



Bruxelles, 13 noiembrie 2017
(OR. en)

14116/17

**Dosar interinstituțional:
2016/0409 (COD)**

**SIRIS 189
ENFOPOL 514
COPEN 335
SCHENGEN 80
COMIX 748
CODEC 1769**

REZULTATUL LUCRĂRILOR

Sursă:	Secretariatul General al Consiliului
Destinatar:	Delegațiile
Nr. doc. ant.:	13454/17
Nr. doc. Csie:	15814/16
Subiect:	Propunere de regulament al Parlamentului European și al Consiliului privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul cooperării polițienești și al cooperării judiciare în materie penală, de modificare a Regulamentului (UE) nr. 515/2014 și de abrogare a Regulamentului (CE) nr. 1986/2006, a Deciziei 2007/533/JAI a Consiliului și a Deciziei 2010/261/UE a Comisiei - Mandat de începere a negocierilor interinstituționale

În cadrul reuniunii sale din 8 noiembrie 2017, Coreperul a fost de acord să mandateze Președinția să înceapă negocierile interinstituționale pe baza textului de compromis revizuit care este cuprins în anexă.

La procesul-verbal al reuniunii Coreperului din 8 noiembrie 2018 va fi anexată o declarație din partea Greciei.

Regatul Unit își menține încă o rezervă generală și o rezervă de examinare parlamentară cu privire la aceste instrumente.

Modificările față de propunerea inițială a Comisiei sunt evidențiate după cum urmează: textul nou sau modificat este redat cu **caractere aldine subliniate**. Textul eliminat este evidențiat prin [...].

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI
privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în
domeniul
cooperării polițienești și al cooperării judiciare în materie penală, de modificare a
Regulamentului (UE)
nr. 515/2014 și de abrogare a Regulamentului (CE) nr. 1986/2006, a Deciziei 2007/533/JAI a
Consiliului
și a Deciziei 2010/261/UE a Comisiei

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 82 alineatul (1) al doilea paragraf litera (d), articolul 85 alineatul (1), articolul 87 alineatul (2) litera (a) și articolul 88 alineatul (2) litera (a),

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

- (1) Sistemul de informații Schengen (SIS) este un instrument esențial pentru aplicarea dispozițiilor acquis-ului Schengen, astfel cum este integrat în cadrul Uniunii Europene. SIS este una dintre cele mai importante măsuri compensatorii și unul dintre instrumentele majore **de asigurare a respectării legii**, contribuind la menținerea unui nivel ridicat de securitate în spațiul de libertate, securitate și justiție al Uniunii Europene prin sprijinirea cooperării operaționale între polițiștii de frontieră, poliție, autoritățile vamale și alte autorități [...] **responsabile de prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor ori de executarea [...] pedepselor sau de verificările asupra resortisanților țărilor terte** [...] ¹.

¹ Formulare conformă cu articolul 43 alineatul (1) litera (c).

- (2) SIS a fost înființat **initial** în temeiul dispozițiilor titlului IV din Convenția din 19 iunie 1990 de punere în aplicare a Acordului Schengen din 14 iunie 1985 dintre guvernele statelor din Uniunea Economică Benelux, Republicii Federale Germania și Republicii Franceze privind eliminarea treptată a controalelor la frontierele comune² (Convenția Schengen). Dezvoltarea SIS de a doua generație (SIS II) a fost încredințată Comisiei în temeiul Regulamentului (CE) nr. 2424/2001 al Consiliului³ și al Deciziei 2001/886/JAI a Consiliului⁴ și acest sistem a fost instituit prin Regulamentul (CE) nr. 1987/2006⁵, precum și prin Decizia 2007/533/JAI a Consiliului⁶. SIS II a înlocuit SIS, astfel cum a fost creat în temeiul Convenției Schengen.
- (3) La trei ani de la intrarea în funcțiune a SIS II, Comisia a efectuat o evaluare a sistemului în conformitate cu articolul 24 alineatul (5), articolul 43 alineatul (5) și articolul 50 alineatul (5) din Regulamentul (CE) nr. 1987/2006 și cu articolul 59 și articolul 65 alineatul (5) din Decizia 2007/533/JAI. Raportul de evaluare și documentul de lucru conex au fost adoptate la 21 decembrie 2016⁷. Recomandările formulate în aceste documente [...] se reflectă, după caz, în prezentul regulament.

² JO L 239, 22.9.2000, p. 19. Convenție astfel cum a fost modificată prin Regulamentul (CE) nr. 1160/2005 al Parlamentului European și al Consiliului (JO L 191, 22.7.2005, p. 18).

³ JO L 328, 13.12.2001, p. 4..

⁴ Decizia 2001/886/JAI a Consiliului din 6 decembrie 2001 privind dezvoltarea Sistemului de Informații Schengen din a doua generație (SIS II) (JO L 328, 13.12.2001, p. 1).

⁵ Regulamentul (CE) nr. 1987/2006 al Parlamentului European și al Consiliului din 20 decembrie 2006 privind instituirea, funcționarea și utilizarea Sistemului de Informații Schengen din a doua generație (SIS II) (JO L 181, 28.12.2006, p. 4).

⁶ Decizia 2007/533/JAI a Consiliului din 12 iunie 2007 privind înființarea, funcționarea și utilizarea Sistemului de informații Schengen de a doua generație (SIS II) (JO L 205, 7.8.2007, p. 63).

⁷ Raportul către Parlamentul European și Consiliu privind evaluarea Sistemului de informații Schengen de a doua generație (SIS II) în conformitate cu articolul 24 alineatul (5), articolul 43 alineatul (3) și articolul 50 alineatul (5) din Regulamentul (CE) nr. 1987/2006 și cu articolul 59 alineatul (3) și articolul 66 alineatul (5) din Decizia 2007/533/JAI și documentul de lucru însoțitor.

- (4) Prezentul regulament constituie temeiul legislativ necesar pentru reglementarea SIS în ceea ce privește aspectele care intră în domeniul de aplicare al titlului V capitolele 4 și 5 din Tratatul privind funcționarea Uniunii Europene. Regulamentul (UE) 2018/... al Parlamentului European și al Consiliului privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen (SIS) în domeniul verificărilor la frontiere⁸ constituie temeiul legislativ necesar pentru reglementarea SIS în ceea ce privește aspectele care intră în domeniul de aplicare al titlului V capitolul 2 din Tratatul privind funcționarea Uniunii Europene.
- (5) Faptul că temeiul legislativ necesar pentru reglementarea SIS constă în instrumente separate nu afectează principiul conform căruia SIS constituie un sistem de informații unic, care ar trebui să funcționeze ca atare **și să cuprindă o singură rețea de birouri SIRENE pentru a asigura schimbul de informații suplimentare**. Prin urmare, anumite dispoziții ale acestor instrumente ar trebui să fie identice.
- (6) Este necesar să se specifice obiectivele SIS, **anumite elemente ale** arhitecturii sale tehnice, [...] finanțarea sa, să se stabilească norme privind funcționarea și utilizarea sa de la un capăt la altul, precum și să se definească responsabilitățile, categoriile de date care trebuie introduse în sistem, scopurile introducerii și **prelucrării** acestora, criteriile introducerii acestora, autoritățile autorizate să aibă acces la date, utilizarea **datelor** biometrice [...] și alte norme privind prelucrarea datelor.

⁸ Regulamentul (UE) 2018/...

- (7) SIS cuprinde un sistem central (SIS central) și sisteme naționale **care pot conține** [...] o copie integrală sau parțială a bazei de date din SIS **ce poate fi utilizată în comun de două sau mai multe state membre**. Având în vedere că SIS este cel mai important instrument de schimb de informații în Europa, este necesar, **pentru asigurarea securității și a unei gestionări eficiente a migrației**, să se asigure funcționarea sa neîntreruptă atât la nivel central, cât și la nivel național. **Disponibilitatea SIS ar trebui să fie supusă unei monitorizări atente la nivel central și la nivelul statelor membre, iar orice incident de întrerupere a disponibilității pentru utilizatorii finali ar trebui înregistrat și raportat părților interesate de la nivel național și de la nivelul UE.** [...] Fiecare stat membru ar trebui să [...] realizeze **o** copie [...] de rezervă **pentru** sistemul **său național**. **De asemenea, statele membre ar trebui să asigure conectarea neîntreruptă cu SIS central prin intermediul unor puncte de conectare duplicate, separate din punct de vedere fizic și geografic. SIS central ar trebui să fie gestionat astfel încât să se asigure funcționarea sa 24 de ore pe zi, 7 zile pe săptămână. În acest scop se poate recurge la o soluție activ-activ.**
- (7A) Arhitectura tehnică a SIS poate face obiectul unor modificări ca urmare a evoluțiilor tehnice, asigurându-se, în același timp, cel mai înalt grad de disponibilitate pentru utilizatorii finali la nivel central și național, îndeplinirea tuturor cerințelor aplicabile privind protecția datelor, serviciile necesare pentru introducerea datelor în SIS și prelucrarea acestora, inclusiv căutările în baza de date din SIS, precum și o rețea de comunicare virtuală criptată destinată datelor din SIS și schimbului de date între birourile SIRENE. Modificările ar trebui să fie stabilite pe baza unei evaluări a impactului și a costurilor și vor fi comunicate Parlamentului European și Consiliului.**
- (8) Este necesar să existe un manual care să stabilească normele detaliate privind schimbul de [...] informații suplimentare referitoare la acțiunea care trebuie întreprinsă ca urmare a semnalărilor. Autoritățile naționale din fiecare stat membru (birourile SIRENE) ar trebui să asigure schimbul acestor informații.

- (9) Pentru a menține schimbul eficient de informații suplimentare [...], este oportun să se consolideze funcționarea birourilor SIRENE prin precizarea cerințelor referitoare la resursele disponibile, la formarea utilizatorilor și la timpul de răspuns la solicitările primite din partea altor birouri SIRENE.
- (10) Gestionarea operațională a componentelor centrale ale SIS este realizată de Agenția Europeană pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție⁹ („agenția”). Pentru a-i permite agenției să aloce resursele financiare și de personal necesare care să acopere toate aspectele legate de gestionarea operațională a SIS central **și a infrastructurii de comunicații**, prezentul regulament ar trebui să îi stabilească în detaliu sarcinile, în special în ceea ce privește aspectele tehnice ale schimbului de informații suplimentare.
- (11) Fără a aduce atingere responsabilității **principale** a statelor membre pentru exactitatea datelor introduse în SIS **și nici rolului birourilor SIRENE de coordonatori pentru calitate**, agenția ar trebui să devină responsabilă cu îmbunătățirea calității datelor prin introducerea unui instrument central de monitorizare a calității datelor și cu prezentarea de rapoarte Comisiei **și** statelor membre, la intervale regulate.
- (12) Pentru a permite o mai bună monitorizare a utilizării SIS în scopul de a analiza tendințele în materie de infracțiuni, agenția ar trebui să fie în măsură să dezvolte un sistem conform cu stadiul actual al tehnologiei în vederea elaborării de rapoarte statistice destinate statelor membre, Comisiei, Europolului și Agenției Europene pentru Poliția de Frontieră și Garda de Coastă, fără a pune în pericol integritatea datelor. Prin urmare, ar trebui să se instituie un registru statistic central. Nicio statistică întocmită nu ar trebui să conțină date cu caracter personal. **Statele membre ar trebui să transmită mecanismului de cooperare statistici referitoare la dreptul de acces la date, de rectificare a datelor inexacte și de ștergere a datelor stocate în mod ilegal.**

⁹ Instituită prin Regulamentul (UE) nr. 1077/2011 al Parlamentului European și al Consiliului din 25 octombrie 2011 de instituire a Agenției Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (JO L 286, 1.11.2011, p. 1).

(13) SIS ar trebui să conțină categorii suplimentare de date pentru a permite utilizatorilor finali să ia decizii în cunoștință de cauză pe baza unei semnalări, fără a pierde timp. Prin urmare, pentru a facilita identificarea persoanelor și pentru a depista identitățile multiple, categoriile de date referitoare la persoane ar trebui să includă o trimitere la documentul de identificare personal sau la numărul de identificare personal și o copie a documentului respectiv, în cazul în care sunt disponibile.

(13A) În cazul în care sunt disponibile, ar trebui introduse toate datele relevante, în special prenumele, atunci când se creează o semnalare, pentru a se reduce la minimum riscul de rezultate pozitive false și activitățile operaționale inutile.

(14) SIS nu ar trebui să stocheze datele utilizate pentru efectuarea de căutări, cu excepția păstrării înregistrărilor cu scopul de a verifica dacă respectiva căutare este legală, de a monitoriza legalitatea prelucrării datelor, de a efectua automonitorizarea și de a asigura funcționarea corespunzătoare a N.SIS, precum și integritatea și securitatea datelor.

(15) SIS ar trebui să permită prelucrarea datelor biometrice pentru a facilita identificarea fiabilă a persoanelor în cauză. În această privință, SIS ar trebui să permită și prelucrarea datelor privind persoanele a căror identitate a fost uzurpată (pentru a se evita inconveniente cauzate de identificarea eronată a acestora), sub rezerva unor garanții adecvate, în special cu acordul persoanei în cauză și cu o limitare strictă a scopurilor în care aceste date pot fi prelucrate în mod legal.

- (16) Statele membre ar trebui să ia măsurile tehnice necesare astfel încât de fiecare dată când utilizatorii finali au dreptul de a efectua o căutare într-o bază de date națională a poliției sau în materie de imigrație, aceștia să efectueze în paralel și căutări în SIS, în conformitate cu articolul 4 din Directiva (UE) 2016/680 a Parlamentului European și a Consiliului¹⁰. Astfel ar trebui să se garanteze că SIS funcționează ca principală măsură compensatorie în spațiul fără controale la frontierele interne și să se abordeze mai bine dimensiunea transfrontalieră a criminalității și mobilitatea infractorilor.
- (17) Prezentul regulament ar trebui să prevadă condițiile de utilizare a datelor dactiloscopice și a imaginilor faciale în scopul identificării. Utilizarea în SIS a imaginilor faciale în scopul identificării ar trebui, **mai ales** [...], să contribuie la asigurarea coerenței în cadrul procedurilor de control la frontiere în cazul în care sunt necesare identificarea și verificarea identității cu ajutorul **datelor dactiloscopice** [...] și al imaginilor faciale. Efectuarea de căutări prin utilizarea datelor dactiloscopice ar trebui să fie obligatorie în cazul în care există vreo îndoială privind identitatea unei persoane. [...]

¹⁰ Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmării penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (JO L 119, 4.5.2016, p. 89).

(18) Introducerea unui sistem automat de identificare a amprentelor digitale în cadrul SIS completează mecanismul Prüm existent privind accesul online transfrontalier reciproc la bazele naționale de date ADN și la sistemele naționale automate de identificare a amprentelor digitale desemnate¹¹. Mecanismul Prüm permite interconectarea sistemelor naționale de identificare a amprentelor digitale, un stat membru putând astfel să introducă o cerere pentru a verifica dacă autorul unei infracțiuni ale cărei amprente digitale au fost găsite este cunoscut în orice alt stat membru. Mecanismul Prüm verifică doar dacă persoana căreia îi aparțin respectivele amprente digitale este cunoscută la un anumit moment. Prin urmare, dacă autorul unei infracțiuni va fi cunoscut ulterior în oricare dintre statele membre, acesta nu va fi neapărat reținut. Căutarea în SIS prin utilizarea amprentelor digitale permite o căutare activă a autorului unei infracțiuni. Prin urmare, ar trebui să fie posibil să se încarce în SIS amprente digitale ale unui autor necunoscut al unei infracțiuni, cu condiția ca persoana căreia îi aparțin respectivele amprente digitale să poată fi identificată cu un grad ridicat de probabilitate ca autor al unei infracțiuni grave sau al unui act de terorism. Acest lucru este valabil în special în cazul în care amprente digitale sunt găsite pe o armă sau pe orice obiect utilizat la comiterea infracțiunii. Simpla prezență a amprentelor digitale la locul infracțiunii nu ar trebui considerată ca indicând cu un grad ridicat de probabilitate că amprente digitale aparțin autorului acesteia. O altă condiție prealabilă pentru crearea unei astfel de semnalări ar trebui să fie aceea ca identitatea autorului infracțiunii să nu poată fi stabilită prin intermediul niciunei alte baze de date naționale, europene sau internaționale. Dacă în urma căutării prin utilizarea amprentelor digitale se identifică o potențială corespondență, statul membru ar trebui să efectueze verificări suplimentare prin utilizarea respectivelor amprente digitale, [...] cu **participarea** experților din domeniul dactiloscopic, pentru a stabili dacă amprente stocate în SIS aparțin respectivei persoane, trebuind de asemenea să îi stabilească identitatea. Procedurile ar trebui să fie reglementate de dreptul național. O identificare în SIS a unei „persoane căutate necunoscute” ca fiind persoana căreia îi aparțin respectivele amprente digitale poate contribui în mod substanțial la investigație și poate duce la arestare, sub rezerva îndeplinirii tuturor condițiilor în vederea arestării.

¹¹ Decizia 2008/615/JAI a Consiliului din 23 iunie 2008 privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere (JO L 210, 6.8.2008, p. 1) și Decizia 2008/616/JAI a Consiliului din 23 iunie 2008 privind punerea în aplicare a Deciziei 2008/615/JAI privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere (JO L 210, 6.8.2008, p. 12).

- (19) Ampretele digitale **sau ampretele palmare** găsite la locul unei infracțiuni ar trebui să poată fi verificate prin consultarea **datelor dactiloscopice** [...] stocate în SIS, dacă se poate stabili cu un grad ridicat de probabilitate că aparțin autorului unei infracțiuni grave sau al unei infracțiuni de terorism. **Ar trebui să se acorde o atenție deosebită stabilirii unor standarde de calitate aplicabile în cazul stocării datelor biometrice, inclusiv a datelor dactiloscopice latente.** Infracțiunile grave ar trebui să fie infracțiunile enumerate în Decizia-cadru 2002/584/JAI a Consiliului¹² și „infracțiunile de terorism” ar trebui să fie infracțiunile [...] **care corespund sau sunt echivalente uneia dintre infracțiunile** menționate în **Directiva (UE) 2017/541**¹³ [...] ¹⁴.
- (20) În cazurile în care datele dactiloscopice, **fotografiile sau imaginile faciale** nu sunt disponibile, ar trebui să fie posibil să se adauge un profil ADN care să fie accesibil doar utilizatorilor autorizați. Profilurile ADN ar trebui să faciliteze identificarea persoanelor dispărute care au nevoie de protecție, în special a copiilor dispăruți, inclusiv prin autorizarea utilizării profilurilor ADN ale **ascendenților, descendenților** [...] sau ale fraților ori surorilor pentru a se putea efectua identificarea. Datele ADN nu ar trebui să conțină trimeri la originea rasială.
- (20A) Ar trebui să fie posibil în toate cazurile să se identifice o persoană prin utilizarea datelor dactiloscopice. Atunci când identitatea unei persoane nu poate fi stabilită prin niciun alt mijloc, ar trebui să se utilizeze datele dactiloscopice în încercarea de a se stabili identitatea.**
- (20B) Profilurile ADN nu ar trebui extrase din SIS decât în cazul în care identificarea este necesară și proporțională în sensul articolului 32 alineatul (2) literele (a) și (c). Profilurile ADN nu ar trebui extrase și prelucrate în niciun alt scop decât scopul în care au fost introduse în conformitate cu articolul 32 alineatul (2) literele (a) și (c). Aplicând normele de protecție a datelor și normele de securitate prevăzute în prezentul regulament, ar trebui introduse, dacă este necesar, garanții suplimentare atunci când se utilizează profilurile ADN, pentru a se preîntâmpina riscul de corespondențe false, de piraterie informatică și de partajare neautorizată cu părți terțe.**

¹² Decizia-cadru 2002/584/JAI a Consiliului din 13 iunie 2002 privind mandatul european de arestare și procedurile de predare între statele membre (JO L 190, 18.7.2002, p. 1).

¹³ Directiva (UE) 2017/541 a Parlamentului European și a Consiliului din 15 martie 2017 privind combaterea terorismului și de înlocuire a Deciziei-cadru 2002/475/JAI a Consiliului și de modificare a Deciziei 2005/671/JAI a Consiliului (JO L 88, 31.3.2017, p. 6).

¹⁴ [...]

- (21) SIS ar trebui să conțină semnalări privind persoane căutate în vederea arestării în scopul predării și al extrădării. În afară de semnalări, este oportun să se asigure, **prin intermediul birourilor SIRENE**, schimbul de informații suplimentare care sunt necesare pentru procedurile de predare și de extrădare. În special, în SIS ar trebui să se prelucreze datele menționate la articolul 8 din Decizia-cadru 2002/584/JAI a Consiliului din 13 iunie 2002 privind mandatul european de arestare și procedurile de predare între statele membre¹⁵. Din motive operaționale, este oportun ca statul membru emitent, cu autorizația autorităților judiciare, să suspende temporar disponibilitatea unei semnalări în vederea arestării atunci când o persoană care face obiectul unui mandat european de arestare este căutată în mod intens și activ, iar utilizatorii finali care nu sunt implicați în operațiunea de căutare concretă pot pune în pericol succesul acesteia. Indisponibilitatea temporară a acestor semnalări nu ar trebui, **în principiu**, să depășească 48 de ore.
- (22) Ar trebui să fie posibil să se adauge în SIS o traducere a datelor suplimentare introduse în scopul predării în temeiul mandatului european de arestare și în scopul extrădării.
- (23) SIS ar trebui să conțină semnalări privind persoane dispărute **sau vulnerabile** pentru a se asigura protecția acestora sau pentru a se preîntâmpina amenințările pentru siguranța publică. Ar trebui să se limiteze emiterea în SIS a semnalărilor privind copiii expuși riscului de răpire (adică pentru a preîntâmpina un prejudiciu viitor care nu s-a produs încă, așa cum se întâmplă în cazul copiilor expuși riscului de a fi răpiți de către unul dintre părinți), fiind deci oportun să se prevadă garanții [...] corespunzătoare. În cazul copiilor, aceste semnalări și procedurile corespunzătoare ar trebui să servească interesul superior al copilului, având în vedere articolul 24 din Carta drepturilor fundamentale a Uniunii Europene și Convenția Organizației Națiunilor Unite cu privire la drepturile copilului din 20 noiembrie 1989.
- (23A) Semnalările privind copiii expuși riscului de răpire ar trebui introduse în SIS la cererea autorităților competente, inclusiv a autorităților judiciare competente în materia răspunderii părintești, în conformitate cu dreptul național.**

¹⁵ Decizia-cadru 2002/584/JAI a Consiliului din 13 iunie 2002 privind mandatul european de arestare și procedurile de predare între statele membre (JO L 190, 18.7.2002, p. 1).

- (23B) Semnalările privind persoanele vulnerabile care trebuie împiedicate să călătorească pentru propria lor protecție ar trebui introduse, de exemplu, atunci când se consideră că efectuarea călătoriei ar crea riscul căsătoriei fortate, al mutilării genitale feminine, al traficului de persoane sau, în cazul copiilor, al implicării în conflictele armate ori al aderării la grupuri infracționale organizate sau la grupuri teroriste.**
- (24) Pentru cazurile în care există suspiciuni legate de terorism și de infracțiuni grave, ar trebui să se includă o nouă acțiune care să permită [...] **interogarea** unei persoane care este suspectată că a comis o infracțiune gravă sau despre care există motive să se creadă că va comite o infracțiune gravă [...],[...] **sub rezerva dreptului național**, pentru a se furniza informații cât mai detaliate posibil statului membru emitent. Această nouă acțiune **care trebuie să se deruleze în timpul verificărilor polițienești și la frontieră** nu ar trebui să implice nici percheziționarea, nici arestarea respectivei persoane, **iar drepturile procedurale ale persoanei ar trebui menținute. De asemenea, ea nu aduce atingere mecanismelor de asistență judiciară reciprocă existente.** Ar trebui totuși să furnizeze suficiente informații pentru ca **autoritățile de emiteră a semnalării și autoritățile de executare** să decidă **între ele, pe cât posibil în timp real**, asupra unor acțiuni suplimentare. Infracțiunile grave ar trebui să fie infracțiunile enumerate în Decizia-cadru 2002/584/JAI a Consiliului.
- (24A) În cazul semnalărilor privind obiecte căutate pentru a fi confiscate sau folosite ca probe în cadrul unor proceduri penale, obiectele ar trebui în principiu să se confişte. Cu toate acestea, dreptul național stabileşte dacă se confiscă un obiect și conform căror condiții, mai ales dacă se află în posesia proprietarului său de drept.**
- (25) SIS ar trebui să conțină noi categorii de obiecte de valoare ridicată, cum ar fi **produse din domeniul tehnologiei informației** [...] care pot fi identificate și care pot face obiectul unei căutări printr-un număr unic.

- (25A) În ceea ce privește documentele de introdus în scopul confiscării sau al folosirii ca probe în cadrul unor proceduri penale, termenul „fals” ar trebui înțeles ca referindu-se atât la documentele falsificate, cât și la cele contrafăcute.**
- (26) Ar trebui să fie posibil ca un stat membru să aplice unei semnalări o mențiune, denumită „indicator de validitate”, care să arate că acțiunea care trebuie întreprinsă pe baza semnalării nu va fi întreprinsă pe teritoriul său. În cazul în care semnalările sunt emise în vederea arestării în scopul predării, nicio dispoziție a prezentului regulament nu ar trebui interpretată pentru a deroga de la dispozițiile Deciziei-cadru 2002/584/JAI sau pentru a împiedica aplicarea acestora. Decizia de a adăuga un indicator de validitate unei semnalări **în scopul neexecutării unui mandat european de arestare** ar trebui să se bazeze numai pe motivele de refuz prevăzute în decizia-cadru menționată.
- (27) În cazul în care s-a adăugat un indicator de validitate și se identifică locul în care se află persoana căutată pentru a fi arestată în vederea predării, acest loc ar trebui comunicat întotdeauna autorității judiciare emitente, care poate decide transmiterea unui mandat european de arestare autorității judiciare competente în conformitate cu dispozițiile Deciziei-cadru 2002/584/JAI.
- (28) Statele membre ar trebui să poată stabili legături între semnalările din SIS. Stabilirea de către un stat membru a unor legături între două sau mai multe semnalări nu ar trebui să aibă efect asupra acțiunii care trebuie întreprinsă, asupra perioadei de păstrare a semnalărilor sau asupra drepturilor de acces la semnalări.

(29) Semnalările nu ar trebui păstrate în SIS mai mult timp decât este necesar în vederea îndeplinirii scopurilor în care au fost emise. În vederea reducerii sarcinii administrative suportate de diversele autorități implicate în prelucrarea datelor privind persoane în diferite scopuri, este oportun să se alinieze perioada de păstrare a semnalărilor privind persoane la perioadele de păstrare prevăzute pentru returnare și cazurile de ședere ilegală. În plus, statele membre extind periodic termenul de expirare a valabilității semnalărilor privind persoane dacă acțiunea necesară nu a putut fi întreprinsă în perioada prevăzută inițial. Prin urmare, perioada de păstrare a semnalărilor privind persoane ar trebui să fie de maximum cinci ani. Ca principiu general, semnalările privind persoane ar trebui șterse automat din SIS după o perioadă de cinci ani, cu excepția semnalărilor emise în scopul efectuării de controale discrete, de verificări prin interviu sau de controale specifice. Acestea ar trebui șterse după un an. Semnalările privind obiecte [...] ar trebui șterse automat din SIS după o perioadă de **zece** [...] ani, deoarece după scurgerea acestei perioade probabilitatea de a găsi obiectele respective este foarte redusă și valoarea lor economică a scăzut în mod semnificativ. **Atunci când sunt legate de semnalări privind persoane** [...], semnalările privind **obiecte nu** ar trebui să fie păstrate **mai mult timp decât semnalările privind persoane de care sunt legate și în niciun caz pe o perioadă mai mare de cinci** [...] ani. Deciziile de a păstra semnalări privind persoane ar trebui să se bazeze pe o evaluare individuală cuprinzătoare. Statele membre ar trebui să reexamineze semnalările privind persoane **și obiecte** la intervale [...] periodice [...] și să întocmească statistici referitoare la numărul de semnalări [...] în cazul cărora care s-a prelungit perioada de păstrare.

- (30) Introducerea și prelungirea datei de expirare a valabilității unei semnalări din SIS ar trebui să facă obiectul cerinței de proporționalitate necesare, examinându-se dacă un caz concret este suficient de adecvat, relevant și important pentru a se introduce o semnalare în SIS.
- Infraacțiunile prevăzute la articolele **3-14 din Directiva (UE) 2017/541** ¹⁶ [...] ¹⁷ reprezintă o amenințare foarte gravă pentru siguranța publică și integritatea vieții persoanelor și pentru societate, iar aceste infracțiuni sunt extrem de dificil de prevenit, de depistat și de investigat într-un spațiu fără controale la frontierele interne în care potențialii infractori circulă liber. În cazul în care se caută o persoană sau un obiect în legătură cu aceste infracțiuni, este [...] necesar să se creeze în SIS o semnalare corespunzătoare privind persoane căutate în vederea unei proceduri judiciare penale, privind persoane sau obiecte care fac obiectul unor controale discrete, al unor verificări prin interviu sau al unor controale specifice, precum și privind obiecte căutate în vederea confiscării, deoarece niciun alt mijloc nu ar fi la fel de eficace în acest scop. **În mod excepțional, statele membre se pot abține de la crearea unei semnalări atunci când aceasta este de natură să obstrucționeze cercetările, investigațiile sau procedurile oficiale ori juridice legate de siguranța publică sau de securitatea națională.**
- (31) Este necesar să se prevadă dispoziții clare în ceea ce privește ștergerea semnalărilor. O semnalare ar trebui să fie păstrată numai pe durata necesară îndeplinirii scopului în care a fost introdusă. Având în vedere practicile divergente ale statelor membre privind definirea momentului în care o semnalare își îndeplinește scopul, este oportun să se prevadă criterii detaliate pentru fiecare categorie de semnalări în scopul de a stabili momentul în care acestea ar trebui să fie șterse din SIS.
- (32) Integritatea datelor din SIS are o importanță majoră. Prin urmare, ar trebui prevăzute garanții corespunzătoare pentru prelucrarea datelor din SIS atât la nivel central, cât și la nivel național, în vederea asigurării securității datelor de la un capăt la altul. Autoritățile implicate în prelucrarea datelor ar trebui să respecte cerințele de securitate prevăzute în prezentul regulament și să aplice o procedură uniformă de raportare a incidentelor.

¹⁶ Directiva (UE) 2017/541 a Parlamentului European și a Consiliului din 15 martie 2017 privind combaterea terorismului și de înlocuire a Deciziei-cadru 2002/475/JAI a Consiliului și de modificare a Deciziei 2005/671/JAI a Consiliului (JO L 88, 31.3.2017, p. 6).

¹⁷ [...]

- (33) Datele prelucrate în SIS în conformitate cu prezentul regulament nu ar trebui să fie transferate sau puse la dispoziția țărilor terțe sau a organizațiilor internaționale. [...]
- (34) Este oportun să se acorde acces la SIS autorităților responsabile cu înmatricularea vehiculelor, a ambarcațiunilor și a aeronavelor pentru a le permite să verifice dacă mijlocul de transport este căutat deja într-un stat membru pentru a fi confiscat sau verificat. [...] ¹⁸
 [...] ¹⁹

(34A) Este oportun să se acorde acces la SIS autorităților responsabile cu înregistrarea armelor de foc pentru a le permite să verifice dacă arma de foc este căutată deja într-un stat membru pentru a fi confiscată sau verificată sau dacă există o semnalare privind persoana care solicită înregistrarea.

¹⁸ [...]

¹⁹ Mutat la considerentul 34B.

(34B)²⁰ Ar trebui să li se acorde acces direct autorităților care sunt servicii publice. Acest acces ar trebui să se limiteze la semnalările privind respectivele mijloace de transport și certificatul ori plăcuța lor de înmatriculare sau privind armele de foc și persoanele care solicită înregistrarea. În consecință, dispozițiile Regulamentului (CE) nr. 1986/2006 al Parlamentului European și al Consiliului²¹ ar trebui să fie incluse în prezentul regulament, iar regulamentul menționat ar trebui abrogat. Orice rezultat pozitiv în SIS trebuie raportat de autoritățile sus-menționate organelor de poliție în scopul unor proceduri suplimentare în conformitate cu semnalarea specifică din SIS, precum și pentru notificarea rezultatului pozitiv statului membru emitent prin intermediul birourilor SIRENE.

- (35) În ceea ce privește prelucrarea datelor de către autoritățile naționale competente în scopul prevenirii, al investigării și al depistării infracțiunilor grave sau al infracțiunilor de terorism ori al urmăririi penale a infracțiunilor și al executării pedepselor, inclusiv garanțiile de asigurare a prevenirii amenințărilor pentru siguranța publică, ar trebui să se aplice dispozițiile naționale de transpunere a Directivei (UE) 2016/680. Dispozițiile Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului²² și ale Directivei (UE) 2016/680 ar trebui detaliate în prezentul regulament, dacă este necesar.
- (36) Regulamentul (UE) 2016/679 ar trebui să se aplice prelucrării datelor cu caracter personal în temeiul prezentului regulament de către autoritățile naționale atunci când nu se aplică Directiva (UE) 2016/680. Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului²³ ar trebui să se aplice prelucrării datelor cu caracter personal de către instituțiile și organele Uniunii atunci când își exercită responsabilitățile care le revin în temeiul prezentului regulament.

²⁰ Mutat parțial de la considerentul (34).

²¹ Regulamentul (CE) nr. 1986/2006 al Parlamentului European și al Consiliului din 20 decembrie 2006 privind accesul la Sistemul de Informații Schengen din a doua generație (SIS II) al serviciilor competente, în statele membre, pentru eliberarea certificatelor de înmatriculare a vehiculelor (JO L 381, 28.12.2006, p. 1).

²² Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

²³ Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date (JO L 8, 12.1.2001, p. 1).

- (37) Dispozițiile Directivei (UE) 2016/680, ale Regulamentului (UE) 2016/679 și ale Regulamentului (CE) nr. 45/2001 ar trebui să fie detaliate în prezentul regulament, în cazul în care este necesar. În ceea ce privește prelucrarea datelor cu caracter personal de către Europol, se aplică Regulamentul (UE) 2016/794 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Regulamentul privind Europolul)²⁴. **În ceea ce privește prelucrarea datelor cu caracter personal de către Eurojust, se aplică Decizia 2002/187.**
- (38) În cazul prelucrării datelor din SIS de către Eurojust se aplică dispozițiile privind protecția datelor prevăzute în Decizia 2002/187/JAI din 28 februarie 2002²⁵ de instituire a Eurojust în scopul consolidării luptei împotriva formelor grave de criminalitate, inclusiv cele privind competențele organului de control comun, înființat în temeiul deciziei menționate, de a monitoriza activitățile Eurojustului și cele privind răspunderea pentru orice prelucrare ilegală a datelor cu caracter personal de către Eurojust. În cazurile în care căutările efectuate în SIS de Eurojust indică existența unei semnalări emise de un stat membru, Eurojust nu poate întreprinde acțiunea necesară. Prin urmare, acesta ar trebui să informeze statul membru în cauză care să îl autorizeze să se ocupe de caz.
- (39) În ceea ce privește confidențialitatea, funcționarii sau alți agenți care sunt angajați și își desfășoară activitatea în legătură cu SIS ar trebui să se supună dispozițiilor corespunzătoare din Statutul funcționarilor Uniunii Europene și din Regimul aplicabil celorlalți agenți ai Uniunii Europene.
- (40) Atât statele membre, cât și agenția ar trebui să dispună de planuri de securitate pentru a facilita punerea în aplicare a obligațiilor privind securitatea și ar trebui să coopereze pentru a aborda aspectele legate de securitate dintr-o perspectivă comună.
- (41) Autoritățile naționale independente de supraveghere ar trebui să monitorizeze legalitatea prelucrării datelor cu caracter personal în legătură cu prezentul regulament de către statele membre. Ar trebui să se stabilească drepturile persoanelor vizate de acces, rectificare și ștergere a datelor lor cu caracter personal stocate în SIS și căile de atac ulterioare în fața instanțelor judecătorești naționale, precum și recunoașterea reciprocă a hotărârilor judecătorești. Prin urmare, este oportun să se solicite statistici anuale din partea statelor membre.

²⁴ Regulamentul (UE) 2016/794 al Parlamentului European și al Consiliului din 11 mai 2016 privind Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) și de înlocuire și de abrogare a Deciziilor 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI și 2009/968/JAI ale Consiliului (JO L 135, 25.5.2016, p. 53).

²⁵ Decizia 2002/187/JAI a Consiliului din 28 februarie 2002 de instituire a Eurojust în scopul consolidării luptei împotriva formelor grave de criminalitate (JO L 63, 6.3.2002, p. 1).

- (42) Autoritățile naționale de supraveghere ar trebui să se asigure că cel puțin din patru în patru ani se efectuează un audit al operațiunilor de prelucrare a datelor în sistemul lor N.SIS în conformitate cu standardele internaționale de audit. Auditul ar trebui să fie efectuat de autoritățile de supraveghere sau autoritățile naționale de supraveghere ar trebui să dispună în mod direct efectuarea auditului de către un auditor independent în materie de protecție a datelor. Auditorul independent ar trebui să rămână sub controlul și responsabilitatea autorității sau autorităților naționale de supraveghere care ar trebui prin urmare să dispună auditul și să definească în mod clar scopul, domeniul de aplicare și metodologia auditului, precum și să ofere îndrumări și să asigure supravegherea auditului și a rezultatelor finale ale acestuia.
- (43) Regulamentul (UE) 2016/794 (Regulamentul privind Europol) prevede că Europol susține și consolidează acțiunile întreprinse de autoritățile competente ale statelor membre și cooperarea acestora în vederea combaterii terorismului și a altor forme grave de criminalitate și furnizează analize și evaluări ale amenințărilor. Extinderea drepturilor de acces ale Europolului la semnalările din SIS privind persoane dispărute ar trebui să îmbunătățească și mai mult capacitatea acestuia de a furniza autorităților naționale de aplicare a legii produse operaționale și analitice cuprinzătoare privind traficul de persoane și exploatarea sexuală a copiilor, inclusiv în mediul online. Extinderea ar contribui la o mai bună prevenire a acestor infracțiuni, la protecția potențialelor victime și la investigarea autorilor infracțiunilor. Centrul european de combatere a criminalității informatice din cadrul Europolului ar beneficia la rândul său de noul acces acordat Europolului la semnalările din SIS privind persoane dispărute, inclusiv în cazurile autorilor itineranți ai unor infracțiuni sexuale și în cele de abuz sexual asupra copiilor în mediul online, în care autorii susțin adeseori că au acces sau pot avea acces la copii care ar putea să fi fost înregistrați ca dispăruți. [...]

- (44) Pentru a elimina lacunele în privința schimbului de informații privind terorismul, mai ales privind luptătorii teroriști străini, ale căror deplasări este extrem de important să fie monitorizate, statele membre [...] **pot** face schimb de informații privind activitățile legate de terorism cu Europolul [...] **atunci când** introduc o semnalare în SIS, precum și privind rezultatele pozitive și informațiile conexe. **Acest schimb de informații ar trebui să se desfășoare sub forma unui schimb de informații suplimentare cu Europolul cu privire la semnalările corespunzătoare. În acest scop, Europolul ar trebui să creeze o conexiune cu infrastructura de comunicații SIRENE.** Acest lucru ar trebui să permită Centrului european de combatere a terorismului din cadrul Europolului să verifice dacă în bazele de date ale Europolului există informații contextuale suplimentare și să furnizeze analize de înaltă calitate care să contribuie la destrămarea rețelelor teroriste și, dacă este posibil, la preîntâmpinarea atacurilor acestora.
- (45) Este necesar, de asemenea, să se stabilească norme clare privind prelucrarea și descărcarea datelor din SIS de către Europol pentru a se permite o utilizare cât mai cuprinzătoare a SIS, cu condiția ca standardele de protecție a datelor să fie respectate, astfel cum se prevede în prezentul regulament și în Regulamentul (UE) 2016/794. În cazurile în care căutările efectuate în SIS de Europol indică existența unei semnalări emise de un stat membru, Europolul nu poate întreprinde acțiunea necesară. Prin urmare, acesta ar trebui să informeze statul membru în cauză **printr-un schimb de informații suplimentare cu biroul SIRENE corespunzător** permițându-i astfel să se ocupe de caz.

(46) Regulamentul (UE) 2016/1624 al Parlamentului European și al Consiliului²⁶ prevede, în sensul prezentului regulament, că statul membru gazdă îi autorizează pe membrii echipelor europene de poliție de frontieră și gardă de coastă sau ai echipelor formate din personalul implicat în sarcini legate de returnare, trimise de Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă, să consulte bazele de date europene, în cazul în care această consultare este necesară pentru îndeplinirea obiectivelor operative specificate în planul operativ privind verificările la frontieră, supravegherea frontierelor și returnare. Alte agenții relevante ale Uniunii, în special Biroul European de Sprijin pentru Azil și Europolul, pot, de asemenea, să trimită în cadrul echipelor de sprijin pentru gestionarea migrației experți care nu sunt membri ai personalului respectivelor agenții ale Uniunii. Obiectivul trimiterii echipelor europene de poliție de frontieră și gardă de coastă, a echipelor formate din personalul implicat în sarcini legate de returnare și a echipelor de sprijin pentru gestionarea migrației este de a oferi întăriri tehnice și operative statelor membre solicitante, în special celor care se confruntă cu provocări disproporționate legate de migrație. În vederea îndeplinirii sarcinilor atribuite echipelor europene de poliție de frontieră și gardă de coastă, echipelor formate din personalul implicat în sarcini legate de returnare și echipelor de sprijin pentru gestionarea migrației este necesar accesul la SIS prin intermediul unei interfețe tehnice a Agenției Europene pentru Poliția de Frontieră și Garda de Coastă care să se conecteze la SIS central. În cazul în care căutările efectuate în SIS de echipa sau de echipele de personal indică existența unei semnalări emise de un stat membru, membrul echipei sau personalul nu poate întreprinde acțiunea necesară, cu excepția cazului în care este autorizat în acest sens de statul membru gazdă. Prin urmare, acesta ar trebui să informeze statul membru **gazdă** [...] permițându-i astfel să se ocupe de caz. **Statul membru gazdă ar trebui să notifice rezultatul pozitiv statului membru emitent printr-un schimb de informații suplimentare.**

²⁶ Regulamentul (UE) 2016/1624 al Parlamentului European și al Consiliului din 14 septembrie 2016 privind Poliția de frontieră și garda de coastă la nivel european și de modificare a Regulamentului (UE) 2016/399 al Parlamentului European și al Consiliului și de abrogare a Regulamentului (CE) nr. 863/2007 al Parlamentului European și al Consiliului, a Regulamentului (CE) nr. 2007/2004 al Consiliului și a Deciziei 2005/267/CE a Consiliului (JO L 251, 16.9.2016, p. 1).

- (47) În conformitate cu propunerea Comisiei de regulament al Parlamentului European și al Consiliului de instituire a Sistemului european de informații și de autorizare privind călătoriile (ETIAS)²⁷, unitatea centrală a ETIAS din cadrul Agenției Europene pentru Poliția de Frontieră și Garda de Coastă va efectua verificări în SIS prin intermediul ETIAS pentru a analiza cererile de autorizații de călătorie în cazul cărora este necesar, printre altele, să se stabilească dacă resortisantul unei țări terțe care solicită o autorizație de călătorie face obiectul unei semnalări în SIS. În acest scop, unitatea centrală a ETIAS din cadrul Agenției Europene pentru Poliția de Frontieră și Garda de Coastă ar trebui să aibă de asemenea acces la SIS în măsura necesară pentru îndeplinirea mandatului său, și anume la toate categoriile de semnalări privind persoane și la semnalările privind documente de identificare personale în alb sau eliberate.
- (48) Dată fiind natura lor tehnică, gradul lor de detaliu și necesitatea de a fi actualizate în mod regulat, anumite aspecte ale SIS nu pot fi reglementate în mod exhaustiv prin dispozițiile prezentului regulament. Printre acestea se numără, de exemplu, normele tehnice privind introducerea, actualizarea, ștergerea datelor și efectuarea de căutări în acestea, calitatea datelor și normele de căutare referitoare la **datele** biometrice [...], normele privind compatibilitatea și prioritatea semnalărilor, [...] legăturile dintre semnalări, specificarea noilor categorii de obiecte din cadrul categoriei echipamentelor tehnice și electronice, stabilirea datei de expirare a valabilității semnalărilor în limitele termenului maxim și schimbul de informații suplimentare. Prin urmare, ar trebui să i se confere Comisiei competențe de executare cu privire la aceste aspecte. Normele tehnice privind efectuarea de căutări în semnalări ar trebui să ia în considerare buna funcționare a aplicațiilor naționale.
- (49) Pentru a se asigura condiții uniforme de punere în aplicare a prezentului regulament, ar trebui să i se confere Comisiei competențe de executare. Aceste competențe ar trebui exercitate în conformitate cu **articolul 5 din** Regulamentul (UE) nr. 182/2011²⁸. Procedura de adoptare a măsurilor de punere în aplicare în temeiul prezentului regulament și al Regulamentului (UE) 2018/xxx (verificări la frontiere) ar trebui să fie aceeași.

²⁷ Documentul COM(2016) 731 final.

²⁸ Regulamentul (UE) nr.182/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 de stabilire a normelor și principiilor generale privind mecanismele de control de către statele membre al exercitării competențelor de executare de către Comisie (JO L 55, 28.2.2011, p. 13).

- (50) Pentru a se asigura transparența, agenția ar trebui să întocmească din doi în doi ani un raport privind funcționarea tehnică a SIS central și funcționarea infrastructurii de comunicații, inclusiv securitatea acesteia, precum și privind schimbul **bilateral și multilateral** de informații suplimentare. Comisia ar trebui să efectueze o evaluare globală din patru în patru ani.
- (51) Întrucât obiectivele prezentului regulament, și anume instituirea și reglementarea unui sistem de informații comun și schimbul de informații suplimentare conexe, nu pot, prin însăși natura lor, să fie realizate în mod satisfăcător de statele membre și, în consecință, pot fi realizate mai bine la nivelul Uniunii, aceasta poate adopta măsuri, în conformitate cu principiul subsidiarității, astfel cum este prevăzut la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, astfel cum este enunțat la articolul respectiv, prezentul regulament nu depășește ceea ce este necesar pentru atingerea acestor obiective.
- (52) Prezentul regulament respectă drepturile fundamentale și principiile recunoscute în special în Carta drepturilor fundamentale a Uniunii Europene. În special, prezentul regulament vizează să asigure un mediu sigur pentru toate persoanele care locuiesc pe teritoriul Uniunii Europene și o protecție specială pentru copiii care ar putea cădea victimă traficului de persoane sau răpirii de către unul dintre părinți, respectând în același timp pe deplin protecția datelor cu caracter personal.
- (53) În conformitate cu articolele 1 și 2 din Protocolul nr. 22 privind poziția Danemarcei, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, Danemarca nu participă la adoptarea prezentului regulament, nu are obligații în temeiul acestuia și acesta nu i se aplică. Deoarece prezentul regulament constituie o dezvoltare a acquis-ului Schengen, Danemarca decide, în conformitate cu articolul 4 din protocolul respectiv, în termen de șase luni de la data la care Consiliul decide cu privire la prezentul regulament dacă îl va pune în aplicare în legislația sa națională.

- (54) Regatul Unit participă la prezentul regulament, în conformitate cu articolul 5 **alineatul (1)** din [...] Protocolul **nr. 19** privind acquis-ul Schengen integrat în cadrul Uniunii Europene, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, și cu articolul 8 alineatul (2) din Decizia 2000/365/CE a Consiliului [...] ²⁹.
- (55) Irlanda participă la prezentul regulament, în conformitate cu articolul 5 din [...] Protocolul **nr. 19** privind acquis-ul Schengen integrat în cadrul Uniunii Europene, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, și cu articolul 6 alineatul (2) din Decizia 2002/192/[...] a Consiliului ³⁰.
- (56) În ceea ce privește Islanda și Norvegia, prezentul regulament constituie o dezvoltare a dispozițiilor acquis-ului Schengen în înțelesul Acordului încheiat între Consiliul Uniunii Europene și Republica Islanda și Regatul Norvegiei în ceea ce privește asocierea acestor două state la punerea în aplicare, asigurarea respectării și dezvoltarea acquis-ului Schengen ³¹, care se află sub incidența articolului 1 punctul G din Decizia 1999/437/CE a Consiliului ³² privind anumite modalități de aplicare a acordului respectiv.

²⁹ [...]

³⁰ [...]

³¹ JO L 176, 10.7.1999, p. 36.

³² JO L 176, 10.7.1999, p. 31.

(57) În ceea ce privește Elveția, prezentul regulament constituie o dezvoltare a dispozițiilor acquis-ului Schengen în înțelesul Acordului [...] între Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană privind asocierea Confederației Elvețiene la punerea în aplicare, asigurarea respectării și dezvoltarea acquis-ului Schengen, care se află sub incidența articolului 1 punctul G din Decizia 1999/437/CE a Consiliului, coroborat cu articolul [...] **3** din Decizia [...] ³³ [...] ³⁴ **2008/149/JAI** a Consiliului ³⁵.

³³ [...]

³⁴ [...]

³⁵ Decizia 2008/149/JAI a Consiliului din 28 ianuarie 2008 privind încheierea, în numele Uniunii Europene, a Acordului între Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană cu privire la asocierea Confederației Elvețiene la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen (JO L 53, 27.2.2008, p. 50).

- (58) În ceea ce privește Liechtensteinul, prezentul regulament constituie o dezvoltare a dispozițiilor acquis-ului Schengen în înțelesul Protocolului semnat între Uniunea Europeană, Comunitatea Europeană, Confederația Elvețiană și Principatul Liechtenstein cu privire la aderarea Principatului Liechtenstein la Acordul dintre Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană privind asocierea Confederației Elvețiene la punerea în aplicare, asigurarea respectării și dezvoltarea acquis-ului Schengen³⁶, care se află sub incidența articolului 1 punctul G din Decizia 1999/437/CE, coroborat cu articolul 3 din Decizia 2011/349/UE a Consiliului³⁷ [...]³⁸.
- (59) În ceea ce privește Bulgaria, [...] România **și Croatia**, prezentul regulament constituie un act care se întemeiază pe acquis-ul Schengen sau care se raportează la acesta în înțelesul articolului 4 alineatul (2) din Actul de aderare din 2005 **și, respectiv, al articolului 4 alineatul (2) din Actul de aderare din 2011 și** ar trebui coroborat cu Decizia 2010/365/UE a Consiliului privind aplicarea dispozițiilor acquis-ului Schengen referitoare la Sistemul de Informații Schengen în Republica Bulgaria și în România³⁹, **respectiv cu Decizia (UE) 2017/733 a Consiliului privind aplicarea dispozițiilor acquis-ului Schengen referitoare la Sistemul de Informații Schengen în Republica Croatia**⁴⁰.

³⁶ JO L 160, 18.6.2011, p. 21.

³⁷ Decizia 2011/349/UE a Consiliului din 7 martie 2011 privind încheierea, în numele Uniunii Europene, a Protocolului dintre Uniunea Europeană, Comunitatea Europeană, Confederația Elvețiană și Principatul Liechtenstein privind aderarea Principatului Liechtenstein la Acordul dintre Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană privind asocierea Confederației Elvețiene la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen, în special în ceea ce privește cooperarea judiciară în materie penală și cooperarea polițienească (JO L 160, 18.6.2011, p. 1).

³⁸ [...]

³⁹ JO L 166, 1.7.2010, p. 17.

⁴⁰ JO L 108, 26.4.2017, p. 31.

- (60) În ceea ce privește Ciprul [...], prezentul regulament constituie un act care se întemeiază pe acquis-ul Schengen sau care se raportează la acesta în înțelesul [...] articolului 3 alineatul (2) din Actul de aderare din 2003 [...].
- (61) Prezentul regulament ar trebui să se aplice Irlandei la date hotărâte în conformitate cu procedurile stabilite în instrumentele relevante privind aplicarea acquis-ului Schengen în cazul acestui stat.
- (62) [...] ⁴¹ [...]
- (63) Prin urmare, Decizia 2007/533/JAI a Consiliului și Decizia 2010/261/UE a Comisiei ⁴² ar trebui abrogate.
- (64) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 28 alineatul (2) din Regulamentul (CE) nr. 45/2001 și a emis un aviz la ...,

⁴¹ [...]

⁴² Decizia 2010/261/UE a Comisiei din 4 mai 2010 privind planul de securitate pentru SIS II central și infrastructura de comunicații (JO L 112, 5.5.2010, p. 31).

CAPITOLUL I

DISPOZIȚII GENERALE

Articolul 1

Scopul general al SIS

Obiectivul SIS este de a asigura un nivel ridicat de securitate în spațiul de libertate, securitate și justiție al Uniunii, inclusiv menținerea siguranței publice și a ordinii publice și garantarea securității pe teritoriile statelor membre, și de a [...] **asigura aplicarea** dispozițiilor părții a treia titlul V capitolul 4 și capitolul 5 din Tratatul privind funcționarea Uniunii Europene referitoare la circulația persoanelor pe teritoriile statelor membre, cu ajutorul informațiilor transmise prin intermediul acestui sistem.

Articolul 2

Domeniul de aplicare

- (1) Prezentul regulament stabilește condițiile și procedurile referitoare la introducerea și prelucrarea în SIS a semnalărilor privind persoane și obiecte, precum și la schimbul de informații suplimentare și date suplimentare în scopul cooperării judiciare și polițienești în materie penală.
- (2) Prezentul regulament stabilește, de asemenea, dispoziții privind arhitectura tehnică a SIS, responsabilitățile statelor membre și ale Agenției Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție, norme generale de prelucrare a datelor, precum și dispoziții privind drepturile persoanelor vizate și răspunderea.

Articolul 3

Definiții

- (1) În sensul prezentului regulament, se aplică următoarele definiții:
- (a) „semnalare” înseamnă un set de date, inclusiv, **dacă este cazul, date** biometrice [...] astfel cum sunt menționate la articolele 22 și 40, introduse în SIS, care permit autorităților competente să identifice o persoană sau un obiect în vederea întreprinderii unei acțiuni specifice;
- (b) „informații suplimentare” înseamnă informații care nu fac parte din datele semnalării stocate în SIS, dar au legătură cu semnalările din SIS, și care urmează a fi transmise **prin intermediul birourilor SIRENE** în cadrul unui schimb de informații:
- (1) pentru a permite statelor membre să se consulte sau să se informeze reciproc la introducerea unei semnalări;
 - (2) pentru a permite întreprinderea acțiunii corespunzătoare în urma obținerii unui rezultat pozitiv;
 - (3) în cazul în care nu se poate întreprinde acțiunea necesară;
 - (4) în ceea ce privește calitatea datelor din SIS;
 - (5) în ceea ce privește compatibilitatea și ordinea de prioritate a semnalărilor;
 - (6) în ceea ce privește drepturile de acces;
- (c) „date suplimentare” înseamnă datele stocate în SIS care au legătură cu semnalările din SIS și care trebuie să fie puse imediat la dispoziția autorităților competente în cazul în care o persoană cu privire la care s-au introdus date în SIS este localizată ca urmare a căutărilor efectuate în acest sistem;
- (d) „date cu caracter personal” înseamnă orice informații privind o persoană fizică identificată sau identificabilă („persoană vizată”);

- (e) „persoană fizică identificabilă” înseamnă o persoană fizică ce poate fi identificată, în mod direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare ori un element de identificare online, sau la unul ori mai multe elemente specifice identității fizice, fiziologice, genetice, mentale, economice, culturale sau sociale ale respectivei persoane fizice;
- (f) „prelucrare a datelor cu caracter personal” înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminare sau punere la dispoziție în alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;
- (g) [...] **„corespondentă”** [...] înseamnă **survenirea următoarelor etape:**
- (1) un utilizator **final** efectuează o căutare;
 - (2) căutarea indică o semnalare introdusă în SIS de un alt stat membru **și**
 - (3) datele privind semnalarea din SIS corespund datelor căutării. [...]

(ga) „rezultat pozitiv” înseamnă orice corespondentă care îndeplinește următoarele criterii:

(a) **a fost confirmată:**

(i) de către utilizatorul final sau,

(ii) în cazul în care corespondența în cauză s-a bazat pe compararea datelor biometrice, de către autoritatea competentă în conformitate cu procedurile naționale

și

([...])b sunt solicitate acțiuni suplimentare.

- (h) „indicator de validitate” înseamnă suspendarea validității unei semnalări la nivel național, care poate fi adăugat semnalărilor în vederea arestării, semnalărilor privind persoane dispărute **și persoane vulnerabile** și semnalărilor în vederea efectuării de controale discrete, de verificări prin interviu și de controale specifice [...];
- (i) „stat membru emitent” înseamnă statul membru care a introdus semnalarea în SIS;
- (j) „stat membru executant” înseamnă statul membru care întreprinde sau a întreprins acțiunile necesare în urma obținerii unui rezultat pozitiv;
- (k) „utilizatori finali” înseamnă autoritățile competente care efectuează căutări în mod direct în CS-SIS, N.SIS sau o copie tehnică a acestora;
- (ka) „date biometrice” înseamnă date biometrice astfel cum sunt definite la articolul 3 punctul 13 din Directiva (UE) 2016/680;**
- (l) „date dactiloscopice” înseamnă [...] **imagini** de amprente digitale, **imagini de amprente digitale latente**, [...] amprente palmare, **amprente palmare latente, precum și șabloane ale unor astfel de imagini (caracteristici codificate ale acestora)**⁴³ care, având în vedere unicitatea lor și punctele de referință pe care le conțin, permit comparații fiabile și concludente referitoare la identitatea unei persoane;
- (la) „imagine facială” înseamnă imagini digitale ale feței, având o rezoluție a imaginii și o calitate suficiente pentru a fi utilizate în compararea automatizată a datelor biometrice;**⁴⁴
- (lb) „profil ADN” înseamnă un cod format din litere sau din cifre care reprezintă un set de caracteristici de identificare a părții necodificate a unui eșantion analizat de ADN uman, adică structura moleculară specifică din diverse segmente de ADN (loci)**⁴⁵;

⁴³ Aceeași definiție ca în Decizia 2008/616/JAI a Consiliului.

⁴⁴ Aceeași definiție ca în propunerea privind EES [a se vedea articolul 3 alineatul (16) din documentul 11037/17 + ADD 1 + ADD 2).

⁴⁵ Aceeași definiție ca la articolul 2 litera (c) din Decizia 2008/616/JAI a Consiliului privind punerea în aplicare a Deciziei 2008/615/JAI privind intensificarea cooperării transfrontaliere, în special în domeniul combaterii terorismului și a criminalității transfrontaliere (JO L 210, 6.8.2008, p. 12).

- (m) „infrațiune gravă” înseamnă infracțiunile enumerate la articolul 2 alineatele (1) și (2) din Decizia-cadru 2002/584/JAI din 13 iunie 2002;⁴⁶
- (n) „infracțiuni de terorism” înseamnă **o** infracțiune [...] prevăzută în dreptul național **care corespunde uneia dintre infracțiunile** menționate în [...] ⁴⁷ [...] **Directiva (UE) 2017/541**⁴⁸ **sau care este echivalentă cu una dintre acestea;**
- (o) **„persoane vulnerabile” înseamnă persoane care necesită protecție din cauza vârstei, a stării de sănătate fizică sau psihică sau a situației lor sociale sau familiale;**
- (p) „amenințare pentru sănătatea publică” înseamnă amenințarea pentru sănătatea publică astfel cum este definită în Regulamentul (UE) 2016/399**⁴⁹.

Articolul 4

Arhitectura tehnică a SIS și modul de funcționare a acestuia

- (1) SIS este compus din următoarele elemente:
- (a) un sistem central (SIS central) format din:
- o funcție de asistență tehnică („CS-CIS”) ce conține o bază de date, „baza de date din SIS”;
 - o interfață națională uniformă (NI-SIS);

⁴⁶ Decizia-cadru 2002/584/JAI a Consiliului din 13 iunie 2002 privind mandatul european de arestare și procedurile de predare între statele membre (JO L 190, 18.7.2002, p. 1).

⁴⁷ [...]

⁴⁸ Directiva (UE) 2017/541 a Parlamentului European și a Consiliului din 15 martie 2017 privind combaterea terorismului și de înlocuire a Deciziei-cadru 2002/475/JAI a Consiliului și de modificare a Deciziei 2005/671/JAI a Consiliului (JO L 88, 31.3.2017, p. 6).

⁴⁹ Regulamentul (UE) 2016/399 al Parlamentului European și al Consiliului din 9 martie 2016 cu privire la Codul Uniunii privind regimul de trecere a frontierelor de către persoane (Codul frontierelor Schengen).

- (b) un sistem național (N.SIS) în fiecare stat membru, care constă în sisteme naționale de date care comunică cu SIS central. Un sistem N.SIS [...] **poate** conține un fișier de date (o „copie națională”) care conține o copie completă sau parțială a bazei de date SIS [...]; **Două sau mai multe state membre pot crea în unul dintre sistemele lor N.SIS o copie care poate fi utilizată în comun de statele membre respective. O astfel de copie comună este considerată drept copia națională a fiecăruia dintre statele membre participante;**
- (ba) cel puțin un sediu pentru copia de rezervă națională sau comună în fiecare sistem N.SIS. O copie comună de rezervă pentru sistemul N.SIS poate fi folosită în comun de două sau mai multe state membre și se consideră ca fiind copia de rezervă pentru sistemul N.SIS al fiecăruia dintre statele membre participante.** În vederea asigurării disponibilității neîntrerupte pentru utilizatorii finali, N.SIS și copia sa de rezervă pot fi folosite simultan; **și**
- (c) o infrastructură de comunicații între CS-SIS și NI-SIS („infrastructura de comunicații”) ce furnizează o rețea virtuală criptată destinată datelor din SIS și schimbului de date dintre birourile SIRENE, astfel cum se menționează la articolul 7 alineatul (2).
- (2) [...] **Statele membre** [...] **introduc** [...], actualizează [...], șterg [...] **datele din SIS** și efectuează căutări [...] în datele respective prin intermediul diferitelor sisteme N.SIS. O copie națională **sau comună** parțială sau integrală este disponibilă pentru efectuarea de căutări automate pe teritoriul fiecărui stat membru care utilizează o astfel de copie. Copia națională parțială **sau comună** conține cel puțin datele enumerate la articolul 20 alineatul (2) în cazul obiectelor și datele enumerate la articolul 20 alineatul (3) literele (a)-(v) **și (z)** din prezentul regulament în cazul semnalărilor privind persoane. Nu este posibil să se efectueze căutări în fișierele de date din sistemul N.SIS al altor state membre.

- (3) CS-SIS îndeplinește funcțiile de supraveghere tehnică și de administrare și are o copie de rezervă a CS-SIS care poate să asigure toate funcționalitățile CS-SIS principal, în cazul în care acesta încetează să funcționeze. **CS-SIS și copia de rezervă a CS-SIS pot funcționa simultan.** CS-SIS și copia de rezervă a CS-SIS sunt amplasate în [...] sediile tehnice ale Agenției Europene pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție, instituită prin Regulamentul (UE) nr. 1077/2011 („agenția”). CS-SIS sau copia de rezervă a CS-SIS poate conține o [...] copie **tehnică** a bazei de date din SIS [...] **care** poate fi utilizată simultan [...], cu condiția ca fiecare dintre acestea să fie în măsură să prelucreze toate operațiunile referitoare la semnalările din SIS.
- (4) CS-SIS furnizează serviciile necesare pentru introducerea datelor în SIS și prelucrarea acestora, inclusiv căutările în baza de date din SIS. CS-SIS asigură:
- (a) actualizarea online a copiilor naționale;
 - (b) sincronizarea și coerența dintre copiile naționale și baza de date din SIS;
 - (c) operațiunile de inițializare și de restabilire a copiilor naționale; **și**
 - (d) disponibilitatea neîntreruptă.

Articolul 5

Costuri

- (1) Costurile aferente funcționării, întreținerii și dezvoltării în continuare a SIS central și a infrastructurii de comunicații se suportă din bugetul general al Uniunii Europene.
- (2) Aceste costuri includ lucrările care vizează CS-SIS și asigură furnizarea serviciilor menționate la articolul 4 alineatul (4).
- (3) Costurile aferente înființării, funcționării, întreținerii și dezvoltării în continuare a fiecărui N.SIS sunt suportate de statul membru în cauză.

CAPITOLUL II

RESPONSABILITĂȚILE STATELOR MEMBRE

Articolul 6 *Sistemele naționale*

Fiecare stat membru este responsabil cu înființarea, funcționarea, întreținerea și dezvoltarea în continuare a sistemului său N.SIS și cu conectarea acestuia la NI-SIS.

Fiecare stat membru este responsabil să asigure funcționarea continuă a N.SIS, conectarea acestuia cu NI-SIS și disponibilitatea neîntreruptă a datelor din SIS pentru utilizatorii finali.

Fiecare stat membru transmite semnalările sale prin intermediul sistemului său N.SIS.⁵⁰

Articolul 7 *Oficiul N.SIS II și biroul SIRENE*

- (1) Fiecare stat membru desemnează o autoritate (oficiul N.SIS) care deține responsabilitatea principală pentru sistemul său N.SIS.

Autoritatea respectivă este responsabilă cu buna funcționare și securitatea N.SIS, asigură accesul autorităților competente la SIS și ia măsurile necesare pentru a garanta respectarea dispozițiilor prezentului regulament. Aceasta este responsabilă să asigure că toate funcționalitățile SIS sunt puse în mod corespunzător la dispoziția utilizatorilor finali.

[...] ⁵¹

⁵⁰ Mutat de la articolul 7 sfârșitul alineatului (1), cu excepția cuvântului „oficiu” de la finalul tezei.

⁵¹ Mutat la sfârșitul articolului 6.

- (2) Fiecare stat membru desemnează autoritatea care asigură schimbul și disponibilitatea tuturor informațiilor suplimentare (biroul SIRENE) în conformitate cu dispozițiile Manualului SIRENE, astfel cum se menționează la articolul 8.

Aceste birouri coordonează, de asemenea, verificarea calității informațiilor introduse în SIS. În aceste scopuri, birourile SIRENE au acces la datele prelucrate în SIS.

- (3) Statele membre informează agenția cu privire la oficiul lor N.SIS II [...] și la biroul lor SIRENE. Agenția publică lista acestora, împreună cu lista menționată la articolul 53 alineatul (8).

Articolul 8

Schimbul de informații suplimentare

- (1) Schimbul de informații suplimentare se efectuează în conformitate cu dispozițiile Manualului SIRENE și cu ajutorul infrastructurii de comunicații. Statele membre furnizează resursele tehnice și **umane** [...] necesare pentru a se asigura disponibilitatea continuă a informațiilor suplimentare și schimbul acestora. În cazul în care infrastructura de comunicații nu poate fi utilizată, statele membre pot folosi pentru schimbul de informații suplimentare alte mijloace tehnice, securizate în mod corespunzător.
- (2) Informațiile suplimentare se utilizează numai în scopul în care au fost transmise în conformitate cu articolul 61, cu excepția cazului în care s-a obținut în prealabil acordul statului membru emitent.
- (3) Birourile SIRENE își îndeplinesc sarcinile în mod rapid și eficient, în special [...] **răspunzând** unei cereri cât mai curând posibil, dar, **de preferat**, nu mai târziu de 12 ore de la primirea cererii.

- (4) **Comisia adoptă acte de punere în aplicare pentru a stabili** norme detaliate privind schimbul de informații suplimentare, **sub forma unui manual intitulat „Manualul SIRENE”**. **Actele de punere în aplicare respective** se adoptă [...] în conformitate cu procedura de examinare menționată la articolul 72 alineatul (2) [...].

Articolul 9

Conformitatea tehnică și funcțională

- (1) La crearea sistemului său N.SIS, fiecare stat membru respectă standardele, protocoalele și procedurile tehnice comune stabilite pentru a se asigura compatibilitatea sistemului său N.[...] SIS cu CS-SIS în vederea unei transmiteri prompte și eficiente a datelor. [...]⁵²
- (2) Statele membre se asigură, prin intermediul serviciilor furnizate de CS-SIS, că datele stocate în copia națională **sau în copia comună** sunt identice și coerente cu baza de date din SIS, prin efectuarea actualizărilor automate menționate la articolul 4 alineatul (4), și că în urma efectuării unei căutări în copia lor națională **sau în copia comună** se obține un rezultat echivalent cu cel generat de efectuarea unei căutări în baza de date din SIS. Utilizatorii finali primesc datele necesare pentru îndeplinirea sarcinilor care le revin, în special toate datele necesare pentru identificarea persoanei vizate și pentru întreprinderea acțiunii necesare.
- (3)⁵³Comisia adoptă acte de punere în aplicare pentru stabilirea și dezvoltarea standardelor, protocoalelor și procedurilor tehnice comune menționate la alineatul (1). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 72 alineatul (2).**

⁵² Mutat la alineatul (3).

⁵³ Mutat de la sfârșitul alineatului (1).

Articolul 10

Securitatea – Statele membre

- (1) Fiecare stat membru adoptă, în legătură cu sistemul său N.SIS, măsurile necesare, inclusiv un plan de securitate, un plan de asigurare a continuității activității și un plan de recuperare în caz de dezastru, pentru:
- (a) a proteja datele din punct de vedere fizic, inclusiv prin elaborarea de planuri de urgență pentru protecția infrastructurii critice;
 - (b) a împiedica accesul persoanelor neautorizate la instalațiile de prelucrare a datelor utilizate pentru prelucrarea datelor cu caracter personal (controlul accesului la instalații);
 - (c) a împiedica citirea, copierea, modificarea sau îndepărtarea neautorizată a suporturilor de date (controlul suporturilor de date);
 - (d) a împiedica introducerea neautorizată de date și inspectarea, modificarea sau ștergerea neautorizată a datelor cu caracter personal stocate (controlul stocării);
 - (e) a împiedica utilizarea sistemelor de prelucrare automată a datelor de către persoane neautorizate cu ajutorul echipamentelor de comunicare a datelor (controlul utilizatorilor);
 - (f) a se asigura că persoanele autorizate să utilizeze un sistem de prelucrare automată a datelor au acces numai la datele pentru care dețin autorizația de acces, prin utilizarea unor [...] **elemente** individuale și unice **de identificare**⁵⁴ a utilizatorului și cu folosirea exclusivă a unor moduri de acces confidențiale (controlul accesului la date);

⁵⁴ Aceeași formulare ca la articolul 12 alineatele (2) și (3) și ca la articolul 18 alineatele (2) și (3).

- (g) a se asigura că toate autoritățile cu drept de acces la SIS sau la instalațiile de prelucrare a datelor creează profiluri care descriu funcțiile și responsabilitățile persoanelor autorizate să acceseze, să introducă, să actualizeze datele și să efectueze căutări în date și că pun fără întârziere aceste profiluri la dispoziția autorităților naționale de supraveghere menționate la articolul 6[...]7, la cererea acestora (profilurile membrilor personalului);
 - (h) a se asigura că este posibil să se verifice și să se stabilească organismele cărora le pot fi transmise date cu caracter personal prin utilizarea echipamentelor de comunicare a datelor (controlul comunicării);
 - (i) a se asigura că ulterior este posibil să se verifice și să se stabilească ce date cu caracter personal au fost introduse în sistemele de prelucrare automată a datelor, când, de către cine și în ce scop au fost introduse datele (controlul introducerii);
 - (j) a împiedica citirea, copierea, modificarea sau ștergerea neautorizată a datelor cu caracter personal în timpul transferurilor de date cu caracter personal sau în timpul transportului suporturilor de date, în special prin utilizarea unor tehnici de criptare corespunzătoare (controlul transportului); și
 - (k) a monitoriza eficacitatea măsurilor de securitate menționate la prezentul alineat și a lua măsurile organizaționale necesare referitoare la monitorizarea internă (auditul intern).
- (2) Statele membre iau măsuri echivalente celor menționate la alineatul (1) în materie de securitate în ceea ce privește prelucrarea informațiilor suplimentare și schimbul de informații suplimentare, inclusiv securizarea sediilor birourilor SIRENE.
- (3) Statele membre iau măsuri echivalente celor menționate la alineatul (1) în materie de securitate în ceea ce privește prelucrarea datelor din SIS de către autoritățile menționate la articolul 43.
- (4) Măsurile descrise la alineatele (1)-(3) pot face parte dintr-o abordare și dintr-un plan de securitate generic la nivel național. Cu toate acestea, cerințele de la prezentul articol și aplicabilitatea sa în ceea ce privește SIS trebuie să fie clar identificabile și asigurate de planul respectiv.**

Articolul 11

Confidențialitatea – Statele membre

Fiecare stat membru aplică propriile norme privind secretul profesional sau alte obligații echivalente de confidențialitate pentru toate persoanele și organismele care lucrează cu date din SIS și cu informații suplimentare, în conformitate cu dreptul său național. Această obligație se aplică și după ce persoanele respective au încetat să mai ocupe o anumită funcție sau un anumit post ori după încetarea activității organismelor respective.

Articolul 12

Păstrarea înregistrărilor la nivel național

(1) Statele membre se asigură că orice accesare a datelor cu caracter personal și toate schimburile de date cu caracter personal din CS-SIS sunt înregistrate în sistemul lor N.SIS în scopul verificării legalității căutării, al monitorizării legalității prelucrării datelor, al automonitorizării și al asigurării funcționării corespunzătoare a N.SIS și a integrității și securității datelor.

Aceasta nu se aplică prelucrărilor automate menționate la articolul 4 alineatul (4) literele (a), (b) și (c).

(2) [...] **Înregistrările** arată, în special, istoricul semnalării, ziua și ora activității de prelucrare a datelor, datele utilizate pentru efectuarea unei căutări, o mențiune cu privire la datele transmise și [...] **elementele individuale și unice de identificare a utilizatorului**⁵⁵, atât ale autorității competente, cât și ale persoanei responsabile cu prelucrarea datelor.

(3) În cazul în care căutarea se efectuează prin utilizarea datelor dactiloscopice sau a imaginilor faciale în conformitate cu articolul [...] 42, înregistrările arată, în special, tipul de date utilizate pentru efectuarea unei căutări, o mențiune cu privire la tipul de date transmise și [...] **elementele individuale și unice de identificare a utilizatorului**⁵⁶, atât ale autorității competente, cât și ale persoanei responsabile cu prelucrarea datelor.

⁵⁵ Aceeași formulare ca la alineatul (3) și la articolul 10 alineatul (1) litera (f).

⁵⁶ Aceeași formulare ca la alineatul (2) și la articolul 10 alineatul (1) litera (f).

- (4) Înregistrările se pot utiliza numai în scopurile menționate la alineatul (1) și se șterg cel mai devreme după un an și cel mai târziu după trei ani de la creare.
- (5) Înregistrările se pot păstra mai mult timp dacă sunt necesare pentru proceduri de monitorizare care se află deja în curs.
- (6) Autoritățile naționale [...] **de supraveghere** responsabile cu verificarea legalității căutărilor, cu monitorizarea legalității prelucrării datelor, cu automonitorizarea și cu asigurarea funcționării corespunzătoare a N.SIS și a integrității și securității datelor au acces, în limitele competenței lor și la cerere, la aceste înregistrări în scopul îndeplinirii atribuțiilor care le revin.
- (7) În cazul în care statele membre efectuează căutări automate prin scanarea plăcuțelor de înmatriculare a autovehiculelor, prin utilizarea sistemelor de recunoaștere automată a plăcuțelor de înmatriculare, acestea păstrează înregistrările căutărilor în conformitate cu dreptul național. [...] ⁵⁷ [...]

(8)⁵⁸Comisia adoptă acte de punere în aplicare pentru stabilirea conținutului înregistrării menționate la alineatul (7). Respectivetele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 72 alineatul (2).

⁵⁷ Text mutat la noul alineat (8).

⁵⁸ Text mutat de la alineatul (7).

Articolul 13
Automonitorizarea

Statele membre se asigură că fiecare autoritate care are drept de acces la datele din SIS ia măsurile necesare pentru a respecta prezentul regulament și cooperează, dacă este necesar, cu autoritatea națională de supraveghere.

Articolul 14
Formarea personalului

Înainte de a fi autorizat să prelucreze datele stocate în SIS și periodic după acordarea accesului la datele din SIS, personalul autorităților care au drept de acces la SIS beneficiază de o formare corespunzătoare privind securitatea datelor, normele de protecție a datelor și procedurile referitoare la prelucrarea datelor, astfel cum se prevede în Manualul SIRENE. Personalul este informat cu privire la toate infracțiunile și sancțiunile relevante.

CAPITOLUL III
RESPONSABILITĂȚILE AGENȚIEI

Articolul 15
Gestionarea operațională

- (1) Agenția este responsabilă cu gestionarea operațională a SIS central. Agenția se asigură, în cooperare cu statele membre și prin utilizarea unei analize cost-beneficiu, că pentru SIS central se utilizează în permanență cea [...] **mai adecvată** tehnologie disponibilă.
- (2) Agenția este, de asemenea, responsabilă cu următoarele sarcini legate de infrastructura de comunicații:
 - (a) supravegherea;
 - (b) securitatea;
 - (c) coordonarea relațiilor dintre statele membre și furnizor.

- (3) Comisia este responsabilă cu toate celelalte sarcini legate de infrastructura de comunicații, în special:
- (a) sarcinile aferente execuției bugetare;
 - (b) achiziții și reînnoire;
 - (c) aspecte contractuale.
- (4) Agenția este, de asemenea, responsabilă cu următoarele sarcini legate de birourile SIRENE și comunicarea dintre birourile SIRENE:
- (a) coordonarea, [...] gestionarea **și sprijinirea activităților** de testare;
 - (b) întreținerea și actualizarea specificațiilor tehnice pentru schimbul de informații suplimentare dintre birourile SIRENE și infrastructura de comunicații și gestionarea impactului modificărilor tehnice în cazul în care acestea afectează atât SIS, cât și schimbul de informații suplimentare dintre birourile SIRENE.
- (5) Agenția dezvoltă și menține un mecanism și proceduri pentru verificarea calității datelor în CS-SIS și prezintă rapoarte periodice statelor membre. Agenția prezintă Comisiei un raport periodic care abordează problemele întâmpinate și statele membre afectate. [...] ⁵⁹

⁵⁹ Text mutat la noul alineat (7).

(6) Gestionarea operațională a SIS central constă în toate sarcinile necesare menținerii SIS central în funcțiune 24 de ore pe zi, șapte zile pe săptămână **în conformitate cu prezentul regulament**, în special activitatea de întreținere și dezvoltările tehnice necesare pentru buna funcționare a sistemului. Aceste sarcini includ de asemenea **coordonarea, gestionarea și sprijinirea** activităților de testare **pentru SIS central și sistemele naționale**, menite să asigure că SIS central și sistemele naționale funcționează în conformitate cu cerințele tehnice și funcționale, astfel cum se prevede la articolul 9 din prezentul regulament.

(7)⁶⁰Comisia adoptă acte de punere în aplicare pentru stabilirea cerințelor tehnice privind infrastructura de comunicații menționată la alineatul (2) și pentru stabilirea mecanismului și procedurilor pentru verificarea calității datelor în CS-SIS, menționate la alineatul (5), și pentru interpretarea respectării standardelor privind calitatea datelor. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 72 alineatul (2).

Articolul 16

Securitatea – Agentia

- (1) Agenția adoptă măsurile necesare, inclusiv un plan de securitate, un plan de asigurare a continuității activității și un plan de recuperare în caz de dezastru pentru SIS central și infrastructura de comunicații în scopul de:
- (a) a proteja datele din punct de vedere fizic, inclusiv prin elaborarea de planuri de urgență pentru protecția infrastructurii critice;
 - (b) a împiedica accesul persoanelor neautorizate la instalațiile de prelucrare a datelor utilizate pentru prelucrarea datelor cu caracter personal (controlul accesului la instalații);

⁶⁰ Text mutat de la alineatul (5).

- (c) a împiedica citirea, copierea, modificarea sau îndepărtarea neautorizată a suporturilor de date (controlul suporturilor de date);
- (d) a împiedica introducerea neautorizată de date și inspectarea, modificarea sau ștergerea neautorizată a datelor cu caracter personal stocate (controlul stocării);
- (e) a împiedica utilizarea sistemelor de prelucrare automată a datelor de către persoane neautorizate cu ajutorul echipamentelor de comunicare a datelor (controlul utilizatorilor);
- (f) a se asigura că persoanele autorizate să utilizeze un sistem de prelucrare automată a datelor au acces numai la datele pentru care dețin autorizația de acces, prin utilizarea unor [...] **elemente** individuale și unice **de identificare** a utilizatorului și cu folosirea exclusivă a unor moduri de acces confidențiale (controlul accesului la date);
- (g) a crea profiluri care descriu funcțiile și responsabilitățile persoanelor care sunt autorizate să acceseze datele sau instalațiile de prelucrare a datelor și de a pune fără întârziere aceste profiluri la dispoziția Autorității Europene pentru Protecția Datelor menționate la articolul 64, la cererea acesteia (profilurile membrilor personalului);
- (h) a se asigura că este posibil să se verifice și să se stabilească organismele cărora le pot fi transmise date cu caracter personal prin utilizarea echipamentelor de comunicare a datelor (controlul comunicării);
- (i) a se asigura că ulterior este posibil să se verifice și să se stabilească ce date cu caracter personal au fost introduse în sistemele de prelucrare automată a datelor, când și de către cine au fost introduse datele (controlul introducerii);
- (j) a împiedica citirea, copierea, modificarea sau ștergerea neautorizată a datelor cu caracter personal în timpul transferurilor de date cu caracter personal sau în timpul transportului suporturilor de date, în special prin utilizarea unor tehnici de criptare corespunzătoare (controlul transportului);
- (k) a monitoriza eficacitatea măsurilor de securitate prevăzute la prezentul alineat și a lua măsurile organizaționale necesare referitoare la monitorizarea internă, astfel încât să se asigure conformitatea cu prezentul regulament (audit intern).

- (2) Agenția ia măsuri echivalente celor menționate la alineatul (1) în materie de securitate în ceea ce privește prelucrarea informațiilor suplimentare și schimbul de informații suplimentare prin intermediul infrastructurii de comunicații.

Articolul 17

Confidențialitatea – [...] Agenția

- (1) Fără a aduce atingere articolului 17 din Statutul funcționarilor Uniunii Europene și Regimul aplicabil celorlalți agenți ai Uniunii Europene, agenția aplică norme corespunzătoare privind secretul profesional sau alte obligații echivalente de confidențialitate pentru toți membrii personalului său care trebuie să lucreze cu date din SIS, la standarde comparabile cu cele prevăzute la articolul 11 din prezentul regulament. Obligația menționată se aplică și după ce persoanele respective au încetat să mai ocupe o anumită funcție sau un anumit post ori după ce și-au încetat activitatea.
- (2) Agenția ia măsuri echivalente celor menționate la alineatul (1) în materie de confidențialitate în ceea ce privește schimbul de informații suplimentare prin intermediul infrastructurii de comunicații.

Articolul 18

Păstrarea înregistrărilor la nivel central

- (1) Agenția se asigură că orice accesare a datelor cu caracter personal și toate schimburile de date cu caracter personal din CS-SIS sunt înregistrate în scopurile menționate la articolul 12 alineatul (1).
- (2) Înregistrările arată, în special, istoricul [...] **semnalării**⁶¹, ziua și ora transmiterii datelor, datele [...] utilizate pentru efectuarea căutărilor, [...] o mențiune cu privire la datele transmise și [...] **elementele individuale și unice de identificare a utilizatorului**⁶² ale autorității competente responsabile cu prelucrarea datelor.

⁶¹ Forma de singular, ca la articolul 12 alineatul (2).

⁶² Aceeași formulare ca la articolul 10 alineatul (1) litera (f) și articolul 12 alineatele (2) și (3).

- (3) În cazul în care căutarea se efectuează cu ajutorul datelor dactiloscopice sau al imaginilor faciale în conformitate cu articolele 40, 41 și 42, înregistrările arată, în special, tipul de date utilizate pentru efectuarea unei căutări, o mențiune cu privire la tipul de date transmise și [...] **elementele individuale și unice de identificare a utilizatorului**, atât ale autorității competente, cât și ale persoanei responsabile cu prelucrarea datelor.
- (4) Înregistrările se pot utiliza numai în scopurile menționate la alineatul (1) și se șterg cel mai devreme după un an și cel mai târziu după trei ani de la creare. Înregistrările care includ istoricul semnalărilor se șterg în termen de unu până la trei ani de la ștergerea semnalărilor.
- (5) Înregistrările se pot păstra mai mult timp dacă sunt necesare pentru proceduri de monitorizare care se află deja în curs.
- (6) [...] **Autoritatea Europeană pentru Protecția Datelor** are acces, în limitele competenței [...] **sale** și la cererea [...] **sa**, la aceste înregistrări în scopul îndeplinirii atribuțiilor care [...] **ii** revin.

CAPITOLUL IV INFORMAREA PUBLICULUI

Articolul 19

Campanii de informare privind SIS

Comisia, în cooperare cu autoritățile naționale de supraveghere și cu Autoritatea Europeană pentru Protecția Datelor, efectuează periodic campanii de informare a publicului privind obiectivele SIS, datele stocate, autoritățile care au acces la SIS și drepturile persoanelor vizate. Statele membre, în cooperare cu propriile autorități naționale de supraveghere, elaborează și pun în aplicare politicile necesare de informare generală a cetățenilor lor cu privire la SIS.

CAPITOLUL V
CATEGORII DE DATE ȘI APLICAREA UNUI INDICATOR DE VALIDITATE

Articolul 20

Categoriile de date

- (1) Fără a aduce atingere articolului 8 alineatul (1) sau dispozițiilor prezentului regulament care prevăd stocarea datelor suplimentare, SIS conține doar categoriile de date care sunt furnizate de fiecare stat membru și care sunt necesare pentru scopurile prevăzute la articolele 26, 32, 34, 36, [...]38 **și 40**.
- (2) Categoriile de date sunt următoarele:
- (a) informații privind persoanele care fac obiectul unei semnalări;
 - (b) informații privind obiectele menționate la articolele **26**, 32, **34**, 36 și 38.
- (3) **Orice semnalare în SIS care include** [...] informații privind persoane [...] conține numai următoarele date:
- (a) numele [...] [...];
 - (b) prenumele [...] [...];
 - (c) numele [...] [...] la naștere;
 - (d) numele folosite anterior și numele de împrumut;
 - (e) orice caracteristică fizică specifică, obiectivă și inalterabilă;
 - (f) locul nașterii;

- (g) data nașterii;
- (h) [...] **genul**;
- (i) cetățenia/cetățeniile;
- (j) dacă persoana în cauză:
 - i. este înarmată [...] **;** [...]
 - ii. **este** violentă [...] **;**
 - iii. s-a **sustras sau** a evadat [...] **;**
 - iv. **prezintă un risc de sinucidere**;
 - v. **reprezintă o** [...] **amenintare pentru sănătatea publică sau**
 - vi. este implicată într-o [...] activitate **legată de terorism** [...];
- (k) motivul semnalării;
- (l) autoritatea care emite semnalarea;
- (m) o trimitere la decizia care a generat semnalarea;
- (n) acțiunea care trebuie întreprinsă;
- (o) legătura (legăturile) cu alte semnalări emise în SIS în temeiul articolului [...] **60**;
- (p) tipul de infracțiune pentru care s-a emis semnalarea;
- (q)** numărul de înregistrare al persoanei în cauză într-un registru național;

- (r) o clasificare a tipului de caz de persoană dispărută (numai pentru semnalările menționate la articolul 32);
 - (s)** categoria document**elor** de identificare ale persoanei;
 - (t) țara care a eliberat document**ele** de identificare ale persoanei;
 - (u) numărul (numerele) document**elor** de identificare al persoanei;
 - (v) data eliberării document**elor** de identificare ale persoanei;
 - (w) fotografiile și imagini faciale;
 - (x) profilurile ADN relevante, sub rezerva articolului 22 alineatul (1) litera (b) din prezentul regulament;
 - (y) date dactiloscopice;
 - (z) o [...] copie **(color, ori de câte ori este posibil)** a document**elor** de identificare.
- (4) Normele tehnice necesare privind introducerea, actualizarea și ștergerea datelor menționate la alineatele (2) și (3) și efectuarea de căutări în acestea se stabilesc și se dezvoltă prin intermediul unor măsuri de punere în aplicare în conformitate cu procedura de examinare menționată la articolul 72 alineatul (2).
- (5) [...] ⁶³ Aceste norme tehnice sunt similare în cazul căutărilor efectuate în CS-SIS, în copiile naționale **sau în copiile comune** și în copiile tehnice, astfel cum se menționează la articolul 53 alineatul (2), și se bazează pe standarde comune stabilite **și** dezvoltate prin intermediul unor măsuri de punere în aplicare în conformitate cu procedura de examinare menționată la articolul 72 alineatul (2).

⁶³ Redundant în raport cu alineatul (4).

Articolul 21
Proportionalitatea

- (1) Înainte de a emite o semnalare și atunci când prelungesc perioada de valabilitate a unei semnalări, statele membre stabilesc dacă respectivul caz este suficient de adecvat, relevant și important pentru a se justifica [...] **existența** unei semnalări în SIS.
- (2) În cazul în care un stat membru caută o persoană sau un obiect în legătură cu o infracțiune care intră sub incidența articolelor [...] **3-14** din **Directiva 2017/541 sau care este echivalentă cu una dintre respectivele infracțiuni** [...] ⁶⁴, statul membru [...] creează o [...] semnalare corespunzătoare [...]. **În mod excepțional, statele membre se pot abține de la crearea semnalării atunci când aceasta este de natură să obstrucționeze cercetările, investigațiile sau procedurile oficiale ori juridice legate de siguranța publică sau securitatea națională.**

Articolul 22⁶⁵
[...]

⁶⁴ [...]

⁶⁵ Articol mutat în noul capitol XIa, devenind articolul 41A.

[...]

Articolul 23

Cerințe privind introducerea unei semnalări

- (1) [...] ⁶⁶ **Se introduc toate datele enumerate la articolul 20 alineatul (3), atunci când sunt disponibile.**⁶⁷
- (2) [...] ⁶⁸ Nu se poate introduce o semnalare privind o persoană fără datele menționate la articolul 20 alineatul (3) literele (a), (g), (k), [...] (n) [...], cu excepția situațiilor menționate la articolul 40⁶⁹.

⁶⁶ Mutat parțial la alineatul (2).

⁶⁷ Mutat parțial de la alineatul (2).

⁶⁸ Mutat parțial la alineatul (1).

⁶⁹ Mutat parțial de la alineatul (1).

Articolul 24

Dispoziții generale privind aplicarea unui indicator de validitate

- (1) În cazul în care un stat membru consideră că a da curs unei semnalări introduse în conformitate cu articolele 26, 32 **sau** [...] 36 este un fapt incompatibil cu dreptul său național, cu obligațiile sale internaționale sau cu interesele sale naționale fundamentale, acesta poate solicita ulterior să se aplice semnalării un indicator de validitate, care să arate că acțiunea care trebuie întreprinsă pe baza semnalării nu va fi întreprinsă pe teritoriul său. Indicatorul de validitate se aplică de către biroul SIRENE al statului membru emitent.
- (2) Pentru ca statele membre să poată solicita aplicarea unui indicator de validitate unei semnalări emise în conformitate cu articolul 26, tuturor statelor membre li se notifică în mod automat orice nouă semnalare din categoria respectivă, printr-un schimb de informații suplimentare.
- (3) Dacă în cazuri extrem de urgente și de grave un stat membru emitent solicită executarea acțiunii, statul membru care execută semnalarea examinează dacă poate să autorizeze retragerea indicatorului de validitate aplicat la cererea sa. Dacă statul membru de executare este în măsură să facă acest lucru, ia măsurile necesare pentru a se asigura că acțiunea care trebuie întreprinsă poate să fie efectuată imediat.

Articolul 25

Aplicarea unui indicator de validitate semnalărilor în vederea arestării în scopul predării

- (1) În cazul în care se aplică Decizia-cadru 2002/584/JAI, unei semnalări în vederea arestării în scopul predării i se [...] aplică un indicator de validitate care împiedică arestarea atunci când autoritatea judiciară competentă în temeiul dreptului național să execute un mandat european de arestare a refuzat executarea acestuia pe baza unui motiv de neexecutare și atunci când s-a solicitat aplicarea indicatorului de validitate.

De asemenea, un stat membru poate solicita să se aplice un indicator de validitate semnalării dacă autoritatea sa judiciară competentă eliberează persoana care face obiectul semnalării în timpul procesului de predare.

- (2) Cu toate acestea, la cererea unei autorități judiciare competente în temeiul dreptului național, pe baza unei instrucțiuni generale sau într-un caz specific, se poate solicita, de asemenea, ca unei semnalări în vederea arestării în scopul predării să i se aplice un indicator de validitate dacă este evident că executarea mandatului european de arestare va trebui să fie refuzată.

CAPITOLUL VI

SEMNALĂRILE PRIVIND PERSOANE CĂUTATE ÎN VEDEREA ARESTĂRII ÎN SCOPUL PREDĂRII SAU AL EXTRĂDĂRII

Articolul 26

Obiectivele semnalărilor și condițiile de emitere a acestora

- (1) Datele privind persoane căutate în vederea arestării în scopul predării pe baza unui mandat european de arestare sau căutate în vederea arestării în scopul extrădării se introduc la cererea autorității judiciare a statului membru emitent.
- (2) Datele privind persoane căutate în vederea arestării în scopul predării se introduc, de asemenea, pe baza mandatelor de arestare emise în conformitate cu acordurile încheiate între Uniunea Europeană și țările terțe în temeiul articolului 37 din Tratatul privind Uniunea Europeană în scopul predării persoanelor pe baza unui mandat de arestare, care prevăd transmiterea unui astfel de mandat de arestare prin intermediul SIS.
- (3) Orice trimitere din prezentul regulament la dispozițiile Deciziei-cadru 2002/584/JAI trebuie înțeleasă ca incluzând dispozițiile corespunzătoare ale acordurilor încheiate între Uniunea Europeană și țările terțe în temeiul articolului 37 din Tratatul privind Uniunea Europeană în scopul predării persoanelor pe baza unui mandat de arestare care prevăd transmiterea unui astfel de mandat de arestare prin intermediul SIS.

(4) [...] **În cazul unei operațiuni [...] în curs, statul membru emitent poate să suspende temporar disponibilitatea unei semnalări existente în vederea arestării emise în temeiul articolului 26, astfel încât semnalarea să nu fie inclusă în rezultatul căutărilor efectuate de utilizatorul final din statul membru implicat în operațiune și să fie accesibilă doar birourilor SIRENE, dacă sunt întrunite următoarele condiții:**

(a) [...] obiectivul operațiunii nu poate fi realizat prin nicio altă măsură;

(b) [...] autoritatea judiciară competentă din statul membru emitent a acordat o autorizație prealabilă [...]; și

(c) toate statele membre implicate în operațiune au fost informate prin schimbul de informații suplimentare.

[...] Funcționalitatea **prevăzută la primul paragraf nu** se utilizează **decât** pe o perioadă de maximum 48 de ore [...]. **Cu toate acestea, dacă** este necesar din punct de vedere operațional, această perioadă poate fi [...] prelungită cu perioade suplimentare de 48 de ore. Statele membre întocmesc statistici referitoare la numărul de semnalări în cazul cărora s-a utilizat această funcționalitate.

(5) Atunci când există indicii clare că obiectul menționat la articolul 38 alineatul (2) literele (a), (b), (c), (e), (g), (h) și (k) are legătură cu o persoană care face obiectul unei semnalări în temeiul alineatelor (1) și (2), se pot emite semnalări privind obiectele respective pentru a se localiza persoana vizată. În aceste cazuri se creează o legătură între semnalarea privind persoana și semnalarea privind obiectul, în conformitate cu articolul 60.

- (6) Comisia adoptă acte de punere în aplicare pentru stabilirea și dezvoltarea normelor necesare privind introducerea, actualizarea și ștergerea datelor menționate la alineatul (5), precum și privind efectuarea de căutări în acestea. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 72 alineatul (2).**

Articolul 27

Date suplimentare privind persoane căutate în vederea arestării în scopul predării

- (1) În cazul în care o persoană este căutată în vederea arestării în scopul predării pe baza unui mandat european de arestare, statul membru emitent introduce în SIS o copie a originalului mandatului european de arestare.
- (2) Statul membru emitent poate introduce o copie a traducerii mandatului european de arestare în una sau mai multe limbi oficiale ale instituțiilor Uniunii Europene.

Articolul 28

Informații suplimentare privind persoane căutate în vederea arestării în scopul predării

Statul membru care a introdus în SIS semnalarea în vederea arestării în scopul predării comunică celorlalte state membre informațiile menționate la articolul 8 alineatul (1) din Decizia-cadru 2002/584/JAI, printr-un schimb de informații suplimentare.

Articolul 29

Informații suplimentare privind persoane căutate în vederea arestării în scopul extrădării

- (1) Statul membru care a introdus în SIS semnalarea în vederea arestării în scopul extrădării comunică celorlalte state membre, printr-un schimb de informații suplimentare cu toate statele membre, următoarele informații:
 - (a) autoritatea care a emis cererea de arestare;

- (b) dacă există un mandat de arestare sau un document cu același efect juridic ori o hotărâre executorie;
 - (c) natura infracțiunii și încadrarea juridică a acesteia;
 - (d) o descriere a circumstanțelor în care s-a comis infracțiunea, inclusiv data, locul și măsura în care persoana care face obiectul semnalării a participat la comiterea infracțiunii;
 - (e) în măsura în care este posibil, consecințele infracțiunii;
 - (f) orice alte informații utile sau necesare pentru executarea semnalării.
- (2) Datele menționate la alineatul (1) nu se comunică în cazul în care datele menționate la articolul 27 sau 28 au fost deja furnizate și sunt considerate suficiente pentru executarea semnalării de către statul membru în cauză.

Articolul 30

Conversia semnalărilor privind persoane căutate în vederea arestării în scopul predării sau al extrădării

Atunci când nu se poate efectua arestarea, fie din cauza refuzului unui stat membru solicitat, exprimat în conformitate cu procedurile privind aplicarea unui indicator de validitate stabilite la articolul 24 sau 25, fie, în cazul unei semnalări în vederea arestării în scopul extrădării, pentru că investigația nu s-a finalizat, statul membru solicitat tratează semnalarea [...] în scopul comunicării locului unde se află persoana vizată.

Articolul 31

Executarea acțiunii pe baza unei semnalări privind o persoană căutată în vederea arestării în scopul predării sau al extrădării

- (1) O semnalare introdusă în SIS în conformitate cu articolul 26, împreună cu datele suplimentare menționate la articolul 27, constituie un mandat european de arestare emis în conformitate cu Decizia-cadru 2002/584/JAI și are același efect ca acesta în cazul în care se aplică decizia-cadru menționată.
- (2) În cazul în care nu se aplică Decizia-cadru 2002/584/JAI, o semnalare introdusă în SIS în conformitate cu articolele 26 și 29 are aceeași forță juridică ca o cerere de arestare provizorie în temeiul articolului 16 din Convenția europeană de extrădare din 13 decembrie 1957 sau al articolului 15 din Tratatul Benelux privind extrădarea și asistența reciprocă judiciară în materie penală din 27 iunie 1962.

CAPITOLUL VII

SEMNALĂRILE PRIVIND PERSOANE DISPĂRUTE SAU VULNERABILE

Articolul 32

Obiectivele semnalărilor și condițiile de emitere a acestora

- (1) [...]

- (2) **Se [...]** introduc **în SIS** următoarele categorii de [...] persoane, **la cererea unei autorități competente a statului membru care emite alerta:**
- (a) persoane dispărute care trebuie plasate sub protecție
 - (i) pentru propria lor protecție;
 - (ii) pentru a preîntâmpina amenințări;
 - (b) persoane dispărute care nu trebuie plasate sub protecție;
 - (c) copii expuși riscului de răpire în conformitate cu alineatul (4), **care trebuie împiedicați să călătorească; sau**
 - (d) persoanele vulnerabile care trebuie împiedicate să călătorească pentru propria lor protecție în conformitate cu alineatul 4 litera (a).**
- (3) **Literele (a) și (d) ale [...]** alineatului (2) [...] se aplică mai ales copiilor și persoanelor **în privința cărora [...]** autoritățile competente **au luat** o decizie.

- (4) La cererea autorităților [...] competente, **inclusiv a autorităților judiciare din statele membre competente în materia răspunderii părintești,** [...] se introduce o semnalare privind un copil din categoria menționată la alineatul 2 litera (c) [...] ⁷⁰ atunci când există un risc concret și evident ca respectivul copil să fie scos ilegal [...] din statul membru în care **sunt** [...] situate **autoritățile** [...] competente. [...]

Autoritatea competentă reexaminează periodic necesitatea de a se menține semnalarea.

- (4a) La cererea autorităților competente, se introduce o semnalare privind persoanele vulnerabile menționate la alineatul 2 litera (d) atunci când se consideră că există un risc concret și evident pentru respectiva persoană dacă ar pleca din statul membru în cauză.**
[...]

Autoritatea competentă reexaminează periodic necesitatea de a se menține semnalarea.

⁷⁰ [...]

- (5) Statele membre se asigură că datele introduse în SIS indică în care dintre categoriile menționate la alineatul (2) se încadrează persoana [...]. În plus, statele membre se asigură că datele introduse în SIS indică despre ce tip de caz [...] este vorba **și că, în ceea ce privește semnalările emise în temeiul alineatului (2) literele (c) și (d), toate informațiile relevante sunt puse la dispoziția biroului SIRENE al statului membru emitent în momentul creării semnalării.** [...] ⁷¹
- (6) Cu patru luni înainte ca un copil care face obiectul unei semnalări în temeiul prezentului articol să împlinească vârsta majoratului **conform dreptului național al statului membru emitent**, CS-SIS notifică automat statului membru emitent că este necesar ca motivul cererii și acțiunea care trebuie întreprinsă să fie actualizate sau ca semnalarea să fie ștearsă.
- (7) În cazul în care există indicii clare că anumite vehicule, ambarcațiuni sau aeronave au legătură cu o persoană care face obiectul unei semnalări prevăzute la alineatul (2), se pot emite semnalări privind vehiculele, ambarcațiunile și aeronavele respective pentru a localiza persoana vizată. În aceste cazuri se creează o legătură între semnalarea privind [...] persoana și semnalarea privind obiectul, în conformitate cu articolul 60. [...] ⁷²

⁷¹ Mutat la alineatul (8).

⁷² Mutat la alineatul (8).

(8)⁷³Comisia adoptă acte de punere în aplicare pentru stabilirea și dezvoltarea normelor privind clasificarea tipurilor de cazuri și introducerea datelor menționate la alineatul (5), precum și a normelor tehnice necesare privind introducerea, actualizarea și ștergerea datelor menționate la alineatul (7), precum și privind căutarea în acestea. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 72 alineatul (2).

Articolul 33

Executarea acțiunii pe baza unei semnalări

- (1) Atunci când o persoană care intră sub incidența articolului 32 este localizată, autoritățile competente comunică statului membru care a emis semnalarea unde se află aceasta, sub rezerva alineatului (2).
- (1a)** În cazul **persoanelor** [...] care trebuie plasate sub protecție **conform articolului 32 alineatul (2) literele (a), (c) și (d)**, statul membru de executare [...] **consultă** imediat **propriile sale autorități competente și pe cele din** statul membru emitent, **printr-un schimb de informații suplimentare**, pentru a se conveni fără întârziere asupra măsurilor care trebuie luate pentru a proteja interesul superior al copilului. Autoritățile competente **din statul membru de executare pot, în conformitate cu dreptul național**, [...] să transfere persoana respectivă într-un loc sigur pentru a o împiedica să își continue călătoria [...].
- (2) Comunicarea datelor, alta decât cea dintre autoritățile competente, privind o persoană dispărută care a fost localizată și care este majoră se face numai cu acordul respectivei persoane. Cu toate acestea, autoritățile competente pot comunica persoanei care a raportat dispariția faptul că semnalarea a fost ștearsă, deoarece persoana dispărută a fost localizată.

⁷³ Mutat de la sfârșitul alineatului (5) și de la sfârșitul alineatului (7).

CAPITOLUL VIII
SEMNALĂRILE PRIVIND PERSOANE CĂUTATE ÎN VEDEREA PARTICIPĂRII LA O
PROCEDURĂ JUDICIARĂ

Articolul 34

Obiectivele semnalărilor și condițiile de emitere a acestora

- (1) Pentru a comunica locul de reședință sau domiciliul persoanelor, statele membre introduc în SIS, la cererea unei autorități competente, date privind:
- (a) martori;
 - (b) persoane citate sau căutate pentru a fi citate să se prezinte în fața autorităților judiciare în cadrul unei proceduri penale pentru a răspunde în legătură cu fapte pentru care sunt urmărite penal;
 - (c) persoane cărora trebuie să li se notifice sau comunice o hotărâre judecătorească sau alte documente privind o procedură penală pentru a răspunde în legătură cu fapte de care sunt urmărite penal;
 - (d) persoane cărora trebuie să li se notifice sau comunice o citație pentru a se prezenta în vederea executării unei pedepse privative de libertate.
- (2) Atunci când există indicii clare că anumite vehicule, ambarcațiuni sau aeronave au legătură cu o persoană care face obiectul unei semnalări în temeiul alineatului (1), se pot emite semnalări privind vehiculele, ambarcațiunile și aeronavele respective pentru a localiza persoana vizată. În aceste cazuri se creează o legătură între semnalările privind persoana și semnalarea privind obiectul, în conformitate cu articolul 60. [...] ⁷⁴.

⁷⁴ Mutat la alineatul (3).

(3)⁷⁵ Comisia adoptă acte de punere în aplicare pentru stabilirea și dezvoltarea normelor tehnice necesare privind introducerea, actualizarea și ștergerea datelor menționate la alineatul (2), precum și privind efectuarea de căutări în acestea. Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 72 alineatul (2).

Articolul 35

Executarea acțiunii pe baza unei semnalări

Informațiile cerute i se comunică statului membru solicitant printr-un schimb de informații suplimentare.

CAPITOLUL IX

**SEMNALĂRILE PRIVIND PERSOANE ȘI OBIECTE ÎN SCOPUL EFECTUĂRII DE
CONTROALE DISCRETE, DE VERIFICĂRI PRIN INTERVIU SAU DE CONTROALE
SPECIFICE**

Articolul 36

Obiectivele semnalărilor și condițiile de emitere a acestora

(1) Datele privind persoanele sau obiectele **menționate la articolul 38 alineatul (2) literele (a), (b), (c), (e), (g), (h), (i), (k) și mijloacele de plată fără numerar** se introduc în conformitate cu dreptul național al statului membru care emite semnalarea, în scopul efectuării de controale discrete, de verificări prin interviu sau de controale specifice, în conformitate cu articolul 37 alineatele **(3), (4) și (5)**.

(1a) Atunci când emit semnalări în scopul efectuării de controale discrete, de verificări prin interviu sau de controale specifice și în cazul în care informațiile solicitate de statul membru emitent sunt suplimentare celor prevăzute la articolul 37 alineatul (1), statul membru emitent adaugă la semnalare toate informațiile solicitate.

⁷⁵ Mutat de la sfârșitul alineatului 2.

- (2) Semnalarea poate fi emisă în scopul **prevenirii, depistării, investigării sau** urmării penale a infracțiunilor, al executării unei pedepse și al preîntâmpinării amenințărilor pentru siguranța publică:
- (a) atunci când există indicii clare că o persoană intenționează să comită sau comite o infracțiune gravă, în special una dintre infracțiunile menționate la articolul 2 alineatul (2) din Decizia-cadru 2002/584/JAI; **sau**
 - (b) atunci când informațiile menționate la articolul 37 alineatul (1) sunt necesare pentru executarea unei pedepse a unei persoane condamnate pentru o infracțiune gravă, în special una dintre infracțiunile menționate la articolul 2 alineatul (2) din Decizia-cadru 2002/584/JAI sau
 - (c) atunci când, în urma evaluării generale a unei persoane, în special pe baza infracțiunilor pe care le-a comis în trecut, există motive să se creadă că respectiva persoană ar putea comite și în viitor infracțiuni grave, în special una dintre infracțiunile menționate la articolul 2 alineatul (2) din Decizia-cadru 2002/584/JAI.
- (3) În plus, se poate emite o semnalare în conformitate cu dreptul național, la cererea autorităților responsabile cu securitatea națională, dacă există indicii concrete că informațiile menționate la articolul 37 alineatul (1) sunt necesare pentru a preîntâmpina o amenințare gravă din partea persoanei vizate sau alte amenințări grave pentru securitatea națională internă sau externă. Statul membru care emite semnalarea în temeiul prezentului alineat informează celelalte state membre cu privire la aceasta. Fiecare stat membru stabilește autoritățile cărora li se transmite această informație **prin intermediul biroului său SIRENE**.
- (4) Atunci când există indicii clare că **obiectele menționate la articolul 38 alineatul (2) literele (a), (b), (c), (e), (g), (h), (i), (k) sau mijloacele de plată fără numerar** [...] au legătură cu infracțiunile grave menționate la alineatul (2) sau cu amenințările grave menționate la alineatul (3), se pot emite semnalări privind respectivele **obiecte** [...] **și se pot crea legături între aceste semnalări și cele introduse în temeiul alineatelor (2) și (3)**.

(5) [...] ⁷⁶ [...]

(6)⁷⁷Comisia adoptă acte de punere în aplicare pentru stabilirea și dezvoltarea normelor tehnice necesare privind introducerea, actualizarea și ștergerea datelor menționate la alineatul (4), precum și privind efectuarea de căutări în acestea, ca și a informațiilor suplimentare menționate la alineatul (1a). Respectivele acte de punere în aplicare se adoptă în conformitate cu procedura de examinare menționată la articolul 72 alineatul (2).

Articolul 37

Executarea acțiunii pe baza unei semnalări

- (1) În scopul efectuării de controale discrete, de verificări prin interviu sau de controale specifice, toate sau unele dintre următoarele informații se colectează și se comunică [...] statului membru [...] emitent:
- (a) faptul că persoana sau **obiectele menționate la articolul [...] 38 alineatul (2) literele (a), (b), (c), (e), (g), (h), (j), (k) sau mijloacele de plată fără numerar** care fac obiectul semnalării sunt **sau au fost** localizate;
 - (b) locul, ora și motivul efectuării controlului sau a verificării;

⁷⁶ Mutat la alineatul (6).

⁷⁷ Mutat de la sfârșitul alineatului (5).

- (c) ruta și destinația călătoriei;
 - (d) persoanele care însoțesc persoana vizată sau ocupanții vehiculului, ambarcațiunii ori aeronavei sau persoanele care îl însoțesc pe titularul documentului oficial în alb sau al documentului de identitate eliberat despre care se poate presupune în mod rezonabil că au legătură cu persoanele vizate;
 - (e) identitatea dezvăluită și descrierea persoanei care utilizează documentul oficial în alb sau documentul de identitate eliberat care face obiectul semnalării;
 - (f) **obiectele menționate la articolul 38 alineatul (2) literele (a), (b), (c), (e), (g), (h), (i), (k) sau mijloacele de plată fără numerar** [...] utilizate;
 - (g) obiectele transportate, inclusiv documentele de călătorie;
 - (h) circumstanțele în care s-a localizat persoana sau **autovehiculul, remorca, rulota,** ambarcațiunea, **containerul,** aeronava, [...] documentul oficial în alb ori **documentul** de identitate eliberat [...] **sau mijlocul de plată fără numerar;**
 - (i) **alte informații, a căror colectare se poate să fi fost solicitată de statul membru emitent în conformitate cu articolul 36 alineatul (1a).**
- (2) Informațiile menționate la alineatul (1) sunt comunicate printr-un schimb de informații suplimentare.
- (3) [...] **Un control discret cuprinde colectarea discretă de cât mai multe informații este posibil dintre cele descrise la alineatul (1) în cursul activităților de rutină derulate de autoritățile naționale competente. Colectarea acestor informații nu trebuie să afecteze caracterul discret al controalelor, iar persoana care face obiectul semnalării nu trebuie sub nicio formă să aibă cunoștință de existența semnalării.**

- (4) [...] **O** verificare prin interviu cuprinde [...] **interviewarea** persoanei [...] ⁷⁸, **inclusiv pe baza informațiilor sau a întrebărilor specifice adăugate semnalării de statul membru emitent. Interviul se desfășoară în conformitate cu dreptul național al statului membru de executare.** [...]
- (5) În timpul controalelor specifice, persoanele, vehiculele, ambarcațiunile, aeronavele, containerele și obiectele transportate pot fi percheziționate [...] în scopurile menționate la articolul 36. Perchezițiile se efectuează în conformitate cu dreptul național. [...] ⁷⁹
- (6)** În cazul în care dreptul [...] **național** [...] nu autorizează controalele specifice, acestea se înlocuiesc în respectivul stat membru cu verificări prin interviu ⁸⁰. **În cazul în care dreptul național nu autorizează verificările prin interviu, acestea se înlocuiesc în respectivul stat membru cu controale discrete** ⁸¹.
- (7)** **Alineatul (6) nu aduce atingere obligației statelor membre de a pune la dispoziția utilizatorilor finali toate informațiile suplimentare menționate la articolul 36 alineatul (1a) și de a asigura colectarea acestor informații și transmiterea lor către statul membru emitent printr-un schimb de informații suplimentare.**

⁷⁸ Mutat la noul alineat (6).

⁷⁹ Transferat la noul alineat (6).

⁸⁰ Mutat de la alineatul (5).

⁸¹ Mutat de la alineatul (4).

CAPITOLUL X

SEMNALĂRILE PRIVIND OBIECTE CĂUTATE PENTRU A FI CONFISCATE SAU FOLOSITE CA PROBE ÎN CADRUL PROCEDURILOR PENALE

Articolul 38

Obiectivele semnalărilor și condițiile de emitere a acestora

- (1) Se introduc în SIS date privind obiectele căutate pentru a fi confiscate [...] sau **pentru a fi** folosite ca probe în cursul procedurilor penale.
- (2) Se introduc următoarele categorii de obiecte ușor identificabile:
 - (a) autovehicule [...], indiferent de sistemul de propulsie;
 - (b) remorci cu o greutate fără încărcătură de peste 750 kg;
 - (c) rulote;
 - (d) echipamente industriale;
 - (e) ambarcațiuni;
 - (f) motoare de ambarcațiuni;
 - (g) containere;
 - (h) aeronave;
 - (ha) motoare aeronautice;**
 - (i) arme de foc;

- (j) documente oficiale în alb care au fost furate, însușite în mod ilegal, [...] pierdute **sau despre care se pretinde că ar astfel de documente, fiind însă false;**
- (k) documente de identitate eliberate, cum ar fi pașapoarte, cărți de identitate, [...] permise de ședere, documente de călătorie **și permise de conducere**, care au fost furate, însușite în mod ilegal, pierdute sau anulate ori despre care se pretinde că ar fi astfel de documente, fiind însă fals[...];
- (l) certificate sau plăcuțe de înmatriculare ale vehiculelor care au fost furate, însușite în mod ilegal, pierdute sau anulate ori despre care se pretinde că ar fi astfel de documente ori plăcuțe, fiind însă fals[...];
- (m) bancnote (bancnote înregistrate)și bancnote fals[...];
- (n) [...] articole din domeniul tehnologiei informației [...] ⁸²;
- (o) componente identificabile ale autovehiculelor;
- (p) componente identificabile ale echipamentelor industriale;
- (q) alte obiecte de mare valoare identificabile⁸³, astfel cum sunt definite în conformitate cu alineatul (3).**

În ceea ce privește documentele menționate la alineatul (2) literele (j), (k) și (l), statul membru emitent poate preciza dacă aceste documente sunt furate, însușite în mod ilegal, pierdute, anulate sau false.

⁸² Mutat la noua literă (q).

⁸³ Mutat de la litera (n).

- (3) Definiția noilor subcategorii de obiecte de la alineatul (2) literele (n), **(o)**, **(p)** și **(q)** și normele tehnice necesare privind introducerea, actualizarea și ștergerea datelor menționate la alineatul (2), precum și privind efectuarea de căutări în acestea, se stabilesc și se dezvoltă prin intermediul unor măsuri de punere în aplicare în conformitate cu procedura de examinare menționată la articolul 72 alineatul (2).

Articolul 39

Executarea acțiunii pe baza unei semnalări

- (1) În cazul în care în urma unei căutări în date se identifică o semnalare privind un obiect care a fost localizat, autoritatea care a stabilit corespondența celor două elemente de date confiscă, în conformitate cu dreptul național, obiectul și contactează autoritatea care a emis semnalarea pentru a se ajunge la un acord privind măsurile care trebuie luate. În acest scop, se pot comunica și date cu caracter personal, în conformitate cu prezentul regulament.
- (2) Informațiile menționate la alineatul (1) se comunică printr-un schimb de informații suplimentare.
- (3) Statul membru care a localizat obiectul ia măsurile solicitate în conformitate cu dreptul național.

CAPITOLUL XI

SEMNALĂRILE PRIVIND PERSOANE CĂUTATE NECUNOSCUTE ÎN SCOPUL IDENTIFICĂRII ÎN CONFORMITATE CU DREPTUL NAȚIONAL [...]⁸⁴

Articolul 40

Semnalările privind persoane căutate necunoscute în scopul [...] identificării în temeiul dreptului național

În SIS se pot introduce date dactiloscopice care nu au legătură cu persoane care fac obiectul semnalărilor. Aceste date dactiloscopice sunt seturi complete sau incomplete de amprente digitale sau de amprente palmare care sunt descoperite la locul comiterii unor infracțiuni **grave sau al unor infracțiuni de terorism** în curs de investigare, [...] și despre care se poate stabili cu un grad ridicat de probabilitate că aparțin [...] **unui** autor al infracțiunii.

Datele dactiloscopice din această categorie se stochează cu mențiunea „persoană căutată sau suspectată necunoscută” **și numai dacă** [...] autoritățile competente **ale statului membru emitent** nu pot stabili identitatea respectivei persoane prin utilizarea niciunei alte baze de date naționale, europene sau internaționale.

Articolul 41

Executarea acțiunii pe baza unei semnalări

În cazul obținerii unui rezultat pozitiv [...] după efectuarea unei căutări în datele stocate în temeiul articolului 40, identitatea persoanei se stabilește în conformitate cu dreptul național, iar **un expert** verifică dacă datele dactiloscopice stocate în SIS aparțin respectivei persoane. Statele membre comunică **informații despre identitatea și localizarea persoanei [...] printr-un schimb de informații suplimentare** în scopul de a facilita investigarea în timp util a cazului.

⁸⁴ Mutat la noul capitol XIa.

CAPITOLUL XIa
NORME SPECIFICE PRIVIND DATELE BIOMETRICE

*Articolul **41A (fostul articol 22)***

Norme specifice privind introducerea fotografiilor, a imaginilor faciale, a datelor dactiloscopice și a profilurilor ADN

- (1) Introducerea în SIS a datelor menționate la articolul 20 alineatul (3) literele (w), (x) și (y) face obiectul următoarelor dispoziții:
- (a) fotografiile, imaginile faciale, datele dactiloscopice și profilurile ADN se introduc doar în urma unei verificări a calității pentru a se asigura îndeplinirea unui standard minim de calitate a datelor;
 - (b) se poate adăuga un profil ADN doar la semnalările prevăzute la articolul 32 alineatul (2) literele (a) și (c) și numai dacă nu sunt disponibile fotografiile, imagini faciale sau date dactiloscopice care să permită identificarea **sau dacă acestea nu sunt suficiente**. Profilurile ADN ale persoanelor care sunt ascendenți direcți, descendenți sau frați ori surori ale persoanei care face obiectul semnalării pot fi adăugate la semnalare cu condiția ca persoanele în cauză să își dea acordul explicit. [...]
- (2) Pentru stocarea datelor menționate la prezentul articol alineatul (1) litera (a) și la articolul 40 se stabilesc standarde de calitate. Specificațiile acestor standarde se stabilesc prin intermediul unor măsuri de punere în aplicare și se actualizează în conformitate cu procedura de examinare menționată la articolul 72 alineatul (2).

Articolul 42

Norme specifice privind verificarea sau efectuarea de căutări cu ajutorul fotografiilor, a imaginilor faciale, a datelor dactiloscopice și a profilurilor ADN

- (1) Fotografiile, imaginile faciale, datele dactiloscopice și profilurile ADN se extrag din SIS, **ori de câte ori este necesar**, pentru a verifica identitatea unei persoane care a fost localizată în urma unei căutări alfanumerice efectuate în SIS.
- (2) [...] **D**acă identitatea unei persoane nu poate fi stabilită prin niciun alt mijloc, **se efectuează căutări în datele dactiloscopice** [...] **în scopul identificării**. **Se pot efectua căutări** în datele dactiloscopice **în orice situație** în scopul identificării unei persoane.
- (3) Se pot efectua căutări în datele dactiloscopice stocate în SIS în legătură cu semnalări emise în temeiul articolelor 26, **32**, 34 [...], **36** și [...] **40** și prin utilizarea unor seturi complete sau incomplete de amprente digitale sau de amprente palmare descoperite la locul comiterii unor infracțiuni **grave sau al unor infracțiuni de terorism**⁸⁵ în curs de investigare și în cazul în care se poate stabili cu un grad ridicat de probabilitate că acestea aparțin **unui** autor [...] al infracțiunii [...].
- (4) De îndată ce acest lucru devine posibil din punct de vedere tehnic, asigurând totodată un nivel ridicat de fiabilitate a identificării, se pot utiliza fotografiile și imaginile faciale pentru identificarea unei persoane. **Înainte de introducerea acestei funcționalități, Comisia prezintă un raport privind disponibilitatea și gradul de adecvare al tehnologiei necesare, în legătură cu care este consultat Parlamentul European.**⁸⁶ Se recurge la identificarea pe baza fotografiilor sau a imaginilor faciale [...] **sub rezerva dreptului național** [...].

⁸⁵ Conform cu articolul 40.

⁸⁶ Similar cu textul de la articolul 22 litera (c) din Regulamentul (CE) nr. 1987/2006 din 20 decembrie 2006 privind instituirea, funcționarea și utilizarea Sistemului de informații Schengen din a doua generație (SIS II).

CAPITOLUL XII
DREPTUL DE ACCES LA SEMNALĂRI ȘI PĂSTRAREA ACESTORA

Articolul 43

Autoritățile care au drept de acces la semnalări

- (1) **Autoritățile naționale competente au drept de acces**[...] la datele introduse în SIS și dreptul de a efectua căutări în aceste date în mod direct sau într-o copie a datelor din SIS [...] **în următoarele scopuri:**
- (a) controlul la frontiere, în conformitate cu Regulamentul (UE) 2016/399 al Parlamentului European și al Consiliului din 9 martie 2016 cu privire la Codul Uniunii privind regimul de trecere a frontierelor de către persoane (Codul frontierelor Schengen);
 - (b) verificările polițienești și vamale efectuate pe teritoriul statului membru în cauză și coordonarea acestor verificări de către autoritățile desemnate;
 - (c) alte [...] activități [...] derulate pentru prevenirea, depistarea, [...] investigarea **sau urmărirea penală** a infracțiunilor **ori pentru executarea pedepselor, inclusiv apărarea împotriva amenințărilor pentru siguranța publică sau securitatea națională și prevenirea acestor amenințări** pe teritoriul statului membru în cauză;
 - (d) examinarea condițiilor și luarea deciziilor privind intrarea și șederea resortisanților țărilor terțe pe teritoriul statelor membre, [...] privind permisele de ședere, [...] privind vizele de lungă ședere, și privind returnarea resortisanților țărilor terțe.
 - (e) **verificări asupra resortisanților țărilor terțe care intră ilegal sau care stau ilegal pe teritoriul statelor membre, precum și asupra solicitanților de protecție internațională.**

(1a) Dreptul de acces la datele introduse în SIS și dreptul de a efectua căutări în mod direct în acestea pot fi exercitate de autoritățile naționale competente responsabile cu acordarea cetățeniei, în îndeplinirea sarcinilor care le revin, astfel cum se prevede în dreptul național, precum și de către autoritățile lor coordonatoare.

- (2) Dreptul de acces la datele introduse în SIS și dreptul de a efectua căutări în mod direct în acestea pot fi exercitate și de autoritățile judiciare naționale, inclusiv cele responsabile cu inițierea urmăririi penale în cadrul procedurilor penale și cu anchetele judiciare anterioare punerii sub acuzare, în îndeplinirea sarcinilor care le revin, astfel cum se prevede în dreptul național, precum și de către autoritățile lor coordonatoare.
- (3) Dreptul de acces la datele introduse în SIS și de a efectua căutări în mod direct în acestea poate fi exercitat de autoritățile competente pentru efectuarea sarcinilor prevăzute la alineatul (1) litera (c) în îndeplinirea sarcinilor respective. Accesul acestor autorități este reglementat de dreptul **național** [...].
- (4) Autoritățile menționate la prezentul articol sunt incluse pe lista prevăzută la articolul 53 alineatul (8).

Articolul 44

Autoritățile de înmatriculare a vehiculelor

- (1) Serviciile din statele membre responsabile cu eliberarea certificatelor de înmatriculare a vehiculelor, astfel cum se menționează în Directiva 1999/37/CE⁸⁷ a Consiliului, au acces la [...] datele introduse în SIS în conformitate cu articolul 38 alineatul (2) literele (a), (b), (c), [...] (l) și (o) din prezentul regulament doar în scopul de a verifica dacă **auto**vehiculele, **precum și certificatele de înmatriculare și plăcuțele de înmatriculare care le însoțesc,** care le sunt prezentate pentru înmatriculare au fost furate, însușite în mod ilegal, pierdute **sau sunt false,** ori dacă sunt căutate pentru a fi folosite ca probe în cadrul unor proceduri penale [...].

⁸⁷ Directiva 1999/37/CE a Consiliului din 29 aprilie 1999 privind documentele de înmatriculare pentru vehicule (JO L 138, 1.6.1999, p. 57).

[...]

[...]

[...]

Accesul la aceste date al serviciilor responsabile cu eliberarea certificatelor de înmatriculare pentru vehicule este reglementat de dreptul național al respectivului stat membru.

- (2) Serviciile menționate la alineatul (1) care sunt servicii publice au dreptul de a accesa în mod direct datele introduse în SIS.
- (3) Serviciile menționate la alineatul (1) care nu sunt servicii publice au dreptul de a accesa datele introduse în SIS numai prin intermediul unei autorități menționate la articolul 43 din prezentul regulament. Această autoritate are dreptul de a accesa în mod direct respectivele date și de a le transmite serviciului în cauză. Statul membru în cauză se asigură că serviciul respectiv și personalul acestuia au obligația de a respecta eventualele limitări impuse în ceea ce privește condițiile de utilizare a datelor care le sunt transmise de către autoritate.
- (4) Articolul 39 din prezentul regulament nu se aplică accesului obținut în conformitate cu prezentul articol. Comunicarea de către serviciile menționate la alineatul (1) către poliție sau autoritățile judiciare a oricărei informații care a fost obținută datorită accesului la SIS [...] este reglementată de dreptul național.

Articolul 45

Autoritățile de înmatriculare a ambarcațiunilor și a aeronavelor

- (1) Serviciile din statele membre responsabile cu eliberarea certificatelor de înmatriculare sau cu asigurarea gestionării traficului pentru ambarcațiuni, inclusiv motoare de ambarcațiuni, și aeronave au acces la următoarele date introduse în SIS în conformitate cu articolul 38 alineatul (2) din prezentul regulament doar în scopul de a verifica dacă ambarcațiunile, inclusiv motoarele de ambarcațiuni[...], aeronavele, **inclusiv motoarele aeronautice** [...] care le sunt prezentate pentru înmatriculare sau care fac obiectul gestionării traficului au fost furate, însușite în mod ilegal sau pierdute ori dacă sunt căutate pentru a fi folosite ca probe în cadrul unor proceduri penale:

- (a) date privind ambarcațiuni;
- (b) date privind motoare de ambarcațiuni;
- (c) date privind aeronave;

(d) date privind motoare aeronautice.

Sub rezerva alineatului (2), dreptul fiecărui stat membru reglementează accesul acestor servicii la datele respective în statul membru în cauză. Accesul la datele enumerate la literele (a)-(d[...]) de mai sus se limitează la competența specifică a serviciilor în cauză.

- (2) Serviciile menționate la alineatul (1) care sunt servicii publice au dreptul de a accesa în mod direct datele introduse în SIS.
- (3) Serviciile menționate la alineatul (1) care nu sunt servicii publice au dreptul de a accesa datele introduse în SIS numai prin intermediul unei autorități menționate la articolul 43 din prezentul regulament. Această autoritate are dreptul de a accesa în mod direct datele și de a le transmite serviciului în cauză. Statul membru în cauză se asigură că serviciul respectiv și personalul acestuia au obligația de a respecta eventualele limitări impuse în ceea ce privește condițiile de utilizare a datelor care le sunt transmise de către autoritatea respectivă.
- (4) Articolul 39 din prezentul regulament nu se aplică accesului obținut în conformitate cu prezentul articol. Comunicarea de către serviciile menționate la alineatul (1) poliției sau autorităților judiciare a oricărei informații care a fost obținută datorită accesului la SIS și care generează suspiciunea comiterii unei infracțiuni este reglementată de dreptul național.

Articolul 45A

Autoritățile de înregistrare a armelor de foc

- (1) Serviciile din statele membre responsabile cu eliberarea certificatelor de înregistrare a armelor de foc au drept de acces la datele privind persoanele care fac obiectul unei semnalări în temeiul articolului 26 sau al articolului 36, precum și la date privind armele de foc introduse în SIS în conformitate cu articolul 38 alineatul (2) din prezentul regulament în scopul de a verifica dacă persoana care solicită înregistrarea reprezintă o amenințare pentru siguranța națională sau securitatea publică sau dacă armele de foc care le sunt prezentate pentru a fi înregistrate sunt căutate pentru a fi confiscate sau pentru a fi folosite ca probe în cursul procedurilor penale.
- (2) Accesul acestor servicii la datele respective este reglementat de dreptul național al statului membru în cauză⁸⁸. Accesul la aceste date se limitează în funcție de competența specifică a serviciilor în cauză.
- (3) Serviciile menționate la alineatul (1) care sunt autorități competente pot avea dreptul de a accesa în mod direct datele introduse în SIS.
- (4) Serviciile menționate la alineatul (1) care nu sunt autorități competente au dreptul de a accesa datele introduse în SIS numai prin intermediul unei autorități dintre cele menționate la articolul 43 din prezentul regulament. Autoritatea intermediară are dreptul de a accesa datele în mod direct și informează serviciul în cauză dacă arma de foc poate fi înregistrată sau nu. Statul membru se asigură că serviciul respectiv și personalul acestuia sunt obligați să respecte toate restricțiile stabilite în ceea ce privește condițiile de utilizare a datelor care le sunt transmise de către autoritatea intermediară.
- (5) Articolul 39 nu se aplică accesului obținut în conformitate cu prezentul articol. Comunicarea de către serviciile menționate la alineatul (1) către poliție sau autoritățile judiciare a oricărei informații care a fost obținută datorită accesului la SIS este reglementată de dreptul național.

⁸⁸ Formulare conformă cu articolul 44 alineatul (1) ultimul paragraf.

Articolul 46
Accesul Europolului la datele SIS

- (1) Agenția Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) are, în limitele mandatului său, dreptul de a accesa și de a efectua căutări în datele introduse în SIS **și poate prelucra informații suplimentare și face schimb de informații suplimentare în conformitate cu dispozițiile din Manualul SIRENE prevăzute la articolul 8.**
- (2) Atunci când o căutare efectuată de Europol indică existența unei semnalări în SIS, Europolul informează statul membru emitent **printr-un schimb de informații suplimentare. Până când Europolul va implementa funcționalitatea pentru schimbul de informații suplimentare, acesta informează statul membru emitent prin** canalele definite în Regulamentul (UE) 2016/794.
- (2a) Europolul poate prelucra informațiile suplimentare pe care i le-au furnizat statele membre în scopul verificării încrucișate, utilizate pentru a identifica conexiunile sau alte legături relevante, precum și pentru analizele strategice, tematice și operationale, astfel cum sunt definite la articolul 18 alineatul (2) literele (a) și (c) din Regulamentul (UE) 2016/794. Orice prelucrare de către Europol a informațiilor suplimentare se efectuează în conformitate cu Regulamentul (UE) 2016/794.**
- (3) Utilizarea informațiilor obținute în urma efectuării unei căutări în [...] SIS **sau a prelucrării de informații suplimentare** este condiționată de acordul statului membru **emitent** [...]. Dacă statul membru autorizează utilizarea informațiilor respective, tratarea acestora de către Europol intră sub incidența Regulamentului (UE) 2016/794. Europolul poate comunica aceste informații țărilor terțe și organismelor terțe numai cu acordul statului membru **emitent** [...].
- (4) [...] ⁸⁹

⁸⁹ În conformitate cu Regulamentul 2016/794, Europolul poate solicita statelor membre, în orice situație, informații legate de infracțiunile care intră în mandatul acestuia. Prin urmare, se poate considera că alineatul (4) este redundant.

(5) Europolul:

(a) fără a aduce atingere alineatelor (3) [...] și (6), nu conectează părți ale SIS la niciun sistem informatic, nu transferă datele din SIS la care are acces către niciun sistem informatic pentru colectarea și prelucrarea datelor efectuate de către Europol sau în cadrul acestuia și nici nu descarcă sau copiază în alt mod vreo parte din SIS;

(aa) în pofida articolului 31 alineatul (1) din Regulamentul (UE) 2016/794, șterge informațiile suplimentare care conțin date cu caracter personal cel târziu la un an de la ștergerea semnalării conexe din SIS, cu excepția cazului în care se consideră necesară menținerea stocării datelor, pe baza unor informații care sunt mai exhaustive decât cele deținute de furnizorul datelor, astfel încât Europolul să își îndeplinească atribuțiile. Europolul informează furnizorul datelor despre menținerea stocării datelor respective și prezintă o motivare în acest sens;

(b) limitează accesul la datele introduse în SIS, **inclusiv la informațiile suplimentare**, la personalul autorizat în mod explicit în acest sens al Europolului;

(c) adoptă și aplică măsurile prevăzute la articolele 10 și 11; **și**

(d) permite Autorității Europene pentru Protecția Datelor să reexamineze activitățile pe care le desfășoară Europolul în exercitarea dreptului său de a accesa datele introduse în SIS și de a face căutări în acestea, **precum și în ceea ce privește schimbul de informații suplimentare și prelucrarea acestora.**

(6) Se pot copia date numai în scopuri tehnice, cu condiția ca respectiva copiere să fie necesară pentru ca personalul Europolului autorizat în mod corespunzător să efectueze o căutare directă. Dispozițiile prezentului regulament se aplică și acestor copii. Copia tehnică se utilizează pentru stocarea datelor din SIS în timp ce se efectuează căutări în aceste date. După ce s-au efectuat căutări în date, acestea trebuie șterse. Aceste utilizări nu se consideră a constitui o descărcare sau o copiere ilegală a datelor din SIS. Europolul nu copiază în alte sisteme ale sale datele semnalărilor sau datele suplimentare emise de statele membre și nici datele din CS-SIS.

- (7) [...]
- (8) [...]
- (9) În scopul verificării legalității prelucrării datelor, al automonitorizării și al asigurării securității și integrității corespunzătoare a datelor, Eurojustul [...] păstrează înregistrările fiecărei accesări a SIS și fiecărei căutări în SIS **în conformitate cu articolul 12**. Nu se consideră că aceste înregistrări și documentații constituie o descărcare sau o copiere ilegală a vreunei părți din SIS.

Articolul 47

Accesul Eurojustului la datele SIS

- (1) Membrii naționali ai Eurojustului și asistenții acestora au dreptul, în limitele mandatului lor, de a accesa și de a efectua căutări în datele introduse în SIS, în conformitate cu articolele 26, 32, 34, 38 și 40.
- (2) În cazul în care o căutare efectuată de un membru național al Eurojustului indică existența unei semnalări în SIS, acesta informează statul membru emitent **despre acest lucru. Orice comunicare a informațiilor obținute în urma unei astfel de căutări poate fi comunicată unor țări și organisme terțe numai cu acordul statului membru emitent.**
- (3) Nicio dispoziție a prezentului articol nu se interpretează ca aducând atingere dispozițiilor Deciziei 2002/187/JAI referitoare la protecția datelor și la răspunderea pentru orice prelucrare neautorizată sau incorectă a acestor date de către membrii naționali ai Eurojustului sau asistenții acestora ori ca afectând competențele organului de control comun instituit în temeiul deciziei menționate.

- (4) Fiecare accesare și fiecare căutare efectuate de un membru național al Eurojustului sau de un asistent al acestuia se înregistrează în conformitate cu dispozițiile articolului 12 și fiecare utilizare de către aceștia a datelor accesate se înregistrează.
- (5) Nicio parte a SIS nu se conectează la un sistem informatic pentru colectarea și prelucrarea datelor efectuate de Eurojust sau în cadrul acestuia și nici nu se transferă către un astfel de sistem datele din SIS la care au acces membrii naționali sau asistenții acestora. Nicio parte a SIS nu se descarcă. Înregistrarea accesului și a căutărilor nu se consideră a constitui o descărcare sau o copiere ilegală a datelor din SIS.
- (6) Accesul la datele introduse în SIS se limitează la membrii naționali și la asistenții acestora și nu se extinde la personalul Eurojustului.
- (7) Se adoptă și se aplică măsuri pentru asigurarea securității și a confidențialității, astfel cum se prevede la articolele 10 și 11.

Articolul 48

Accesul la datele din SIS de către echipele europene de poliție de frontieră și gardă de coastă, echipele formate din personalul implicat în sarcini legate de returnare și membrii echipelor⁹⁰ de sprijin pentru gestionarea migrației

- (1) [...] **Membrii** echipelor europene de poliție de frontieră și gardă de coastă sau echipele formate din personalul implicat în sarcini legate de returnare și membrii echipelor de sprijin pentru gestionarea migrației, **înființate în conformitate cu articolele 18, 20 și 32 din Regulamentul (UE) 2016/1624**, au, în limitele mandatului lor **și cu condiția să fie autorizate să efectueze controale în conformitate cu articolul 43**, dreptul de a accesa datele introduse în SIS și de a face căutări în acestea [...]. **Accesul la datele introduse în SIS nu se acordă membrilor altor echipe⁹¹.**

⁹⁰ Forma de plural, ca în Regulamentul (UE) 2018/...

⁹¹ Text mutat de la alineatul (5).

- (2) Membrii echipelor europene de poliție de frontieră și gardă de coastă sau ai echipelor formate din personalul implicat în sarcini legate de returnare, precum și membrii echipelor de sprijin pentru gestionarea migrației **își exercită dreptul de** acces și efectuează căutări în datele introduse în SIS în conformitate cu alineatul (1) prin intermediul interfeței tehnice înființate și întreținute de Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă, astfel cum se menționează la articolul 49 alineatul (1).
- (3) În cazul în care o căutare efectuată de un membru al echipelor europene de poliție de frontieră și gardă de coastă sau al echipelor formate din personalul implicat în sarcini legate de returnare sau de un membru al echipelor de sprijin pentru gestionarea migrației indică existența unei semnalări în SIS, statul membru emitent este informat cu privire la aceasta. În conformitate cu articolul 40 din Regulamentul (UE) 2016/1624, membrii echipelor pot acționa ca răspuns la o semnalare în SIS numai dacă primesc instrucțiuni de la polițiștii de frontieră sau de la membrii personalului implicați în sarcini legate de returnare ai statului membru gazdă în care își desfășoară activitatea și, ca regulă generală, în prezența acestora. Statul membru gazdă poate autoriza membrii echipelor să acționeze în numele său.
- (4) Fiecare accesare a datelor și fiecare căutare în acestea de către un membru al echipelor europene de poliție de frontieră și gardă de coastă sau al echipelor formate din personalul implicat în sarcini legate de returnare sau de un membru al echipelor de sprijin pentru gestionarea migrației se înregistrează în conformitate cu dispozițiile articolului 12, la fel ca și fiecare utilizare de către membrul respectiv a datelor pe care le-a accesat.
- (5) [...] ⁹²
- (6) **Echipele europene de poliție de frontieră și gardă de coastă sau echipele formate din personalul implicat în sarcini legate de returnare sau membrii echipelor de sprijin pentru gestionarea migrației iau** măsuri pentru a asigura securitatea și confidențialitatea, astfel cum se prevede la articolele 10 și 11 [...].

⁹² Fuzionat cu alineatul (1).

Articolul 49

Accesul la SIS al Agenției Europene pentru Poliția de Frontieră și Garda de Coastă

- (1) În sensul articolului 48 alineatul (1) [și al [...] articolului **49A**], Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă înființează și întreține o interfață tehnică care permite conectarea directă la SIS central.
- (2)⁹³ [...]
- (3)⁹⁴ [...]
- (4) Nicio dispoziție a prezentului articol nu se interpretează ca aducând atingere dispozițiilor Regulamentului (UE) 2016/1624 privind protecția datelor și răspunderea pentru orice prelucrare neautorizată sau incorectă a acestor date de către Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă.
- (5) Fiecare accesare a datelor și fiecare căutare în acestea de către Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă se înregistrează în conformitate cu dispozițiile articolului 12, la fel ca și fiecare utilizare de către aceasta a datelor pe care le-a accesat.
- (6) **Cu excepția cazurilor în care se aplică alineatul (1) al prezentului articol**, nicio parte a SIS nu se conectează la un sistem informatic pentru colectarea și prelucrarea datelor efectuate de către Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă sau în cadrul acesteia și nici nu se transferă către un astfel de sistem datele din SIS la care are acces Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă. Nicio parte a SIS nu se descarcă. Înregistrarea accesului și a căutărilor nu se consideră a constitui o descărcare ilegală sau o copiere ilegală a datelor din SIS.

⁹³ Alineat mutat la articolul 49A alineatul (1).

⁹⁴ Alineat mutat la articolul 49A alineatul (2).

- (7) **Agencia Europeană pentru Poliția de Frontieră și Garda de Coastă** ia măsuri pentru a asigura securitatea și confidențialitatea, astfel cum se prevede la articolele 10 și 11 [...].

[Articolul 49A]⁹⁵

Accesul la datele din SIS de către unitatea centrală a ETIAS

- (1) **Agencia Europeană pentru Poliția de Frontieră și Garda de Coastă are dreptul de a accesa și de a efectua căutări în datele introduse în SIS, în conformitate cu articolele 26, 32, 34 și 36 și cu articolul 38 alineatul (2) literele (i) și (k), în scopul de a-și îndeplini sarcinile care i-au fost atribuite prin Regulamentul de instituire a Sistemului european de informații și de autorizare privind călătoriile (ETIAS).**
- (2) **În cazul în care o verificare efectuată de Agencia Europeană pentru Poliția de Frontieră și Garda de Coastă indică existența unei semnalări în SIS, se aplică procedura prevăzută la articolele 18, 20A și 22 din Regulamentul de instituire a Sistemului european de informații și de autorizare privind călătoriile (ETIAS)]⁹⁶.**

Articolul 49B

Evaluarea utilizării SIS de Europol, Eurojust și Agencia Europeană pentru Poliția de Frontieră și Garda de Coastă

- (1) **Comisia realizează, cel puțin o dată la cinci ani, o evaluare a funcționării și a utilizării SIS conform prezentului regulament de Europol, Eurojust și Agencia Europeană pentru Poliția de Frontieră și Garda de Coastă.**

⁹⁵ Dispoziții mutate de la articolul 49 alineatele (2) și (3).

⁹⁶ Conținutul și/sau introducerea acestor dispoziții depind de textul final al propunerii de regulament al Parlamentului European și al Consiliului de instituire a Sistemului european de informații și de autorizare privind călătoriile (ETIAS) și de modificare a Regulamentelor (UE) nr. 515/2014, (UE) 2016/399, (UE) 2016/794 și (UE) 2016/1624 (a se vedea doc. 10017/17) și de data intrării sale în vigoare.

- (2) Echipa responsabilă cu această evaluare la fața locului este formată din cel mult doi reprezentanți ai Comisiei, asistați de cel mult opt experți desemnați de statele membre. [...]
- (3) Comisia întocmește un raport de evaluare după fiecare evaluare, în consultare cu experții desemnați de statele membre. Raportul de evaluare se bazează pe constatările echipei de evaluare la fața locului și analizează aspectele calitative, cantitative, operaționale, administrative și organizaționale ale funcționării și utilizării SIS, după caz, și enumeră toate deficiențele identificate în cursul evaluării.
- (4) Europolul, Eurojustul și Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă au ocazia de a transmite observații înainte de adoptarea raportului.
- (5) Raportul de evaluare se transmite Parlamentului European și Consiliului. Raportul de evaluare se clasifică drept document EU RESTRICTED/RESTREINT UE, în conformitate cu normele de securitate aplicabile. Clasificarea nu împiedică punerea informațiilor la dispoziția Parlamentului European.
- (6) Având în vedere constatările și evaluările cuprinse în raportul de evaluare respectiv, Comisia elaborează recomandări privind acțiuni de remediere vizând abordarea eventualelor deficiențe identificate în timpul evaluării, oferind indicații referitoare la prioritățile pentru punerea lor în aplicare, precum și, după caz, exemple de bune practici.
- (7) În urma unei evaluări, Europolul, Eurojustul și Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă îi furnizează Comisiei un plan de acțiune în scopul remedierii eventualelor deficiențe identificate în raportul de evaluare, continuând apoi să raporteze din trei în trei luni, până la punerea în aplicare deplină a raportului, în privința progreselor înregistrate.

Articolul 50
Limitele de acces

Utilizatorii finali, inclusiv Europolul, membrii naționali ai Eurojustului și asistenții acestora, [...] Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă [...], **membrii echipelor europene de politie de frontieră și gardă de coastă sau ai echipelor formate din personalul implicat în sarcini legate de returnare, precum și membrii echipelor de sprijin pentru gestionarea migrației** pot accesa doar datele care le sunt necesare în scopul îndeplinirii sarcinilor care le revin.

Articolul 51
*Perioada de păstrare a semnalărilor - persoane*⁹⁷

- (1) Semnalările **privind persoane** introduse în SIS în temeiul prezentului regulament se păstrează numai pe durata necesară îndeplinirii scopurilor pentru care au fost introduse.
- (2) **În legătură cu semnalările privind persoane:**
 - (a) **Un stat membru poate emite o semnalare pentru o perioadă de cinci ani.**
 - (b) [...] Statul membru emitent [...] reexaminează, în termen de cinci ani de la introducerea **semnalării** [...] în SIS, nevoia de a o păstra. [...] ⁹⁸ [...]
- (3) [...]

⁹⁷ S-a introdus un nou articol 51A pentru a reglementa perioada de păstrare a semnalărilor privind obiectele.

⁹⁸ Mutat la alineatul (3).

Prin derogare de la alineatul (2), în legătură cu semnalările emise în sensul articolului 32 alineatul (2) literele (c) și (d) și al articolului 36 din prezentul regulament⁹⁹:

(a) Un stat membru poate emite o semnalare pentru o perioadă de un an.

(b) Statul membru emitent reexaminează, în termen de un an de la introducerea semnalării în SIS, nevoia de a o păstra.

(4) Fiecare stat membru stabilește, după caz, perioade de reexaminare mai scurte, în conformitate cu dreptul său național.

(5) **În timpul perioadei de reexaminare, statul membru emitent poate decide, în urma unei evaluări individuale cuprinzătoare care se înregistrează, să păstreze semnalarea mai mult timp, dacă acest lucru se dovedește necesar pentru scopul în care a fost emisă semnalarea privind o persoană. În această situație, alineatul (2) litera (a) sau alineatul (3) litera (a), după caz, se aplică și prelungirii termenului de păstrare. Orice prelungire a termenului de păstrare a unei semnalări se comunică CS-SIS¹⁰⁰.**

[...] ¹⁰¹

⁹⁹ Text mutat parțial de la alineatul (2).

¹⁰⁰ Mutat de la alineatul (2) litera (a).

¹⁰¹ Mutat la alineatul (8).

(6) [...] ¹⁰²

Semnalările se șterg automat după expirarea perioadei de reexaminare menționate la alineatul (2) **litera (b) și la alineatul (3) litera (b)**, cu excepția cazurilor în care statul membru **emitent** a informat CS-SIS despre prelungirea termenului de păstrare a semnalării **privind o persoană** în temeiul alineatului **(5)**. CS-SIS informează automat statele membre despre ștergerea programată a datelor din sistem, cu patru luni în prealabil¹⁰³.

(7) [...] ¹⁰⁴

Statele membre întocmesc statistici referitoare la numărul semnalărilor **privind persoane** a căror perioadă de păstrare a fost prelungită în conformitate cu alineatul [...] **(5)**¹⁰⁵.

(8) [...] ¹⁰⁶

¹⁰² Mutat la alineatul (2) litera (a).

¹⁰³ Mutat de la alineatul (7).

¹⁰⁴ Mutat la alineatul (6).

¹⁰⁵ Mutat de la alineatul (8).

¹⁰⁶ Mutat la alineatul (7).

În cazurile în care devine clar pentru personalul biroului SIRENE, care este responsabil de coordonarea și verificarea calității datelor, că o semnalare privind o persoană și-a atins scopul și ar trebui să fie ștearsă din SIS, personalul **aduce acest fapt în atenția** [...] autorității care a creat semnalarea [...]. Autoritatea are la dispoziție 30 de zile calendaristice de la data primirii notificării pentru a indica că semnalarea a fost ștearsă sau va fi ștearsă ori pentru a motiva păstrarea semnalării. Dacă perioada de 30 de zile expiră fără un astfel de răspuns, semnalarea se șterge de personalul biroului SIRENE, **dacă acest lucru este permis în temeiul dreptului național**. Birourile SIRENE raportează autorității lor naționale de supraveghere toate problemele recurente în acest domeniu¹⁰⁷.

Articolul 51A¹⁰⁸

Perioada de păstrare a semnalărilor - obiecte

- (1) Semnalările privind obiectele introduse în SIS în temeiul prezentului regulament se păstrează numai atât timp cât este necesar pentru realizarea scopurilor în care au fost introduse.**
- (2) În legătură cu semnalările privind obiecte:**
 - (a) Un stat membru poate emite o semnalare privind obiecte pentru o perioadă de zece ani.**
 - (b) Un stat membru poate emite o semnalare privind alte obiecte în conformitate cu articolele 26, 32, 34, 36 sau 38 pentru o perioadă de cinci ani dacă aceasta este legată de o semnalare privind persoane.**
 - (c) Perioadele de păstrare menționate la alineatul (2) literele (a) și (b) pot fi prelungite dacă acest lucru se dovedește necesar pentru scopul în care a fost emisă semnalarea. În acest caz, alineatul (2) literele (a) și (b) se aplică și prelungirii.**
 - (d) Pentru categoriile de semnalări privind obiecte se pot stabili perioade de păstrare mai scurte prin intermediul unor măsuri de punere în aplicare adoptate în conformitate cu procedura de examinare menționată la articolul 72 alineatul (2).**

¹⁰⁷ Mutat de la alineatul (5).

¹⁰⁸ Acest articol nou se referă în mod specific la perioada de păstrare a semnalărilor privind obiecte și reproduce, *mutatis mutandis*, dispozițiile referitoare la perioada de păstrare a semnalărilor privind persoane (articolul 51).

- (3) Statele membre întocmesc statistici privind numărul semnalărilor privind obiecte a căror perioadă de păstrare a fost prelungită în conformitate cu alineatul (2) litera (c).**

CAPITOLUL XIII ȘTERGEREA SEMNALĂRILOR

Articolul 52

Ștergerea semnalărilor

- (1) Semnalările în vederea arestării în scopul predării sau al extrădării prevăzute la articolul 26 se șterg după ce persoana în cauză a fost predată sau extrădată autorităților competente din statul membru emitent. Ștergerea **se efectuează** [...] și atunci când hotărârea judecătorească în temeiul căreia s-a emis semnalarea a fost revocată de autoritatea judiciară competentă conform dreptului național.
- (2) Semnalările privind **persoane** dispărute, **copii expuși riscului de răpire sau persoane vulnerabile în temeiul articolului 32** se șterg în conformitate cu următoarele norme:
- (a) În legătură cu copiii dispăruți [...] **și cu copiii expuși riscului de răpire** [...], semnalarea se șterge:
- după soluționarea cazului, de exemplu atunci când copilul a fost repatriat sau autoritățile competente din statul membru de executare au adoptat o decizie privind îngrijirea copilului;
 - la încetarea valabilității semnalării în conformitate cu articolul 51;
 - după adoptarea unei decizii de către autoritatea competentă a statului membru emitent; sau
 - [...]
 - **când a dispărut riscul de răpire.**

- (b) În legătură cu adulții dispăruți [...], în cazul în care nu se solicită măsuri de protecție, semnalarea se șterge:
- după executarea acțiunii care trebuie întreprinsă (statul membru de executare a stabilit locul unde se află persoana);
 - la încetarea valabilității semnalării în conformitate cu articolul 51; sau
 - după adoptarea unei decizii de către autoritatea competentă a statului membru emitent.
- (c) În legătură cu adulții dispăruți, în cazul în care se solicită măsuri de protecție [...], semnalarea se șterge:
- după executarea acțiunii care trebuie întreprinsă (persoana a fost plasată sub protecție);
 - la încetarea valabilității semnalării în conformitate cu articolul 51; sau
 - după adoptarea unei decizii de către autoritatea competentă a statului membru emitent.
- (d) În legătură cu persoanele vulnerabile care trebuie împiedicate să călătorească pentru propria lor protecție, semnalarea se șterge:**
- **după executarea acțiunii care trebuie întreprinsă (persoana a fost plasată sub protecție);**
 - **la încetarea valabilității semnalării în conformitate cu articolul 51; sau**
 - **după adoptarea unei decizii de către autoritatea competentă a statului membru emitent**¹⁰⁹.

Sub rezerva dreptului național, în cazul în care o persoană a fost internată în urma deciziei unei autorități competente, semnalarea poate fi păstrată până la repatrierea respectivei persoane.

¹⁰⁹ Text similar celui de la litera (c).

- (3) [...] În legătură cu semnalările privind persoane căutate în scopul unei proceduri judiciare în temeiul articolului 34, semnalarea se șterge:
- (a) după ce locul unde se află persoana a fost comunicat autorității competente a statului membru emitent. În cazul în care nu se pot întreprinde acțiuni pe baza informațiilor transmise, biroul SIRENE al statului membru emitent informează biroul SIRENE al statului membru de executare pentru a soluționa problema;
 - (b) la încetarea valabilității semnalării în conformitate cu articolul 51; sau
 - (c) după adoptarea unei decizii de către autoritatea competentă a statului membru emitent.
- În cazul în care s-a obținut un rezultat pozitiv într-un stat membru, iar datele privind adresa au fost transmise statului membru emitent și un rezultat pozitiv obținut ulterior în respectivul stat membru indică aceleași date privind adresa, rezultatul pozitiv se înregistrează în statul membru de executare, însă nu se retrimite statului membru emitent nici datele privind adresa, nici informații suplimentare. În aceste cazuri, statul membru de executare informează statul membru emitent cu privire la rezultatele pozitive repetate și statul membru emitent analizează necesitatea de a menține semnalarea.
- (4) [...] În ceea ce privește semnalările în scopul efectuării de controale discrete, de verificări prin interviu sau de controale specifice prevăzute la articolul 36, semnalarea se șterge:
- (d) la încetarea valabilității semnalării în conformitate cu articolul 51;
 - (e) după adoptarea de către autoritatea competentă a statului membru emitent a unei decizii de ștergere a acesteia.

- (5) [...] În ceea ce privește ștergerea semnalărilor privind obiecte căutate pentru a fi confiscate sau folosite ca probe în cadrul unor proceduri penale prevăzute la articolul 38, semnalarea se șterge:
- (a) după confiscarea obiectului sau în cazul unei măsuri echivalente după efectuarea schimbului necesar ulterior de informații suplimentare între birourile SIRENE sau atunci când obiectul este vizat de o altă procedură judiciară sau administrativă;
 - (b) la încetarea valabilității semnalării; sau
 - (c) după adoptarea de către autoritatea competentă a statului membru emitent a unei decizii de ștergere a acesteia.
- (6) Semnalările privind persoane căutate necunoscute prevăzute la articolul 40 se șterg în conformitate cu următoarele norme:
- [...](a) după identificarea persoanei; sau
 - [...](b) la încetarea valabilității semnalării.

CAPITOLUL XIV
NORME GENERALE DE PRELUCRARE A DATELOR

Articolul 53

Prelucrarea datelor din SIS

- (1) Statele membre pot prelucra datele menționate la articolul 20 numai în scopurile prevăzute pentru fiecare categorie de semnalări menționată la articolele 26, 32, 34, 36, 38 și 40.
- (2) Datele se pot copia doar în scopuri tehnice, cu condiția ca această copiere să fie necesară pentru ca autoritățile menționate la articolul 43 să poată efectua o căutare directă **sau pentru ca agentia să asigure disponibilitatea neîntreruptă a SIS central**. Dispozițiile prezentului regulament se aplică și acestor copii. Un stat membru nu copiază datele semnalărilor sau datele suplimentare introduse de un alt stat membru din sistemul său N.SIS sau din CS-SIS în alte fișiere de date naționale.
- (3) Copiile tehnice, astfel cum se menționează la alineatul (2), care conduc la baze de date offline se pot păstra maximum 48 de ore. Această perioadă se poate prelungi în caz de urgență până la încetarea urgenței.
- (4) Statele membre țin un inventar actualizat al acestor copii, îl pun la dispoziția autorității lor naționale de supraveghere și se asigură că dispozițiile prezentului regulament, în special cele ale articolului 10, se aplică în cazul acestor copii.
- (5) Accesul la date este autorizat numai în limitele competenței autorităților naționale menționate la articolul 43 și numai pentru personalul autorizat în mod corespunzător.

- (6) În ceea ce privește semnalările prevăzute la articolele 26, 32, 34, 36, 38 și 40 din prezentul regulament, orice prelucrare a informațiilor conținute de acestea în alte scopuri decât cele pentru care au fost introduse în SIS trebuie să aibă legătură cu un caz specific și să fie justificată de necesitatea de a preveni o amenințare gravă iminentă pentru ordinea publică și siguranța publică, de motive întemeiate de securitate națională sau în scopul prevenirii unei infracțiuni grave. În acest scop, se obține o autorizare prealabilă din partea statului membru care a emis semnalarea.
- (7) Orice utilizare a datelor care contravine alineatelor (1)-(6) se consideră a fi utilizare abuzivă în temeiul dreptului național al fiecărui stat membru.
- (8) Fiecare stat membru trimite agenției o listă a autorităților sale competente care sunt autorizate să efectueze în mod direct căutări în datele din SIS în temeiul prezentului regulament, precum și orice modificări aduse acestei liste. Lista specifică, pentru fiecare autoritate, datele în care aceasta poate efectua căutări și în ce scopuri. Agenția asigură publicarea anuală a listei în *Jurnalul Oficial al Uniunii Europene*.
- (9) În măsura în care dreptul Uniunii nu stabilește dispoziții specifice, dreptul fiecărui stat membru se aplică datelor introduse în sistemul său N.SIS.

Articolul 54

Datele din SIS și fișierele naționale

- (1) Articolul 53 alineatul (2) nu aduce atingere dreptului unui stat membru de a păstra în fișierele sale naționale date din SIS în legătură cu care s-a întreprins o acțiune pe teritoriul său. Aceste date se păstrează în fișierele naționale pentru o perioadă maximă de trei ani, cu excepția cazului în care dispoziții specifice din dreptul național prevăd o perioadă de păstrare mai îndelungată.
- (2) Articolul 53 alineatul (2) nu aduce atingere dreptului unui stat membru de a păstra în fișierele sale naționale datele dintr-o anumită semnalare emisă în SIS de respectivul stat membru.

Articolul 55

Informații în cazul neexecutării semnalării

Dacă o acțiune solicitată nu poate fi întreprinsă, statul membru solicitat informează imediat statul membru **emitent** [...] **printr-un schimb de informații suplimentare**.

Articolul 56

Calitatea datelor prelucrate în SIS

- (1) Statul membru **emitent** [...] este responsabil să asigure că datele sunt exacte, actualizate și introduse în mod legal în SIS.
- (2) Numai statul membru **emitent** [...] este autorizat să modifice, să completeze, să corecteze, să actualizeze sau să șteargă datele pe care le-a introdus.
- (3) În cazul în care un stat membru, altul decât cel care a emis semnalarea, are probe care sugerează că un element al datelor conține erori de fapt sau a fost stocat ilegal, respectivul stat membru aduce acest fapt la cunoștința statului membru emitent, printr-un schimb de informații suplimentare, cât mai curând posibil și în maximum 10 zile de la data la care a identificat probele respective. Statul membru emitent verifică respectiva comunicare și, dacă este necesar, corectează sau șterge imediat elementul în cauză.
- (4) În cazul în care statele membre nu ajung la un acord în termen de două luni de la data identificării inițiale a probelor, astfel cum se descrie la alineatul (3), statul membru care nu a emis semnalarea sesizează **Autoritatea Europeană pentru Protecția Datelor care acționează ca mediator împreună cu** autoritățile naționale de supraveghere competente [...] ¹¹⁰.

¹¹⁰ Text inspirat din articolul 49 alineatul (4) din Decizia 2007/533/JAI a Consiliului.

- (5) Statele membre fac schimb de informații suplimentare în cazul în care o persoană depune o plângere în care susține că nu este persoana vizată de o semnalare. În cazul în care rezultatul verificării arată că, de fapt, este vorba de două persoane diferite, reclamantul este informat cu privire la măsurile prevăzute la articolul 59.
- (6) În cazul în care o persoană face deja obiectul unei semnalări în SIS, statul membru care introduce o nouă semnalare **tine seama de compatibilitate și respectă prioritatea semnalărilor și, dacă este necesar, face schimb de informații suplimentare** [...].

Articolul 57

Incidente de securitate

- (1) Orice eveniment care are sau poate avea un impact asupra securității SIS [...] **sau** care poate cauza daune sau pierderi datelor din SIS **sau informațiilor suplimentare** este considerat a fi un incident de securitate, în special în cazul în care este posibil să se fi accesat datele sau în cazul în care au fost afectate sau este posibil să fi fost afectate disponibilitatea, integritatea și confidențialitatea datelor.
- (2) Incidentele de securitate se gestionează astfel încât să se asigure un răspuns rapid, eficace și corespunzător.
- (3) Statele membre, **Europolul, Eurojustul și Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă** notifică incidentele de securitate Comisiei, agenției și autorității naționale de supraveghere. Agenția notifică incidentele de securitate Comisiei și Autorității Europene pentru Protecția Datelor.
- (4) Informațiile referitoare la un incident de securitate care are sau care poate să aibă un impact asupra funcționării SIS într-un stat membru sau în cadrul agenției sau asupra disponibilității, a integrității și a confidențialității datelor introduse sau trimise de alte state membre **sau a informațiilor suplimentare schimbate** se pun la dispoziția **tuturor** statelor membre și se raportează în conformitate cu planul de gestionare a incidentelor furnizat de agenție.

Articolul 58

Diferențierea persoanelor care prezintă caracteristici similare

În cazul în care, la momentul introducerii unei noi semnalări, se constată că există deja în SIS o persoană cu aceleași elemente de descriere a identității, se aplică următoarea procedură:

- (b) (a) biroul SIRENE contactează autoritatea solicitantă pentru a clarifica dacă semnalarea se referă sau nu la aceeași persoană; **și**
- (c) (b) în cazul în care verificarea încrucișată arată că persoana care face obiectul noii semnalări este într-adevăr persoana deja înregistrată în SIS, biroul SIRENE aplică procedura privind introducerea de semnalări multiple, astfel cum se menționează la articolul 56 alineatul (6). În cazul în care rezultatul verificării arată că, de fapt, sunt două persoane diferite, biroul SIRENE aprobă cererea de introducere a celei de a doua semnalări, adăugând elementele necesare pentru a se evita orice identificare eronată.

Articolul 59

Date suplimentare în scopul tratării cazurilor de uzurpare de identitate

- (1) În cazul în care pot apărea confuzii între o persoană care face, de fapt, obiectul unei semnalări și o persoană a cărei identitate a fost uzurpată, statul membru emitent adaugă în semnalare, pentru a se evita consecințele negative ale identificării eronate și sub rezerva acordului explicit al respectivei persoane, date care o privesc.
- (2) Datele privind o persoană a cărei identitate a fost uzurpată se folosesc doar în următoarele scopuri:
 - (a) pentru a permite autorității competente să distingă între persoana a cărei identitate a fost uzurpată și persoana care face, de fapt, obiectul semnalării;
 - (b) pentru a permite persoanei a cărei identitate a fost uzurpată să își dovedească identitatea și pentru a se stabili faptul că identitatea sa a fost uzurpată.

(3) În scopul prezentului articol, se pot introduce și prelucra ulterior în SIS doar următoarele date cu caracter personal **ale persoanei a cărei identitate a fost uzurpată**:

- (a) numele [...] [...];
- (b) prenumele [...] [...];
- (a) numele [...] [...] la naștere;
- (b) numele folosite anterior și orice nume de împrumut care să fie introduse separat, dacă este posibil;
- (c) orice caracteristică fizică, obiectivă [...] specifică și inalterabilă;
- (d) locul nașterii;
- (e) data nașterii;
- (f) [...] **genul**;
- (g) fotografiile și imagini faciale;
- (h) [...] **date dactiloscopice**;
- (i) cetățenie/**cetățeni**[...];
- (j) categoria document**elor** de identificare **ale** persoanei;
- (k) țara care a eliberat document**ele** de identificare **ale** persoanei;
- (l) numărul (numerele) documentului de identificare al persoanei;
- (m) data eliberării document**elor** de identificare **ale** persoanei;
- (n) adresa **persoanei** [...];
- (o) numele tatălui [...] **persoanei**;
- (p) numele mamei [...] **persoanei**.

- (4) Normele tehnice necesare privind introducerea și prelucrarea ulterioară a datelor menționate la alineatul (3) se stabilesc prin intermediul unor măsuri de punere în aplicare prevăzute și dezvoltate în conformitate cu procedura de examinare menționată la articolul 72 alineatul (2).
- (5) Datele menționate la alineatul (3) se șterg în același timp cu semnalarea corespunzătoare sau mai devreme, dacă respectiva persoană solicită acest lucru.
- (6) Doar autoritățile care au drept de acces la semnalarea corespunzătoare pot accesa datele menționate la alineatul (3). Acestea pot accesa datele respective doar în scopul evitării unei identificări eronate.

Articolul 60

Legături între alerte

- (1) Un stat membru poate crea o legătură între semnalările pe care le introduce în SIS. Scopul unei astfel de legături este de a stabili o relație între două sau mai multe semnalări.
- (2) Crearea unei legături nu afectează acțiunea specifică ce trebuie întreprinsă pe baza fiecărei semnalări puse în legătură sau perioada de păstrare a fiecăreia dintre semnalările puse în legătură.
- (3) Crearea unei legături nu aduce atingere drepturilor de acces prevăzute în prezentul regulament. Autoritățile care nu au drept de acces la anumite categorii de semnalări nu pot vedea legătura cu o semnalare la care nu au acces.
- (4) Un stat membru creează o legătură între semnalări în cazul în care acest lucru este necesar din punct de vedere operațional.
- (5) În cazul în care un stat membru consideră că crearea de către un alt stat membru a unei legături între semnalări este incompatibilă cu dreptul său național sau cu obligațiile sale internaționale, acesta poate lua măsurile necesare pentru a se asigura că respectiva legătură nu poate fi accesată de pe teritoriul său național sau de către autoritățile sale situate în afara teritoriului său.
- (6) Normele tehnice privind crearea unei legături între semnalări se stabilesc și se dezvoltă în conformitate cu procedura de examinare menționată la articolul 72 alineatul (2).

Articolul 61

Scopul informațiilor suplimentare și perioada de păstrare a acestora

- (1) Statele membre păstrează în cadrul biroului SIRENE o trimitere la deciziile care au generat o semnalare pentru a sprijini schimbul de informații suplimentare.
- (2) Datele cu caracter personal din fișierele deținute de biroul SIRENE ca urmare a unui schimb de informații se păstrează numai pe perioada care este necesară în vederea realizării scopurilor în care au fost furnizate. În orice caz, acestea se șterg în termen de maximum un an după ce semnalarea conexă a fost ștearsă din SIS.
- (3) Alineatul (2) nu aduce atingere dreptului unui stat membru de a păstra în fișierele naționale date referitoare la o anumită semnalare pe care a emis-o respectivul stat membru sau la o semnalare în legătură cu care s-a întreprins o acțiune pe teritoriul său. Perioada pentru care aceste date se pot păstra în respectivele fișiere este reglementată de dreptul național.

Articolul 62

Transferul datelor cu caracter personal către terți

Datele prelucrate în SIS și informațiile suplimentare conexe prevăzute în prezentul regulament nu se transferă și nici nu se pun la dispoziția țărilor terțe sau a organizațiilor internaționale.

Articolul 63

[...]

[...]

CAPITOLUL XV PROTECȚIA DATELOR

Articolul 64

Legislația aplicabilă

- (1) Regulamentul (CE) nr. 45/2001 se aplică prelucrării datelor cu caracter personal de către agenție **și de către Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă în temeiul prezentului regulament. Regulamentul (UE) 2016/794 (Regulamentul privind Europolul) se aplică prelucrării datelor cu caracter personal de către Europol în temeiul prezentului regulament. Decizia 2002/187 (Eurojust) se aplică prelucrării datelor cu caracter personal de către Eurojust în temeiul prezentului regulament.**
- (2) Regulamentul (UE) 2016/679 se aplică prelucrării datelor cu caracter personal cu condiția ca [...] Directiva (UE) 2016/680 să nu se aplice.

- (3) **Se aplică dispozițiile naționale de transpunere a Directivei (UE) 2016/680** [...] pentru prelucrarea datelor de către autoritățile naționale competente în scopul prevenirii, depistării, investigării sau urmării penale a infracțiunilor sau al executării pedepselor, inclusiv în scopul asigurării prevenirii amenințărilor pentru siguranța publică [...].

Articolul 65

Dreptul de accesare, de rectificare a datelor inexacte și de ștergere a datelor stocate în mod ilegal

- (1) Dreptul persoanelor vizate de a avea acces la datele introduse în SIS care le privesc și de rectificare sau de ștergere a acestor date se exercită în conformitate cu dreptul statului membru în care invocă acest drept.
- (2) [...]
- (3) Un alt stat membru decât cel care a emis o semnalare poate comunica informații privind aceste date **unei persoane vizate** numai [...] **după ce fiecare** stat membru **emitent** [...] **își dă** [...] [...] **consimțământul** [...]. Acest lucru se realizează printr-un schimb de informații suplimentare.
- (4) Un stat membru ia decizia de a nu comunica, integral sau parțial, informații persoanei vizate, în conformitate cu dreptul național, în măsura în care și atât timp cât o astfel de restricționare parțială sau integrală constituie o măsură necesară și proporțională într-o societate democratică, ținând seama în mod corespunzător de drepturile fundamentale și de interesele legitime ale persoanei [...] vizate, pentru:

- (a) a evita obstrucționarea cercetărilor, a investigațiilor sau a procedurilor oficiale ori juridice;
 - (b) a evita afectarea prevenirii, a depistării, a investigării sau a urmăririi penale a infracțiunilor sau a executării pedepselor;
 - (c) a proteja siguranța publică;
 - (d) a proteja securitatea națională; **sau**
 - (e) a proteja drepturile și libertățile celorlalți.
- (5) [...]
- (6) [...] **În urma unei cereri de acces, de rectificare sau de ștergere, persoana vizată** este informată cât de curând posibil [...] după data [...] **cererii despre rezultatul exercitării acestor drepturi**¹¹¹.
- (7) [...]¹¹²

Articolul 66

Căi de atac

- (1) Orice persoană poate introduce o acțiune în fața instanțelor judecătorești sau a oricărei [...] autorități competente în temeiul dreptului **național** [...] pentru accesarea, rectificarea sau ștergerea informațiilor ori pentru obținerea de informații sau de despăgubiri în legătură cu o semnalare care o privește.

¹¹¹ Alineat fuzionat cu alineatul (7).

¹¹² Fuzionat cu alineatul (6).

- (2) Statele membre se angajează reciproc să execute deciziile definitive pronunțate de instanțele judecătorești sau de autoritățile menționate la alineatul (1) al prezentului articol, fără a aduce atingere dispozițiilor articolului 70.
- (3) [...] Autoritățile naționale [...] **(...) raportează** anual cu privire la:
- (a) numărul de cereri de acces ale persoanelor vizate înaintate operatorului și numărul de cazuri în care s-a acordat acces la date;
 - (b) numărul de cereri de acces ale persoanelor vizate înaintate autorității naționale de supraveghere și numărul de cazuri în care s-a acordat acces la date;
 - (c) numărul de cereri de rectificare a datelor inexacte și de ștergere a datelor stocate în mod ilegal înaintate operatorului și numărul de cazuri în care datele au fost rectificate sau șterse;
 - (d) numărul de cereri de rectificare a datelor inexacte și de ștergere a datelor stocate în mod ilegal înaintate autorității naționale de supraveghere;
 - (e) numărul de cazuri **în care s-a pronunțat o hotărâre judecătorească definitivă**¹¹³ [...] [...] ¹¹⁴[...]. **și**
 - (g) orice observație privind cazurile de recunoaștere reciprocă a hotărârilor definitive pronunțate de instanțele judecătorești sau de autoritățile altor state membre privind semnalările create de statul membru care a emis semnalarea.

Rapoartele elaborate de autoritățile naționale de supraveghere se transmit mecanismului de cooperare stabilit la articolul 69.

¹¹³ Text provenind de la litera (f).

¹¹⁴ Fuzionat cu litera (e).

Articolul 67
Supravegherea N.SIS

- (1) Fiecare stat membru se asigură că autoritatea [...] națională de supraveghere desemnată în fiecare stat membru și investită cu competențele menționate în capitolul VI din Directiva (UE) 2016/680 sau în capitolul VI din Regulamentul (UE) 2016/679 monitorizează în mod independent legalitatea prelucrării datelor cu caracter personal din SIS pe teritoriul său și transmiterea acestor date de pe teritoriul său, precum și schimbul de informații suplimentare și prelucrarea lor ulterioară **pe teritoriul său**.
- (2) Autoritatea națională de supraveghere se asigură că, cel puțin din patru în patru ani, se efectuează un audit al operațiunilor de prelucrare a datelor în sistemul său N.SIS, efectuat în conformitate cu standardele internaționale de audit. Auditul fie se efectuează de autoritatea [...] națională de supraveghere, fie autoritatea națională de supraveghere dispune în mod direct efectuarea auditului de un auditor independent în materie de protecție a datelor. Autoritatea națională de supraveghere păstrează în permanență controlul asupra auditorului independent și își asumă responsabilitățile acestuia.
- (3) Statele membre se asigură că autoritatea lor națională de supraveghere are resurse suficiente pentru a îndeplini sarcinile care i-au fost încredințate în temeiul prezentului regulament.

Articolul 68
Supravegherea agenției

- (1) Autoritatea Europeană pentru Protecția Datelor se asigură că activitățile de prelucrare a datelor cu caracter personal desfășurate de agenție se efectuează în conformitate cu prezentul regulament. Atribuțiile și competențele menționate la articolele 46 și 47 din Regulamentul (CE) nr. 45/2001 se aplică în consecință.

- (2) Autoritatea Europeană pentru Protecția Datelor [...] **efectuează**, cel puțin din patru în patru ani, un audit al activităților de prelucrare a datelor cu caracter personal desfășurate de agenție, în conformitate cu standardele internaționale de audit. Raportul de audit se trimite Parlamentului European, Consiliului, agenției, Comisiei și autorităților naționale de supraveghere. Agenției i se oferă posibilitatea de a face observații înainte de adoptarea raportului.

Articolul 69

Cooperarea dintre autoritățile naționale de supraveghere și Autoritatea Europeană pentru Protecția Datelor

- (1) Autoritățile naționale de supraveghere și Autoritatea Europeană pentru Protecția Datelor, acționând fiecare în limitele competențelor deținute, cooperează în mod activ în cadrul responsabilităților care le revin și asigură supravegherea coordonată a SIS.
- (2) Aceste autorități, acționând fiecare în limitele competențelor deținute, fac schimb de informații relevante, se asistă reciproc în efectuarea auditurilor și a inspecțiilor, examinează dificultățile legate de interpretarea sau aplicarea prezentului regulament și a altor acte juridice aplicabile ale Uniunii, analizează problemele identificate prin exercitarea supravegherii independente sau prin exercitarea drepturilor persoanelor vizate, elaborează propuneri armonizate în vederea găsirii unor soluții comune la eventualele probleme și promovează sensibilizarea cu privire la drepturile în materie de protecție a datelor, dacă este necesar.
- (3) În scopurile enunțate la alineatul (2), autoritățile naționale de supraveghere și Autoritatea Europeană pentru Protecția Datelor se reunesc de cel puțin două ori pe an în cadrul Comitetului european pentru protecția datelor, instituit prin Regulamentul (UE) 2016/679. [...] Regulamentul de procedură se adoptă în cadrul primei reuniuni. Dacă este necesar, se elaborează de comun acord alte metode de lucru.
- (4) Comitetul instituit prin Regulamentul (UE) 2016/679 transmite [...] **anual** Parlamentului European, Consiliului și Comisiei un raport comun privind activitățile de supraveghere coordonată.

CAPITOLUL XVI
RĂSPUNDEREA SIS SANCTIUNILE¹¹⁵

Articolul 70

Răspunderea

- (1) Fiecare stat membru răspunde, **în conformitate cu dreptul național**, de orice prejudiciu cauzat unei persoane ca urmare a utilizării sistemului N.SIS. Acest lucru se aplică și daunelor cauzate de statul membru emitent, în cazul în care acesta din urmă a introdus date care conțin erori de fapt sau a stocat date în mod ilegal.
- (2) În cazul în care statul membru împotriva căruia se introduce o acțiune nu este statul membru care a emis semnalarea, acesta din urmă este obligat să ramburseze, la cerere, sumele plătite drept despăgubire, cu excepția cazului în care utilizarea datelor de către statul membru care solicită rambursarea încalcă prezentul regulament.
- (3) În cazul în care orice nerespectare de către un stat membru a obligațiilor care îi revin în temeiul prezentului regulament provoacă daune SIS, respectivul stat membru este răspunzător de aceste daune, cu excepția cazului și în măsura în care agenția sau [...] alt stat membru care participă la SIS nu a luat măsuri rezonabile pentru a preveni producerea daunelor sau pentru a le reduce impactul.

Articolul 70A

Sanctiunile¹¹⁶

Statele membre se asigură că orice utilizare abuzivă a datelor introduse în SIS sau orice schimb de informații suplimentare care contravin prezentului regulament fac obiectul unor sancțiuni eficiente, proporționale și disuasive în conformitate cu dreptul național.

¹¹⁵ S-a adăugat „și sancțiunile” ca urmare a includerii articolului nou 53A / 70A.

¹¹⁶ Articol nou, similar articolului 65 din Decizia 2007/533/JAI.

CAPITOLUL XVII DISPOZIȚII FINALE

Articolul 71

Monitorizarea și statisticile

- (1) Agenția se asigură că există proceduri pentru a monitoriza funcționarea SIS din perspectiva obiectivelor legate de rezultate, eficacitatea costurilor, securitate și calitatea serviciului.
- (2) În scopul întreținerii tehnice, al raportării, **al elaborării de rapoarte privind calitatea** și al întocmirii de statistici, agenția are acces la informațiile necesare referitoare la operațiunile de prelucrare efectuate în SIS central.
- (3) Agenția întocmește zilnic, lunar și anual statistici care prezintă numărul de înregistrări pentru fiecare categorie de semnalări, **în total și pentru fiecare stat membru. De asemenea, agenția furnizează rapoarte privind** [...] numărul de rezultate pozitive pentru fiecare categorie de semnalări, numărul de căutări efectuate în SIS și numărul de accesări ale SIS în scopul introducerii, al actualizării sau al ștergerii unei semnalări, în total și pentru fiecare stat membru. Statisticile întocmite nu conțin date cu caracter personal. Raportul statistic anual se publică. Agenția furnizează de asemenea statistici anuale privind utilizarea funcționalității de suspendare temporară, în cazul efectuării de căutări, a disponibilității unei semnalări emise în temeiul articolului 26 din prezentul regulament, în total și pentru fiecare stat membru, inclusiv orice prelungire a perioadei **inițiale** de 48 de ore de indisponibilitate **în cazul efectuării de căutări**.
- (4) Statele membre, precum și Europolul, Eurojustul și Agenția Europeană pentru Poliția de Frontieră și Garda de Coastă furnizează agenției și Comisiei informațiile necesare pentru elaborarea rapoartelor menționate la alineatele (3), **(5)**, (7) și (8)¹¹⁷.

¹¹⁷ Text mutat la alineatul (4a).

(4a)¹¹⁸ Aceste informații includ statistici separate privind numărul de căutări efectuate de serviciile din statele membre responsabile cu eliberarea certificatelor de înmatriculare a vehiculelor și de serviciile din statele membre responsabile cu eliberarea certificatelor de înmatriculare sau cu asigurarea gestionării traficului pentru ambarcațiuni, inclusiv motoare de ambarcațiuni [...] **și** aeronave, **inclusiv motoare aeronautice** [...], sau în numele respectivelor servicii. Statisticile arată, de asemenea, numărul de rezultate pozitive pentru fiecare categorie de semnalări.

(5) Agenția furnizează statelor membre, Comisiei, Eurojustului și Agenției Europene pentru Poliția de Frontieră și Garda de Coastă toate rapoartele statistice pe care le elaborează. Pentru a monitoriza punerea în aplicare a actelor juridice ale Uniunii, **în special a Regulamentului (UE) nr. 1053/2013 al Consiliului**¹¹⁹, Comisia este în măsură să solicite agenției să furnizeze rapoarte statistice specifice suplimentare, periodice sau ad-hoc, privind performanța sau utilizarea SIS **central** și [...] **privind schimbul de informații suplimentare**.

(6) În scopul prezentului articol alineatele (3), (4) [...] **sau** (5) și al articolului 15 alineatul (5), agenția creează, pune în aplicare și găzduiește în sediile sale tehnice un registru central care conține [...] **rapoartele** menționate la prezentul articol alineatul (3) și la articolul 15 alineatul (5) care nu fac posibilă identificarea persoanelor și care permite Comisiei și agențiilor menționate la alineatul (5) să obțină rapoarte și statistici speciale. Agenția acordă statelor membre, Comisiei, Eurojustului și Agenției Europene pentru Poliția de Frontieră și Garda de Coastă un acces securizat la registrul central prin intermediul infrastructurii de comunicații cu un control al accesului și profiluri de utilizator specifice, exclusiv în scopul întocmirii de rapoarte și statistici¹²⁰.

[...](7) [...] **Din doi în** doi ani [...], agenția prezintă Parlamentului European și Consiliului un raport privind funcționarea tehnică a SIS central și privind funcționarea infrastructurii de comunicații, inclusiv securitatea acestora, și schimbul bilateral și multilateral de informații suplimentare dintre statele membre.

¹¹⁸ Mutat de la alineatul (4).

¹¹⁹ Regulamentul (UE) nr. 1053/2013 al Consiliului din 7 octombrie 2013 de instituire a unui mecanism de evaluare și monitorizare în vederea verificării aplicării acquis-ului Schengen și de abrogare a Deciziei Comitetului executiv din 16 septembrie 1998 de instituire a Comitetului permanent pentru evaluarea și punerea în aplicare a Acordului Schengen (JO L 295, 6.11.2013, p. 27).

¹²⁰ Text mutat la alineatul (9).

(8) [...] **Din patru în patru** ani [...], Comisia efectuează o evaluare globală a SIS central și a schimbului bilateral și multilateral de informații suplimentare dintre statele membre. Această evaluare globală include o examinare a rezultatelor obținute în raport cu obiectivele și o analiză a menținerii valabilității raționamentului care stă la baza sistemului, a aplicării prezentului regulament în ceea ce privește SIS central, a securității SIS central și a oricăror implicații asupra viitoarelor operațiuni. Comisia transmite evaluarea Parlamentului European și Consiliului.

(9)¹²¹Comisia adoptă acte de punere în aplicare pentru stabilirea și dezvoltarea unor norme detaliate privind funcționarea registrului central **menționat la alineatul (6)** și unor norme de securitate aplicabile **respectivului registru. Actele** de punere în aplicare **respective se** adoptă în conformitate cu procedura de examinare menționată la articolul 72 alineatul (2).

Articolul 72

Procedura comitetului

- (1) Comisia este asistată de un comitet în sensul Regulamentului (UE) nr. 182/2011.
- (2) Atunci când se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.

¹²¹ Text mutat de la sfârșitul alineatului (6).

Articolul 73

[...]

[...] ¹²² [...] * [...] **

[...] *

[...] **

[...] ¹²³

Articolul 74

Abrogarea

La data aplicării prezentului regulament se abrogă următoarele acte juridice:

Regulamentul (CE) nr. 1986/2006 al Parlamentului European și al Consiliului din 20 decembrie 2006 privind accesul la Sistemul de Informații Schengen din a doua generație (SIS II) al serviciilor competente, în statele membre, pentru eliberarea certificatelor de înmatriculare a vehiculelor;

¹²² [...]

¹²³ Articol eliminat, întrucât prezentul instrument nu modifică Regulamentul (UE) nr. 515/2014.

Decizia [...] 2007/**533**/JAI a Consiliului din 12 iunie 2007 privind înființarea, funcționarea și utilizarea Sistemului de informații Schengen de a doua generație (SIS II);

Decizia 2010/261/UE a Comisiei din 4 mai 2010 privind planul de securitate pentru SIS II central și infrastructura de comunicații¹²⁴.

Articolul 75

Intrarea în vigoare și aplicarea

- (1) Prezentul regulament intră în vigoare în a douăzecea zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.
- (2) Prezentul regulament se aplică de la data stabilită de către Comisie după ce:
 - (a) s-au adoptat măsurile necesare de punere în aplicare;
 - (b) statele membre au notificat Comisiei [...] că au luat măsurile tehnice și juridice necesare pentru prelucrarea datelor din SIS și efectuarea schimbului de informații suplimentare în temeiul prezentului regulament;
 - (c) agenția a notificat Comisiei finalizarea **cu succes a** tuturor activităților de testare în ceea ce privește CS-SIS și interacțiunea dintre C.SIS și N-SIS.

[...] Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în statele membre în conformitate cu tratatele.

¹²⁴ Decizia 2010/261/UE a Comisiei din 4 mai 2010 privind planul de securitate pentru SIS II central și infrastructura de comunicații (JO L 112, 5.5.2010, p. 31).