securității înainte de lansarea serviciilor lipsește.

Cadrul legal și instituțional (Î2). Cadrul normativ este, formal, avansat și aliniat la standardele europene. Legea nr. 195/2024 și Legea nr. 48/2023 oferă instrumentele necesare: notificare în 72 de ore, informarea persoanelor, evaluări de impact, sancțiuni, inclusiv pentru autorități publice. Problema este aplicarea: legea protecției datelor era în vigoare de două luni, iar primul ciclu de verificare a conformității cu legea securității cibernetice nu ajunsese la scadență. Între AGE, STISC, deținătorii registrelor, ASC și CNPDCP există goluri și suprapuneri de responsabilitate care trebuie clarificate.

Riscurile (Î3). Riscurile cele mai mari sunt fraudele personalizate, care vizează disproporționat persoanele vulnerabile, și profilarea la scară națională prin agregarea cu alte seturi de date, în contextul avertismentelor publice privind colectarea coordonată a datelor cetățenilor de către servicii străine. O parte din riscuri vor rămâne ridicate pe termen lung, pentru că datele de identitate nu pot fi schimbate.

Experiența altor state (Î4). Cazurile comparate arată că vulnerabilitățile de acest tip apar și în statele cele mai avansate digital, că notificarea individuală rapidă și anchetele independente cu raport public protejează încrederea, că instituțiile publice pot fi trase la răspundere și că atribuirea către actori statali are greutate doar când este susținută de probe.

Conformitatea europeană (Î5). Republica Moldova are un nivel ridicat de aliniere formală la GDPR și Convenția 108+ și un nivel parțial față de NIS2 și eIDAS 2. Incidentul va fi un test al capacității de aplicare, relevant pentru negocierile de aderare.

Măsurile (Î6). Prioritățile imediate sunt notificarea individuală și sprijinul pentru persoanele afectate, poarta de securitate pentru repunerea serviciilor, detectarea comportamentală, o anchetă independentă cu raport public și o coaliție anti-fraudă. Pe termen mediu și lung, reforma trebuie să treacă de la securitatea infrastructurii la securitatea fiecărui serviciu, de la răspunderea persoanelor la răspunderea sistemului și de la conformitatea formală la cea demonstrată.

Incidentul nu invalidează strategia de digitalizare a Republicii Moldova. El arată însă că digitalizarea fără garanții de securitate la nivelul fiecărui serviciu transformă eficiența în vulnerabilitate. Modul în care statul va răspunde în lunile următoare — prin transparență, remedieri verificabile și protecția persoanelor afectate — va conta pentru încrederea cetățenilor mai mult decât incidentul în sine.

11. Limitele studiului

Date preliminare și în evoluție. Cifrele privind amploarea incidentului au fost comunicate de autorități ca preliminare. Ele pot fi revizuite după finalizarea investigațiilor. Studiul reflectă situația la 3 noiembrie 2026 și nu include rezultatele audierilor parlamentare din 4 noiembrie 2026 sau alte evoluții ulterioare.

Lipsa accesului la date tehnice. Studiul se bazează exclusiv pe surse publice. Autorul nu a avut acces la jurnalele de sistem, la rapoartele interne ale AGE, STISC, ASC sau SIS, ori la dosarul penal. Încadrarea vectorului de atac în categoriile OWASP este o interpretare analitică pe baza declarațiilor oficiale, nu o constatare tehnică.

Informații neconfirmate. Câteva elemente relevante au rămas neconfirmate sau indisponibile la data de referință: data și conținutul notificării transmise de AGE către CNPDCP; deciziile Consiliului Național de Securitate; punerea în circulație a datelor extrase; atribuirea tehnică a atacului; încadrarea formală a AGE în regimul Legii nr. 48/2023; includerea Republicii Moldova în eGovernment Benchmark 2025; resursele umane și financiare ale instituțiilor de securitate cibernetică.

Interpretarea juridică. Aplicarea Legii nr. 195/2024 față de instituții publice este netestată. Interpretările din acest studiu reflectă textul legii și analizele publicate, dar interpretarea finală aparține CNPDCP și instanțelor. Studiul nu constituie consultanță juridică.

Evaluarea riscurilor și a costurilor. Scorurile de probabilitate și impact, precum și ordinele de mărime ale costurilor, reflectă judecata experțială a autorului. Ele sunt destinate prioritizării și trebuie rafinate prin evaluări interne și calcule bugetare.

Surse de presă. O parte din fapte provin din presă și au fost marcate ca atare. Unele relatări timpurii au fost ulterior corectate de autorități (de exemplu, perioada incidentului); studiul a folosit versiunea cea mai recentă.

Bibliografie

Toate sursele online au fost consultate între 27 octombrie și 3 noiembrie 2026.

Acte normative, tratate și jurisprudență

1. Codul penal al Republicii Moldova nr. 985 din 18.04.2002, Capitolul XI „Infracțiuni informatice și infracțiuni în domeniul comunicațiilor electronice” (art. 259–260⁶), cu modificările ulterioare.
2. Consiliul Europei, Convenția privind criminalitatea informatică (STE nr. 185), Budapesta, 23.11.2001.
3. Curtea de Justiție a Uniunii Europene, Hotărârea din 14 decembrie 2023, cauza C-340/21, VB împotriva Natsionalna agentsia za prihodite.
4. Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (NIS2).
5. Hotărârea Guvernului nr. 1028/2023 privind organizarea și funcționarea Agenției pentru Securitate Cibernetică.
6. Hotărârea Guvernului nr. 211/2019 privind platforma de interoperabilitate (MConnect).
7. Hotărârea Guvernului nr. 333 din 08.05.2024 privind Consiliul de coordonare în domeniul securității cibernetice.
8. Hotărârea Guvernului nr. 482/2020 privind Serviciul Tehnologia Informației și Securitate Cibernetică (atribuții de echipă de răspuns la incidente pentru sectorul guvernamental).
9. Hotărârea Guvernului nr. 562 din 03.09.2025, act de punere în aplicare a Legii nr. 48/2023 privind securitatea cibernetică (cerințe de securitate pentru furnizorii de servicii); nota informativă: https://www.gov.md/sites/default/files/media/documents/sedinte-de-guvern/2025-09/NU-49-MDED-2025.pdf.
10. Hotărârea Guvernului nr. 760 din 18.08.2010 cu privire la Instituția publică „Agenția de Guvernare Electronică” (cu modificările ulterioare), inclusiv Statutul AGE.
11. Hotărârea Guvernului nr. 821/2025 cu privire la aprobarea Programului național de securitate cibernetică pentru anii 2026–2030.
12. Hotărârea Guvernului nr. 823/2025 privind planul național de gestionare a incidentelor și crizelor cibernetice.
13. Hotărârea Guvernului nr. 824/2025 privind divulgarea coordonată a vulnerabilităților.
14. Hotărârea Guvernului nr. 860/2024 cu privire la identificarea furnizorilor de servicii.
15. Legea nr. 124 din 19.05.2022 privind identificarea electronică și serviciile de încredere.
16. Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal (abrogată odată cu intrarea în vigoare a Legii nr. 195/2024).
17. Legea nr. 142 din 19.07.2018 cu privire la schimbul de date și interoperabilitate.
18. Legea nr. 195 din 25.07.2024 privind protecția datelor cu caracter personal, Monitorul Oficial din 23.08.2024, în vigoare din 23.08.2026.
19. Legea nr. 48 din 16.03.2023 privind securitatea cibernetică, Monitorul Oficial 2023, nr. 151–153, art. 225, în vigoare din 01.01.2025.
20. Legea nr. 6 din 02.02.2009 pentru ratificarea Convenției Consiliului Europei privind criminalitatea informatică.
21. Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 (Regulamentul general privind protecția datelor).

22. Regulamentul (UE) 2024/1183 al Parlamentului European și al Consiliului din 11 aprilie 2024 de modificare a Regulamentului (UE) nr. 910/2014 în ceea ce privește instituirea cadrului european privind identitatea digitală (eIDAS 2).

Documente și comunicări instituționale

23. AGE, comunicat privind restabilirea a 61 de servicii publice digitale, 30 octombrie 2026, preluat de Agenția Moldpres: https://www.moldpres.md/rom/societate/peste-60-de-servicii-publice-digitale-au-fost-restabilite-si-sunt-disponibile-pe-portalul-evo.

24. AGE, Serviciul Tehnologia Informației și Securitate Cibernetică (STISC) și Agenția pentru Securitate Cibernetică (ASC), comunicat comun privind incidentul de securitate cibernetică asupra serviciilor publice digitale, 24 octombrie 2026, egov.md.

25. Agenția de Guvernare Electronică (AGE), comunicat privind estimările preliminare ale incidentului cibernetic din 19–23 octombrie 2026, 27 octombrie 2026, https://egov.md/ro/node/41145.

26. CNIL, „Data breach: 5 million euro fine for France Travail”, 22 ianuarie 2026, https://www.cnil.fr/en/data-breach-5million-fine-france-travail.

27. CNPDCP, „Îndrumări/explicații în vederea aplicării corecte a Legii nr. 195/2024 privind protecția datelor cu caracter personal”, 2026, https://datepersonale.md/wp-content/uploads/2026/02/CONSIDERENTE_Legea_195.pdf.

28. CNPDCP, „Legea nr. 195/2024 privind protecția datelor cu caracter personal (în vigoare din 23 august 2026)”, material informativ, 2026, https://datepersonale.md/wp-content/uploads/2026/03/Legea-nr.1952024.pdf.

29. CNPDCP, comunicat privind ratificarea prin Legea nr. 36 din 20.03.2026 a Protocolului de amendare a Convenției 108 (CETS nr. 223), https://datepersonale.md/en/protocol-amending-convention-for-the-protection-of-individuals-with-regard-to-automatic-processing-of-personal-data-published-in-the-official-gazette/.

30. Committee of Inquiry into the Cyber Attack on SingHealth Patient Database System, Public Report, Singapore, 10 ianuarie 2019.

31. Consiliul Europei, „Republic of Moldova Becomes the 34th State to Ratify the Convention 108+”, 15 mai 2026, https://www.coe.int/en/web/data-protection/-/republic-of-moldova-becomes-the-34th-state-to-ratify-the-convention-108-.

32. Consiliul Europei, Biroul Comitetului Convenției 108 (T-PD-BUR), raport de reuniune, 2026, https://rm.coe.int/t-pd-bur-2026-66rapabr-en/48802dc789.

33. Consiliul I.P. „Agenția de Guvernare Electronică”, Decizia nr. 23 din 23.12.2025 (Raportul privind realizarea Planului de acțiuni al AGE pentru anul 2025), https://egov.md/sites/default/files/decizie_nr._23_din_23.12.2025_a_consiliului_i.p._age.semnat.signed_0.pdf.

34. Guvernul Republicii Moldova, „Lista structurilor organizaționale în care Cancelaria de Stat are calitatea de fondator”, https://gov.md/ro/lista-structurilor-organizationale-care-cancelaria-de-stat-are-calitatea-de-fondator.

35. Procuratura Generală, aviz din 29.11.2023 la proiectul de lege privind protecția datelor cu caracter personal, https://procuratura.md/sites/default/files/2024-02/29.11.2023%20Aviz%20PG%20proiect.pdf.

36. Proiect de lege pentru modificarea Codului penal și a Codului contravențional (alinierea la Directiva 2013/40/UE), nota informativă, https://particip.gov.md/ro/download_attachment/31395.

37. STISC, comunicat privind funcționarea normală a semnăturii electronice și a serviciilor de încredere, 1 noiembrie 2026.

38. U.S. House of Representatives, Committee on Oversight and Government Reform, The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation, raport al majorității, septembrie 2016.

Presă

39. Agerpres și Moldpres, relatări privind declarațiile STISC despre riscurile asociate codurilor IBAN extrase și data audierilor parlamentare, 29 octombrie 2026.

40. Agerpres, „Directorul SIS avertizează că Rusia se pregătește deja de următoarele alegeri din Republica Moldova", 2026, https://agerpres.ro/politic-extern/2026/07/09/directorul-sis-avertizeaza-ca-rusia-se-pregateste-deja-de-urmatoarele-alegeri-din-republica-moldova--1574709.

41. Arab News (AP), „Albania reports 2nd cyberattack by Iran, on border systems", 10 septembrie 2022, https://arabnews.pk/node/2159936.

42. BankInfoSecurity, „Australian Telecom Watchdog Sues Optus Over 2022 Data Breach", 2024, https://www.bankinfosecurity.com/australian-telecom-watchdog-sues-optus-over-2022-data-breach-a-25321.

43. Biometric Update, „House oversight committee OPM breach report calls for zero trust model, empowered CIOs", septembrie 2016, https://www.biometricupdate.com/201609/house-oversight-committee-opm-breach-report-calls-for-zero-trust-model-empowered-cios.

44. BleepingComputer, „France fines unemployment agency €5 million over data breach", ianuarie 2026, https://www.bleepingcomputer.com/news/security/france-fines-unemployment-agency-5-million-over-data-breach/.

45. Computer Weekly, „SingHealth and IT supplier fined S$1m for data breach", ianuarie 2019, https://www.computerweekly.com/news/252455861/SingHealth-and-IT-supplier-fined-S1m-for-data-breach.

46. CPO Magazine, „Optus Sued by Australian Privacy Regulator Over 2022 Data Breach", 2025, https://www.cpomagazine.com/data-protection/optus-sued-by-australian-privacy-regulator-over-2022-data-breach/.

47. CSO Online, „Optus breach occurred due to a coding error, alleges ACMA", 2024, https://www.csoonline.com/article/2492520/optus-breach-occurred-due-to-a-coding-error-alleges-acma.html.

48. Cyber Security Hub, „Albania hit with cyber attack after severing ties with Iran", septembrie 2022, https://cshub.com/attacks/news/iotw-albania-hit-with-cyber-attack-after-severing-ties-with-iran.

49. Digi24, „Consiliul de Securitate al R. Moldova, convocat după un atac cibernetic în care au fost furate datele personale a 750.000 de cetățeni", 28 octombrie 2026, https://www.digi24.ro/stiri/externe/moldova/consiliul-de-securitate-al-r-moldova-convocat-dupa-un-atac-cibernetic-in-care-au-fost-furate-datele-personale-a-750-000-de-cetateni-4013145.

50. Digi24, „Serviciile secrete ale Rusiei colectează datele personale ale moldovenilor, avertizează SIS de la Chișinău", iunie 2026, https://www.digi24.ro/stiri/externe/moldova/serviciile-secrete-ale-rusiei-colecteaza-datele-personale-ale-moldovenilor-avertizeaza-sis-de-la-chisinau-3819279; comunicatul SIS din 17 iunie 2026.

51. Ecom.md, „GDPR în Moldova: legea nr. 195/2024 pentru magazinul online", 2026, https://ecom.md/en/blog/protectia-datelor-lege-195-2024; i-Avocat.md, „Legea nr. 195/2024 privind protecția datelor cu caracter personal: prevederi aplicabile din 23 august 2026", 2026.

52. ERR News, „AK: RIA unlikely to be fined over mass photo hack, victims not compensated", 2021, https://news.err.ee/1608294000/ak-ria-unlikely-to-be-fined-over-mass-photo-hack-victims-not-compensated.

53. Gândul, „Cel mai puternic atac cibernetic asupra Republicii Moldova a fost anunțat în ziua vizitei premierului Niculescu la Chișinău”, 27 octombrie 2026, https://www.gandul.ro/actualitate/atac-cibernetic-republica-moldova-date-personale-21046430.

54. IPN, „Utilizatorii EVO vor trebui să instaleze cea mai recentă versiune a aplicației”, octombrie 2026, https://ipn.md/utilizatorii-evo-vor-trebui-sa-instaleze-cea-mai-recenta-versiune-a-aplicatiei.

55. iTnews, „US OPM CIO quits”, 2016, https://www.itnews.com.au/news/us-opm-cio-quits-415496.

56. Jurnal.md, relatare privind volumul de aproximativ 11 milioane de solicitări înregistrate în timpul atacului, octombrie 2026.

57. Logos Press, „Amenzi de până la 2 milioane de lei pentru încălcarea regulilor privind protecția datelor personale”, 2026, https://logos-pres.md/noutati/amenzi-de-pana-la-2-milioane-de-lei-pentru-incalcarea-regulilor-privind-protectia-datelor-personale/.

58. Logos Press, „How Moldova Managed to Rank Fifth in the World in Cybersecurity”, 2026, https://logos-pres.md/en/news/how-moldova-managed-to-rank-fifth-in-the-world-in-cybersecurity/.

59. Mediacritica, „Atacul asupra datelor personale: ce știm, ce nu știm și ce pericole subestimăm”, 2026, https://mediacritica.md/atacul-asupra-datelor-personale-ce-stim-ce-nu-stim-si-ce-pericole-subestimam/.

60. Moldpres, „Moldova - leader among EU expansion candidate states”, noiembrie 2025, https://www.moldpres.md/eng/eu-1/moldova-leader-among-eu-expansion-candidate-states.

61. NewsMaker, „(GHID) Ce faci dacă datele tale personale au ajuns la hackeri. Ce drepturi ai și când poți cere despăgubiri”, octombrie 2026, https://newsmaker.md/ro/ghid-ce-faci-dacă-datele-tale-personale-au-ajuns-la-hackeri-ce-drepturi-ai-și-când-poți-cere-despăgubiri.

62. NewsMaker, „Ce pot face moldovenii după scurgerea datelor personale? Centrul pentru Protecția Datelor cu Caracter Personal explică”, 29 octombrie 2026, https://newsmaker.md/ro/ce-pot-face-moldovenii-dupa-scurgerea-datelor-personale-centrul-pentru-protectia-datelor-cu-caracter-personal-explica.

63. NewsMaker, „Datele a circa 750.000 de persoane din Moldova au ajuns la hackeri. Autoritățile avertizează: pot fi folosite pentru fraudă”, 27 octombrie 2026, https://newsmaker.md/ro/datele-a-circa-750-000-de-persoane-din-moldova-au-ajuns-la-hackeri-autoritățile-avertizează-pot-fi-folosite-pentru-fraudă.

64. NewsMaker, relatare privind declarațiile prim-ministrului Vasile Tofan în ședința Guvernului din 28 octombrie 2026.

65. Postimees, „Hacker gains access to hundreds of thousands of document photos”, iulie 2021, https://news.postimees.ee/7303667/hacker-gains-access-to-hundreds-of-thousands-of-document-photos.

66. Radio Chișinău, „Agenția de Guvernare Electronică a activat actualizarea obligatorie a aplicației EVO”, 30 octombrie 2026, https://radiochisinau.md/agentia-de-guvernare-electronica-a-activat-actualizarea-obligatorie-a-aplicatiei-evo---230480.html.

67. Radio Moldova, „Datele personale a 750.000 de cetățeni, extrase în urma atacului cibernetic asupra sistemelor guvernamentale”, octombrie 2026, https://radiomoldova.md/p/88297.

68. Realitatea.md, „Cine răspunde pentru scurgerea datelor a sute de mii de moldoveni? Igor Grosu: Vor fi organizate audieri”, octombrie 2026, https://realitatea.md/video-cine-raspunde-pentru-scurgerea-datelor-a-sute-de-mii-de-moldoveni-igor-grosu-vor-fi-organizate-audieri/.

69. Security Affairs, „Albania was hit by a new cyberattack and blames Iran”, 11 septembrie 2022, https://securityaffairs.com/?p=135602.

70. Security Affairs, „Estonia's police arrested a Tallin resident who stole 286K ID scans from a government DB”, 30 iulie 2021, https://securityaffairs.com/120684/cyber-crime/estonia-s-police-hacker-id-scans.html.

71. Security Affairs, „France Travail data breach impacted 43 Million people”, 16 martie 2024, https://securityaffairs.com/160556/data-breach/france-travail-data-breach-34m-people.html.

72. Spotmedia, „Atac cibernetic masiv asupra Republicii Moldova”, octombrie 2026, https://spotmedia.ro/stiri/eveniment/atac-cibernetic-masiv-asupra-republicii-moldova.

73. TechPartner News, „OAIC takes Optus to court over 2022 data breach”, 8 august 2025, https://www.techpartner.news/news/oaic-takes-optus-to-court-over-2022-data-breach-619433.

74. Telegraph.md și Pivot.md, relatări privind notificarea Centrului Național pentru Protecția Datelor cu Caracter Personal de către AGE, octombrie 2026.

75. The Baltic Times, „Hundreds of thousands of ID photos illegally downloaded in Estonia”, 28 iulie 2021, https://www.baltictimes.com/hundreds_of_thousands_of_id_photos_illegally_downloaded_in_estonia.

76. The Record (Recorded Future News), relatare privind atacul asupra serviciilor publice digitale ale Republicii Moldova și cele aproximativ 11 milioane de solicitări, octombrie 2026.

77. The Record, „Estonia says a hacker downloaded 286,000 ID photos from government database”, iulie 2021, https://therecord.media/estonia-says-a-hacker-downloaded-286000-id-photos-from-government-database.

78. Threatpost, „OPM Hack Expands to Include Data of 21.5 Million People; Director Archuleta Resigns”, iulie 2015, https://threatpost.com/opm-hack-expands-to-include-data-of-21-5-million-people/113717.

79. Timpul.md, „CNPDCP investighează extragerea neautorizată a datelor asociate cu aproximativ 750.000 de IDNP-uri”, 31 octombrie 2026, https://timpul.md/articol/cnpdcp-investigheaza-extragerea-neautorizata-a-datelor-asociate-cu-aproximativ-750000-de-idnp-uri-b12f4b8c.html.

80. TVR Moldova, „Cine răspunde pentru furtul de date ale moldovenilor? Procuratura a pornit o urmărire penală”, 30 octombrie 2026, https://tvrmoldova.md/article/332627a01e45d8f2/cine-raspunde-pentru-scurgerea-de-date-ale-moldovenilor-procuratura-a-pornit-o-urmarire-penala.html.

81. Unimedia, interviu cu Nicoleta Colomeeț, directoarea AGE, 31 octombrie 2026.

82. Washington Examiner, „Government hacks hit 22.1 million”, iulie 2015, https://www.washingtonexaminer.com/politics/2004691/government-hacks-hit-22-1-million/.

83. Wiki.sg, „SingHealth data breach (2018)”, https://wiki.sg/p/SingHealth_data_breach_(2018).

84. Ziar.md, „Alte 11 servicii publice digitale au devenit disponibile după atacurile cibernetice”, noiembrie 2026, https://ziar.md/alte-11-servicii-publice-digitale-au-devenit-disponibile-dupa-atacurile-cibernetice/.

85. Ziar.md, „CEC renunță la identificarea digitală a alegătorilor la scrutinele din 1 noiembrie”, octombrie 2026, https://ziar.md/cec-renunta-la-identificarea-digitala-a-alegatorilor-la-scrutinele-din-1-noiembrie/.

86. Ziar.md, „Noi informații despre atacul cibernetic: 61 de servicii publice au fost restabilite, iar 21 rămân temporar indisponibile”, 30 octombrie 2026, https://ziar.md/noi-informatii-despre-atacul-cibernetic-61-de-servicii-publice-au-fost-restabilite-2/.

Rapoarte, indici, standarde și literatură de specialitate

87. „Prevenirea și combaterea criminalității informatice prin cooperare la nivel național și internațional”, articol științific, Zenodo, https://zenodo.org/records/7573428.

88. CMS, GDPR Enforcement Tracker Report – Bulgaria, 21 mai 2026, https://cms.law/en/bgr/publication/gdpr-enforcement-tracker-report/bulgaria.

89. Comisia Europeană (Capgemini și parteneri), eGovernment Benchmark 2025, publicat în 2026, https://www.capgemini.com/insights/research-library/results-of-the-egov-benchmark/.

90. e-Governance Academy, National Cyber Security Index, profilul Republicii Moldova (ultima actualizare a datelor: 29.01.2026), https://ncsi.ega.ee/country/md/.

91. Internet Society Pulse, profilul Republicii Moldova, https://pulse.internetsociety.org/en/reports/md.

92. ISMS.online, „As Optus Is Sued, What Went Wrong and What Lessons Can We Learn?”, 2025, https://www.isms.online/data-protection/as-optus-is-sued-what-went-wrong-and-what-lessons-can-we-learn/.

93. ISO/IEC 27005:2022, Information security, cybersecurity and privacy protection — Guidance on managing information security risks.

94. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), informații instituționale, https://ccdcoe.org.

95. NIST, Special Publication 800-207, Zero Trust Architecture, august 2020.

96. NIST, Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessments, septembrie 2012.

97. OWASP Foundation, OWASP API Security Top 10 – 2023, https://owasp.org/API-Security/.

98. Society for Computers & Law, „Singapore's worst cyber attack: the outcome of the investigation”, 2019, https://www.scl.org/10405-singapore-s-worst-cyber-attack-the-outcome-of-the-investigation/.

99. SOCRadar, „Diplomatic Crisis: Cyber Attack from Iran to Albania”, 19 septembrie 2022, https://socradar.io/diplomatic-crisis-cyber-attack-from-iran-to-albania/.

100. Uniunea Internațională a Telecomunicațiilor (ITU), Global Cybersecurity Index 2024, ediția a 5-a, 2024, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf.

Anexa 1. Cronologia detaliată

Tabelul A1. Cronologia detaliată a incidentului și a răspunsului instituțional

Data și ora	Eveniment	Sursa	Nivel de certitudine
17 iun. 2026	SIS avertizează public privind colectarea coordonată a datelor personale ale cetățenilor de către serviciile speciale ruse	SIS, preluat de presă[237]	Declarație oficială
23 aug. 2026	Intră în vigoare Legea nr. 195/2024 privind protecția datelor	CNPDCP[238]	Confirmat
19 oct. 2026	Începutul perioadei de extragere identificate ulterior	AGE[239]	Confirmat oficial (preliminar)
19–23 oct.	Interogări folosind circa 1 milion de IDNP; circa 11 milioane de solicitări	AGE; presă; conducerea AGE[240,241,242]	Confirmat oficial (IDNP); confirmat în interviu (solicitări)
22 oct., seara	Cetățeni observă accesări suspecte în EVO și le semnalează public	Presă[243,244]	Relatat de presă
23 oct., 11:20	Incidentul este înregistrat formal, după rapoartele cetățenilor către suport	Conducerea AGE[245]	Declarație în interviu
23 oct., 11:30	Extragerea este oprită	AGE[246]	Confirmat oficial
23 oct.	82 de servicii publice și peste 30 de sisteme și panouri de administrare deconectate preventiv	AGE[247]	Confirmat oficial
24 oct.	Comunicat comun AGE, STISC, ASC; incidentul plasat inițial „în noaptea de 22 octombrie”	AGE, STISC, ASC[248]	Confirmat oficial

[237]Digi24, „Serviciile secrete ale Rusiei colectează datele personale ale moldovenilor, avertizează SIS de la Chișinău”, iunie 2026 comunicatul SIS din 17 iunie 2026.

[238]CNPDCP, „Îndrumări/explicații în vederea aplicării corecte a Legii nr. 195/2024 privind protecția datelor cu caracter personal”, 2026.

[239]Agenția de Guvernare Electronică (AGE), comunicat privind estimările preliminare ale incidentului cibernetic din 19–23 octombrie 2026, 27 octombrie 2026.

[240]Agenția de Guvernare Electronică (AGE), comunicat privind estimările preliminare ale incidentului cibernetic din 19–23 octombrie 2026, 27 octombrie 2026.

[241]The Record (Recorded Future News), relatare privind atacul asupra serviciilor publice digitale ale Republicii Moldova și cele aproximativ 11 milioane de solicitări, octombrie 2026.

[242]Unimedia, interviu cu Nicoleta Colomeeț, directoarea AGE, 31 octombrie 2026.

[243]NewsMaker, „(GHID) Ce faci dacă datele tale personale au ajuns la hackeri. Ce drepturi ai și când poți cere despăgubiri”, octombrie 2026.

[244]Gândul, „Cel mai puternic atac cibernetic asupra Republicii Moldova a fost anunțat în ziua vizitei premierului Niculescu la Chișinău”, 27 octombrie 2026.

[245]Unimedia, interviu cu Nicoleta Colomeeț, directoarea AGE, 31 octombrie 2026.

[246]Agenția de Guvernare Electronică (AGE), comunicat privind estimările preliminare ale incidentului cibernetic din 19–23 octombrie 2026, 27 octombrie 2026.

[247]Agenția de Guvernare Electronică (AGE), comunicat privind estimările preliminare ale incidentului cibernetic din 19–23 octombrie 2026, 27 octombrie 2026.

Data și ora	Eveniment	Sursa	Nivel de certitudine
25 oct., ~02:00	Tentativă de acces forțat, blocată	AGE[249]	Confirmat oficial
27 oct., ~07:00	Noi tentative de extragere, fără succes	AGE[250]	Confirmat oficial
27 oct.	AGE publică estimările preliminare: circa 750.000 de IDNP cu date extrase; categoriile de date; nicio modificare în registre	AGE[251]	Confirmat oficial
28 oct.	Prim-ministrul anunță retragerea directoarei AGE și desemnarea unui interimar; declarații privind o campanie mai largă cu implicarea unor actori statali străini	Guvern, presă[252,253]	Confirmat oficial (decizia); atribuirea neconfirmată
28 oct., seara	Președinta convoacă Consiliul Național de Securitate; Președinția afirmă că atacul a fost cel mai probabil facilitat de inteligența artificială	Președinția[254]	Confirmat oficial (convocarea)
28–29 oct.	Comisia parlamentară decide în unanimitate organizarea de audieri	Parlament, presă[255]	Confirmat oficial
29 oct.	CNPDCP: responsabilitatea revine instituțiilor care dețin bazele de date; căi de sesizare pentru cetățeni	CNPDCP[256]	Confirmat oficial
29 oct.	STISC: IBAN-ul singur nu permite accesul la cont; audierile fixate pentru 4 noiembrie	STISC, presă[257]	Confirmat oficial
30 oct.	61 de servicii restabilite, 21 indisponibile; pregătirea notificării individuale; actualizarea obligatorie a EVO; limitarea „e-Traversare”	AGE[258,259,260]	Confirmat oficial

[248]AGE, Serviciul Tehnologia Informației și Securitate Cibernetică (STISC) și Agenția pentru Securitate Cibernetică (ASC), comunicat comun privind incidentul de securitate cibernetică asupra serviciilor publice digitale, 24 octombrie 2026, egov.md.

[249]Agenția de Guvernare Electronică (AGE), comunicat privind estimările preliminare ale incidentului cibernetic din 19–23 octombrie 2026, 27 octombrie 2026.

[250]Agenția de Guvernare Electronică (AGE), comunicat privind estimările preliminare ale incidentului cibernetic din 19–23 octombrie 2026, 27 octombrie 2026.

[251]Agenția de Guvernare Electronică (AGE), comunicat privind estimările preliminare ale incidentului cibernetic din 19–23 octombrie 2026, 27 octombrie 2026.

[252]NewsMaker, relatare privind declarațiile prim-ministrului Vasile Tofan în ședința Guvernului din 28 octombrie 2026.

[253]TVR Moldova, „Cine răspunde pentru furtul de date ale moldovenilor? Procuratura a pornit o urmărire penală”, 30 octombrie 2026.

[254]Digi24, „Consiliul de Securitate al R. Moldova, convocat după un atac cibernetic în care au fost furate datele personale a 750.000 de cetățeni”, 28 octombrie 2026.

[255]Realitatea.md, „Cine răspunde pentru scurgerea datelor a sute de mii de moldoveni? Igor Grosu: Vor fi organizate audieri”, octombrie 2026.

[256]NewsMaker, „Ce pot face moldovenii după scurgerea datelor personale? Centrul pentru Protecția Datelor cu Caracter Personal explică”, 29 octombrie 2026.

[257]Agerpres și Moldpres, relatări privind declarațiile STISC despre riscurile asociate codurilor IBAN extrase și data audierilor parlamentare, 29 octombrie 2026.

[258]AGE, comunicat privind restabilirea a 61 de servicii publice digitale, 30 octombrie 2026.

Data și ora	Eveniment	Sursa	Nivel de certitudine
30 oct. (anunț public)	Procuratura municipiului Chișinău a pornit urmărirea penală	Procuratura, presă[261]	Confirmat oficial
30 oct.	Predarea interimatului la conducerea AGE	Presă	Relatat de presă
31 oct.	CNPDCP anunță inițierea unei investigații	Presă[262]	Relatat de presă
31 oct.	Interviul fostei directoare a AGE: detectarea prin rapoartele cetățenilor; monitorizarea nu a semnalat traficul	Presă[263]	Declarație în interviu
1 nov.	Alegeri desfășurate fără identificarea alegătorilor prin EVO; STISC: semnătura electronică și serviciile de încredere funcționează normal	CEC, STISC[264,265]	Confirmat oficial
Început de nov.	Alte 11 servicii restabilite, inclusiv extrase din registrele populației și persoanelor juridice	AGE, presă[266]	Confirmat oficial
4 nov., 09:00	Audieri parlamentare cu ușile închise (programate)	Parlament, presă[267,268]	Anunțat oficial

[259]Ziar.md, „Noi informații despre atacul cibernetic: 61 de servicii publice au fost restabilite, iar 21 rămân temporar indisponibile”, 30 octombrie 2026.

[260]Radio Chișinău, „Agenția de Guvernare Electronică a activat actualizarea obligatorie a aplicației EVO”, 30 octombrie 2026.

[261]TVR Moldova, „Cine răspunde pentru furtul de date ale moldovenilor? Procuratura a pornit o urmărire penală”, 30 octombrie 2026.

[262]Timpul.md, „CNPDCP investighează extragerea neautorizată a datelor asociate cu aproximativ 750.000 de IDNP-uri”, 31 octombrie 2026.

[263]Unimedia, interviu cu Nicoleta Colomeeț, directoarea AGE, 31 octombrie 2026.

[264]Ziar.md, „CEC renunță la identificarea digitală a alegătorilor la scrutinele din 1 noiembrie”, octombrie 2026.

Anexa 2. Glosar

Tabelul A2. Glosarul termenilor folosiți în studiu

Termen	Explicație
API (interfață de programare)	Mecanism prin care un sistem informatic oferă date sau funcții altor sisteme, în mod automat
Atribuire	Procesul de identificare a autorului unui atac cibernetic, cu un anumit nivel de încredere
Autentificare	Stabilirea identității celui care face o cerere
Autorizare la nivel de obiect	Verificarea, la fiecare cerere, că solicitantul are dreptul să acceseze datele unei anumite persoane sau înregistrări
Bug bounty	Program prin care o organizație recompensează cercetătorii care raportează responsabil vulnerabilități
Divulgare coordonată a vulnerabilităților	Procedură prin care o vulnerabilitate descoperită este raportată, remediată și abia apoi făcută publică
Doxxing	Publicarea, cu intenție de intimidare, a datelor personale ale unei persoane
Enumerare	Generarea sau colectarea sistematică a unor identificatori pentru a fi folosiți în interogări
Evaluarea impactului asupra protecției datelor	Analiză obligatorie, înaintea unei prelucrări cu risc ridicat, a riscurilor pentru persoane și a măsurilor de reducere a acestora
Expunere excesivă de date	Returnarea de către un serviciu a mai multor date decât sunt necesare scopului său
IDNP	Numărul de identificare de stat al persoanei fizice
Inginerie socială	Manipularea persoanelor pentru a le determina să divulge informații sau să efectueze acțiuni
Interoperabilitate	Capacitatea sistemelor informatice de a schimba date între ele
Încălcarea securității datelor	Breșă care duce la distrugerea, pierderea, modificarea, divulgarea sau accesarea neautorizată a datelor personale
Încredere zero (Zero Trust)	Model de securitate în care nicio cerere nu este considerată de încredere implicit
Limitarea ratei de cereri	Restricționarea numărului de cereri pe care un solicitant le poate face într-un interval de timp
Operator	Entitatea care stabilește scopurile și mijloacele prelucrării datelor personale
Persoană împuternicită	Entitatea care prelucrează date personale în numele operatorului

[265]STISC, comunicat privind funcționarea normală a semnăturii electronice și a serviciilor de încredere, 1 noiembrie 2026.

[266]Ziar.md, „Alte 11 servicii publice digitale au devenit disponibile după atacurile cibernetice”, noiembrie 2026.

[267]Realitatea.md, „Cine răspunde pentru scurgerea datelor a sute de mii de moldoveni? Igor Grosu: Vor fi organizate audieri”, octombrie 2026.

[268]Agerpres și Moldpres, relatări privind declarațiile STISC despre riscurile asociate codurilor IBAN extrase și data audierilor parlamentare, 29 octombrie 2026.

Termen	Explicație
Profilare	Prelucrarea automată a datelor pentru a evalua sau a prezice aspecte privind o persoană
SOC	Centru de operațiuni de securitate, care monitorizează permanent sistemele și răspunde la incidente
Test de penetrare	Simulare autorizată a unui atac pentru a identifica vulnerabilități
Vishing	Fraudă prin apel telefonic, în care atacatorul se prezintă drept bancă, instituție sau rudă

Anexa 3. Tabele suplimentare

Tabelul A3. Riscul rezidual estimat după implementarea măsurilor recomandate

Cod	Risc	Nivel actual	Măsuri principale	Nivel rezidual estimat
R1	Fraude personalizate	Critic (20)	A1, A3, A7, A11	Ridicat (12)
R2	Furt de identitate	Ridicat (12)	A7, A8, întărirea verificărilor de identitate	Moderat (8)
R3	Credite frauduloase	Ridicat (12)	A8, A7	Moderat (6)
R4	Țintirea grupurilor vulnerabile	Ridicat (16)	A1, A3, A11	Ridicat (12)
R5	Expunerea datelor de sănătate	Moderat (9)	A1, B3	Moderat (6)
R6	Șantaj și presiuni	Ridicat (12)	A12	Moderat (9)
R7	Doxxing și hărțuire	Ridicat (12)	A12, A1	Moderat (9)
R8	Presiuni asupra diasporei	Moderat (9)	A1, A11	Moderat (6)
R9	Siguranța minorilor	Ridicat (10)	A1, A11	Moderat (5)
R10	Operațiuni hibride	Ridicat (16)	A11, A12, cooperare internațională	Ridicat (12)
R11	Manipulare electorală	Ridicat (12)	A11, C3	Moderat (9)
R12	Profilare prin agregare	Critic (20)	A12, B3, C2	Ridicat (16)
R13	Recrutare și contrainformații	Ridicat (15)	A12	Ridicat (10)
R14	Erodarea încrederii	Ridicat (12)	A1, A9, A11, C6	Moderat (6)
R15	Impact asupra aderării la UE	Moderat (9)	A9, A10, C4	Scăzut (4)
R16	Repetarea atacului	Ridicat (15)	A4, A5, A6, B1, B6	Moderat (6)
R17	Ocolirea verificărilor la distanță	Ridicat (12)	A7, coordonarea cu sectorul financiar	Moderat (8)
R18	Contagiune în sectorul privat	Ridicat (12)	A7	Moderat (6)
R19	Suprasolicitarea instituțiilor	Moderat (8)	A2, A3	Scăzut (4)

Evaluarea aparține autorului. Nivelul rezidual presupune implementarea integrală și în termen a măsurilor indicate.

Tabelul A4. Actele normative și documentele analizate

Act / document	Obiect	Relevanță pentru incident
Legea nr. 195/2024	Protecția datelor cu caracter personal (în vigoare din 23.08.2026)	Obligații de securitate, notificare, evaluare de impact; sancțiuni
Legea nr. 133/2011	Fosta lege a protecției datelor (abrogată)	Regimul anterior; termen de comparație
Legea nr. 48/2023	Securitatea cibernetică (în vigoare din 01.01.2025)	Gestionarea riscurilor și notificarea incidentelor
HG nr. 1028/2023	Agenția pentru Securitate Cibernetică	Autoritate competentă și echipă națională de răspuns
HG nr. 333/2024	Consiliul de coordonare în domeniul securității cibernetice	Coordonare interinstituțională
HG nr. 860/2024	Identificarea furnizorilor de servicii	Domeniul de aplicare al Legii nr. 48/2023
HG nr. 562/2025	Cerințe de securitate pentru furnizorii de servicii	Prima evaluare a conformității în 24 de luni

Act / document	Obiect	Relevanță pentru incident
HG nr. 821/2025	Programul național de securitate cibernetică 2026–2030	Cadrul strategic
HG nr. 823/2025	Gestionarea incidentelor și crizelor cibernetice	Răspunsul la criză
HG nr. 824/2025	Divulgarea coordonată a vulnerabilităților	Raportarea vulnerabilităților
Legea nr. 142/2018	Schimbul de date și interoperabilitatea	Cadrul MConnect
HG nr. 211/2019	Platforma de interoperabilitate MConnect	Rolurile AGE și STISC
Legea nr. 124/2022	Identificarea electronică și serviciile de încredere	MPass, MSign, EVO
HG nr. 760/2010	Instituția publică AGE	Statutul și fondatorul AGE
Codul penal, art. 259–260[6]	Infracțiuni informatice	Răspunderea penală a autorilor
Legea nr. 6/2009	Ratificarea Convenției de la Budapesta	Cooperarea internațională în anchetă
Legea nr. 36/2026	Ratificarea Protocolului CETS nr. 223 (Convenția 108+)	Standarde internaționale de protecție a datelor
Regulamentul (UE) 2016/679	GDPR	Standard de referință pentru aliniere
Directiva (UE) 2022/2555	NIS2	Standard de referință pentru securitatea cibernetică
Regulamentul (UE) 2024/1183	eIDAS 2	Standard pentru identitatea digitală
Hotărârea CJUE, cauza C-340/21	Răspunderea operatorului și prejudiciul moral	Interpretarea acțiunilor în despăgubire