



GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. ____

din _____ 2022

Chișinău

Cu privire la aprobarea Conceptului Sistemului informațional „Gestiunea dosarelor de expertiză judiciară”

În temeiul art. 2 alin. (1), al art. 16 alin. (1) din Legea nr. 71/2007 cu privire la registre (Monitorul Oficial al Republicii Moldova, 2007, nr. 70-73, art. 314), cu modificările ulterioare, și al art. 22 lit. c) din Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr. 6-12, art. 44), cu modificările ulterioare, Guvernul HOTĂRĂȘTE:

1. Se aprobă Conceptul Sistemului informațional „Gestiunea dosarelor de expertiză judiciară”, conform anexei.
2. Se instituie Registrul de stat al dosarelor de expertiză judiciară, format de Sistemul informațional „Gestiunea dosarelor de expertiză judiciară”
3. Instituirea, dezvoltarea, întreținerea și asigurarea funcționării Sistemului informațional „Gestiunea dosarelor de expertiză judiciară” se realizează din contul și în limitele mijloacelor financiare aprobate anual în bugetul Ministerului Justiției, precum și din alte surse prevăzute de legislație.
4. În termen de 3 luni de la data intrării în vigoare a prezentei hotărâri, Ministerul Justiției va elabora și va prezenta Guvernului spre aprobare proiectul hotărârii Guvernului pentru aprobarea Regulamentului privind modul de ținere a Registrului de stat al dosarelor de expertiză judiciară.

5. Controlul asupra executării prezentei hotărâri se pune în sarcina Ministerului Justiției.

Prim-ministru

NATALIA GAVRILIȚA

Contrasemnează:

Ministrul justiției

Sergiu Litvinenco

Ministrul sănătății

Ala Nemerenco

Ministrul afacerilor interne

Ana Revenco

Ministrul finanțelor

Dumitru Budianschi

CONCEPTUL

Sistemului informațional „Gestiunea dosarelor de expertiză judiciară”

INTRODUCERE

Instituțiile de expertiză judiciară reprezintă o parte integrantă a sistemului de justiție din Republica Moldova, întrucât reprezintă forma organizatorică a activității experților judiciari, care, la rândul lor, contribuie la ameliorarea eficienței judiciare, oferind judecătorilor răspunsuri clare și argumentate asupra problemelor specifice și complexe cu care se confruntă aceștia la înfăptuirea justiției. Calitatea și acuratețea investigațiilor și expertizelor judiciare sau extrajudiciare au un impact imens asupra calității justiției și a percepției generale a societății cu privire la sistemul de justiție. În pofida importanței și locului acestora în sectorul justiției, instituțiile de expertiză judiciară au beneficiat de asistență și de sprijin limitat în eforturile lor de modernizare în comparație cu alte sisteme din cadrul sectorului justiției, așa cum a fost cazul sistemului judecătoresc – în cadrul căruia a fost implementat Programul integrat de gestionare a dosarelor (PIGD) sau al Procuraturii – pentru care a fost dezvoltat și ulterior implementat Sistemul informațional „Urmărire penală: E-Dosar”.

Deși în ultimii ani s-au întreprins eforturi importante la nivel național pentru a promova eficiența, transparența, corectitudinea și accesibilitatea sectorului justiției, totuși pentru o administrare mai eficientă a sectorului justiției este necesară continuarea implementării unor soluții care să asigure o coordonare coerentă între instituțiile din sectorul justiției, astfel încât atât bărbații, cât și femeile, în special și cei din grupuri minoritare, să-și poată revendica drepturile și accesa justiția în mod egal și eficient.

Astfel, în baza celor menționate *supra*, s-a decis implementarea Sistemului informațional „Gestiunea dosarelor de expertiză judiciară” (în continuare – *SIGDEJ*).

I. DISPOZIȚII GENERALE

1. Conceptul Sistemului informațional „Gestiunea dosarelor de expertiză judiciară” (în continuare – *Concept*) stabilește scopul, obiectivele, funcțiile, structura organizațională și cadrul juridico-normativ, necesare pentru crearea și exploatarea *SIGDEJ*, de asemenea, obiectele informaționale și lista datelor care se păstrează în acesta, infrastructura tehnologică și măsurile de asigurare a securității și protecției informației, precum și măsurile privind crearea, implementarea, exploatarea și menținerea *SIGDEJ*.

2. SIGDEJ reprezintă o soluție informatică din categoria Guvern pentru Guvern (G2G) și constituie totalitatea de resurse și tehnologii informaționale interdependente, inclusiv mijloace software, hardware și infrastructura utilizatorului, destinată păstrării, prelucrării și furnizării informației și formării resursei informaționale cu privire la dosarele de expertiză judiciară.

3. SIGDEJ formează resursa informațională Registrul dosarelor de expertiză judiciară (în continuare – *RDEJ*).

4. Noțiunile principale utilizate în prezentul Concept semnifică următoarele:

1) *expertiză* – expertiză judiciară, expertiză extrajudiciară, constatare tehnico-științifică, constatare medico-legală, astfel cum sunt acestea definite în legislație;

2) *raport de expertiză* – raport de expertiză judiciară, raport de expertiză extrajudiciară, raport de constatare tehnico-științifică, raport de constatare medico-legală;

3) *instituție de expertiză judiciară* – orice instituție publică de expertiză judiciară și birou de expertiză judiciară, așa cum sunt ele definite în Legea nr. 68/2016 cu privire la expertiza judiciară și statutul expertului judiciar;

4) *solicitant* – ordonator al expertizei judiciare (organul de urmărire penală, instanța de judecată sau un alt participant al unui proces derulat conform legislației de procedură civilă, penală sau contravențională, care are dreptul de a dispune sau de a solicita în mod independent efectuarea unei expertize judiciare; persoană fizică sau juridică care solicită efectuarea unei expertize extrajudiciare);

5) *cabinet virtual* – spațiu virtual în cadrul SIGDEJ care înglobează toate funcționalitățile și documentele relevante solicitantului;

6) *solicitare de expertiză* – act de dispunere a expertizei judiciare (ordonanță a organului de urmărire penală sau încheiere a instanței de judecată prin care se dispune efectuarea expertizei judiciare sau, după caz, cererea de efectuare a expertizei judiciare depusă de către părți din proprie inițiativă și pe cont propriu în condițiile codurilor de procedură civilă, penală și contravențional; cererea scrisă a persoanei fizice sau juridice privind efectuarea expertizei extrajudiciare).

5. SIGDEJ înglobează posibilități funcționale de gestionare a fluxurilor de lucru, schimb de informații, funcții de înștiințare, depozitare a datelor și solicitare de expertize online, necesare pentru procesarea dosarelor de expertiză judiciară.

6. RDEJ este un registru de stat departamental care se ține în scopul înregistrării rapoartelor de expertiză întocmite de către sau cu participarea experților judiciari care activează în cadrul instituțiilor de expertiză judiciară

înregistrate în Republica Moldova, precum și al formării dosarelor de expertiză judiciară în conformitate cu prevederile art. 39 alin. (2) din Legea nr. 68/2016 cu privire la expertiza judiciară și statutul expertului judiciar. Acesta reprezintă o resursă informațională de stat oficială și este parte integrantă a resurselor informaționale de stat ale Republicii Moldova.

7. SIGDEJ pune la dispoziția solicitanților următoarele servicii:

- 1) obținerea rapoartelor de expertiză;
- 2) acces la informațiile privind procesul de efectuare a expertizei;
- 3) depunerea online a solicitărilor de expertize;
- 4) evidența strictă a obiectelor de expertizat;
- 5) achitarea online pentru serviciile de expertiză;
- 6) semnarea electronică a documentelor.

8. Obiectivele SIGDEJ sunt:

1) crearea resursei informaționale a activității de expertiză judiciară desfășurată de către instituțiile de expertiză judiciară înregistrate în Republica Moldova, în vederea creării și păstrării dosarelor de expertiză judiciară prin stocarea, sistematizarea și actualizarea informațiilor ce sunt procesate de către acestea (de exemplu, solicitări de expertize, dosare de expertiză și documente aferente acestora, rapoarte de expertiză etc.) și a asigurării unui nivel adecvat de protecție a datelor vehiculate în SIGDEJ;

2) eficientizarea lucrului personalului din cadrul instituțiilor de expertiză judiciară prin înlocuirea metodei de culegere și înscriere a informațiilor pe suport de hârtie, cu stocarea și procesarea datelor relevante în regim electronic, în contextul realizării activității de expertiză judiciară;

3) asigurarea lanțului de trasabilitate și custodie a obiectelor de expertizat;

4) asigurarea calității și veridicității informației vehiculate în cadrul proceselor de efectuare a expertizelor;

5) identificarea unică și asigurarea gestiunii și trasabilității documentelor, înregistrărilor, dosarelor și rapoartelor de expertiză, parte a proceselor de efectuare a expertizelor, precum și a altor documente stabilite ulterior în coordonare cu instituțiile de expertiză judiciară din Republica Moldova;

6) eliminarea poverii de completare în regim manual a diferitelor registre și rapoarte pe suport de hârtie. Acestea ar urma să fie generate din SIGDEJ în baza datelor primare introduse în sistem;

7) centralizarea tuturor datelor și informațiilor referitoare la dosarele de expertiză judiciară într-o bază de date unică și oferirea accesului la informații atât agregate, cât și în detaliu, de diferite forme de prezentare;

8) asigurarea protecției datelor și a altor aspecte de securitate informațională referitoare la expertiza judiciară;

9) reducerea timpului pentru colectarea datelor necesare și pentru elaborarea și consolidarea rapoartelor integrate prin utilizarea unui instrument

tehnologic modern de raportare. Acesta urmează să asigure generarea rapoartelor statistice și analitice predefinite și de tip *custom* în regim ad-hoc;

10) minimizarea interacțiunii fizice dintre solicitanții de expertize și instituțiile de expertiză judiciară;

11) crearea unui mecanism pentru ca solicitanții de expertize să poată urmări evoluția solicitărilor lor;

12) contribuirea la diminuarea volumului de documente procesate pe suport de hârtie în cadrul instituțiilor de expertiză judiciară.

9. Principiile de bază ale SIGDEJ sunt următoarele:

1) principiul legalității, potrivit căruia funcțiile și operațiile efectuate de utilizatori sunt legale și conforme cu drepturile omului și legislația națională în vigoare;

2) principiul autenticității datelor, care presupune că informațiile păstrate pe dispozitive de stocare a datelor sau pe suport de hârtie corespund stării reale a obiectelor din SIGDEJ;

3) principiul identificării, conform căruia entităților informaționale li se atribuie un cod de identificare unic la nivel de sistem, prin care este posibilă identificarea univocă și raportarea la acestea;

4) principiul temeiniciei datelor, care prevede că introducerea datelor în SIGDEJ se efectuează doar în baza înscririlor din documentele acceptate ca surse de informații;

5) principiul auditului sistemului, care presupune înregistrarea informației despre schimbările care au loc în sistem, pentru a face posibilă reconstituirea istoriei unui document sau starea lui la o etapă anterioară;

6) principiul independenței de platforma software, conform căruia SIGDEJ poate fi construit pe baza modulelor elaborate la comandă sau a produselor software existente. Prezentul Concept nu limitează în niciun fel abordarea dezvoltării sistemului atât timp cât sunt satisfăcute nevoile identificate și se oferă cea mai mare valoare pentru prețul oferit;

7) principiul accesibilității și integrabilității, care presupune că SIGDEJ, chiar dacă oferă funcționalități multiple, este construit ca un element integral și folosit de utilizatori prin intermediul unei interfețe unice. Mai mult decât atât, acest principiu prevede că expansiunea și dezvoltarea sistemului se vor face prin protocoale și puncte de conexiune proiectate din start;

8) principiul confidențialității informației, care prevede răspunderea personală, în conformitate cu legislația în vigoare, a colaboratorilor responsabili de prelucrarea informației în sistem pentru utilizarea și difuzarea neautorizată a informației din sistem;

9) principiul compatibilității, conform căruia SIGDEJ trebuie să fie compatibil cu sistemele existente atât în țară, cât și peste hotarele ei;

10) principiul orientării spre utilizator, potrivit căruia structura, conținutul, mijloacele de acces și navigarea sunt focalizate spre utilizatori;

11) principiul extensibilității, conform căruia componentele SIGDEJ oferă facilități de ajustare și extindere a funcționalităților existente pentru conformare cu necesitățile în continuă schimbare ale domeniului;

12) principiul dezvoltării progresive, potrivit căruia elaborarea sistemului și modificarea permanentă a componentelor sale se efectuează în conformitate cu tehnologiile informaționale avansate;

13) principiul consecutivității, care presupune elaborarea și implementarea sistemului pe etape;

14) principiul eficienței funcționării, care presupune optimizarea raportului dintre calitate și cost;

15) principiul utilizării standardelor deschise, care se aplică pentru a asigura atât interoperabilitatea cu sistemele externe, cât și păstrarea informației, în conformitate cu normele în vigoare;

16) principiul securității informaționale, care presupune asigurarea nivelului dorit de integritate, exclusivitate, accesibilitate și eficiență a protecției datelor împotriva pierderii, denaturării, distrugerii și utilizării neautorizate. Securitatea sistemului presupune rezistența la atacuri și protecția caracterului secret, a integrității și pregătirii pentru lucru atât a SIGDEJ, cât și a datelor acestuia;

17) principiul protecției datelor cu caracter personal, care presupune că acestea vor fi prelucrate în SIGDEJ în conformitate cu actele normative naționale și tratatele internaționale la care Republica Moldova este parte în domeniul protecției datelor cu caracter personal.

II. CADRUL NORMATIV AL FUNCȚIONĂRII SIGDEJ

10. Cadrul normativ al SIGDEJ include legislația națională, tratatele și convențiile internaționale la care Republica Moldova este parte. La crearea și implementarea SIGDEJ se iau în considerare, în special, cadrul normativ cu privire la expertiza judiciară și statutul expertului judiciar, precum și cu privire la tehnologia informației și comunicațiilor, și anume:

- 1) Legea nr. 982/2000 privind accesul la informație;
- 2) Legea nr. 1069/2000 cu privire la informatică;
- 3) Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat;
- 4) Legea nr. 71/2007 cu privire la registre;
- 5) Legea nr. 133/2011 privind protecția datelor cu caracter personal;
- 6) Legea nr. 91/2014 privind semnătura electronică și documentul electronic;
- 7) Legea nr. 68/2016 cu privire la expertiza judiciară și statutul expertului judiciar;
- 8) Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate;

9) Hotărârea Guvernului nr. 562/2006 cu privire la crearea sistemelor și resurselor informaționale automatizate de stat;

10) Hotărârea Guvernului nr. 1123/2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal;

11) Hotărârea Guvernului nr. 546/2011 privind aprobarea Regulamentului cu privire la acordarea serviciilor Sistemului de telecomunicații al autorităților administrației publice și operarea modificărilor în unele hotărâri ale Guvernului”;

12) Hotărârea Guvernului nr. 710/2011 cu privire la aprobarea Programului strategic de modernizare tehnologică a guvernării (e-Transformare);

13) Hotărârea Guvernului nr. 329/2012 cu privire la Serviciul Guvernamental de Plăți Electronice (MPay);

14) Hotărârea Guvernului nr. 280/2013 cu privire la unele acțiuni de implementare a Serviciului Guvernamental de Plăți Electronice (MPay);

15) Hotărârea Guvernului nr. 857/2013 cu privire la Strategia națională de dezvoltare a societății informaționale „Moldova Digitală 2020”;

16) Hotărârea Guvernului nr. 1090/2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass);

17) Hotărârea Guvernului nr. 128/2014 privind platforma tehnologică guvernamentală comună (MCloud);

18) Hotărârea Guvernului nr. 404/2014 cu privire la pilotarea platformei de interoperabilitate;

19) Hotărârea Guvernului nr. 405/2014 privind serviciul electronic guvernamental integrat de semnătură electronică (MSign);

20) Hotărârea Guvernului nr. 700/2014 pentru aprobarea Concepției privind principiile datelor guvernamentale deschise;

21) Hotărârea Guvernului nr. 708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog);

22) Hotărârea Guvernului nr. 201/2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică;

23) Hotărârea Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat;

24) Hotărârea Guvernului nr. 211/2019 privind platforma de interoperabilitate (MConnect);

25) Hotărârea Guvernului nr. 376/2020 pentru aprobarea Conceptului serviciului guvernamental de notificare electronică (MNotify) și a Regulamentului privind modul de funcționare și utilizare a serviciului guvernamental de notificare electronică (MNotify).

III. SPAȚIUL FUNCȚIONAL AL SIGDEJ

11. Funcțiile de bază ale SIGDEJ sunt:

1) formarea resursei informaționale – funcțiile de bază la formarea resursei informaționale a SIGDEJ sunt trecerea în evidență inițială, actualizarea datelor și radierea din evidență a obiectelor informaționale (schimbarea statutului obiectului). Acestea se realizează în funcție de îndeplinirea anumitor scenarii de bază, după cum urmează:

a) luarea în evidență inițială – evidența inițială a obiectelor informaționale se realizează după adoptarea de către registrator a deciziei cu privire la includerea obiectului în RDEJ. În acest caz, fiecărui obiect informațional, cu excepția obiectelor informaționale împrumutate, i se atribuie un identificator unic care rămâne neschimbat pe toată perioada existenței obiectului în RDEJ, iar în baza de date a SIGDEJ se introduc date despre obiectul de evidență în cantitatea stabilită;

b) actualizarea datelor – actualizarea datelor SIGDEJ constă în actualizarea sistematică a băncii de date a acestuia în cazul modificării sau completării atributelor obiectelor de evidență. Toate modificările se păstrează în ordine cronologică;

c) radierea din evidență – radierea din evidență a obiectului informațional constă în modificarea, în baza deciziei registratorului, a statutului obiectului, inclusiv în transferul datelor despre obiectul evidenței în arhivă la sfârșitul ciclului său de viață, precum și la survenirea anumitor evenimente, prin inserarea unei note speciale, fapt care nu reprezintă excluderea fizică a datelor despre obiect din RDEJ. Informația se introduce în SIGDEJ numai în baza deciziei registratorului în prezența documentelor justificative sau a informației primite din alte sisteme informaționale, care confirmă veridicitatea informațiilor referitoare la documentul sau la resursa informațională în baza căreia a fost actualizată informația;

2) organizarea asigurării informaționale – informația din banca de date a RDEJ este pusă la dispoziția conducerii și a subdiviziunilor cointerestate ale instituțiilor de expertiză judiciară, precum și în cadrul schimbului informațional între participanții la SIGDEJ. Cu toate acestea, fiecare participant este obligat să utilizeze informația numai în scopuri legale. Nivelul de acces al utilizatorului la informația solicitată din SIGDEJ este stabilit de legislație, în funcție de statutul său juridic și de regimul juridic al informației. Procedura și tipul informației furnizate utilizatorilor se stabilesc în Regulamentul cu privire la modul de ținere a RDEJ și în alte acte normative elaborate de comun acord de deținătorul și de posesorul SIGDEJ;

3) asigurarea securității și protecției informației – se realizează în conformitate cu cerințele standardului SM ISO CEI 27001 la toate etapele de colectare, depozitare și utilizare a resurselor informaționale ce se referă la procesul de efectuare a expertizei;

4) asigurarea calității informației – se efectuează prin crearea și menținerea componentelor sistemului de calitate, bazate pe principiul abordării de proces în conformitate cu cerințele standardului SM SR EN ISO 9001;

5) asigurarea multilaterală a funcționării SIGDEJ – presupune interacțiunea și integrarea cu alte sisteme informaționale de stat sau servicii electronice guvernamentale.

12. În cadrul funcționării SIGDEJ se realizează funcții specifice, grupate în contururi funcționale speciale.

13. Conturul funcțional de interacțiune informațională a tuturor participanților sistemului „ADMINISTRARE ȘI MONITORIZARE” reprezintă un subsistem integrat de control și monitorizare a formării și utilizării resursei informaționale de gestiune a dosarelor de expertiză judiciară. Conturul include următoarele funcții:

- 1) asigurarea integrității logice a SIGDEJ;
- 2) administrarea bazelor de date ale SIGDEJ;
- 3) elaborarea și mentenanța ghidurilor de sistem și a clasificatoarelor;
- 4) delimitarea drepturilor de acces pentru utilizatori;
- 5) evidența rapoartelor de expertiză și a documentelor dosarelor;
- 6) asigurarea securității, protecției și integrității informației în sistem conform cerințelor standardului național SM EN ISO/IEC 27001:2017 „Tehnologia informației. Tehnici de securitate. Sisteme de management al securității informației. Cerințe”;
- 7) asigurarea respectării cerințelor SIGDEJ de protecție a datelor cu caracter personal.

14. Conturul funcțional „DOSAR DE EXPERTIZĂ” include funcții de evidență a:

- 1) solicitării de expertiză;
- 2) obiectelor de expertizat;
- 3) raportului de expertiză;
- 4) notificării de refuz privind efectuarea expertizei;
- 5) scrisorii de însoțire a raportului de expertiză;
- 6) oricărei comunicări cu solicitantul sub formă de documente de intrare/ieșire;
- 7) oricărui document care poate apărea pe parcursul desfășurării activității de expertiză.

15. Conturul funcțional „PARTICIPANȚI AI SISTEMULUI” include funcții de evidență a:

- 1) solicitanților de expertize;
- 2) instituțiilor de expertiză judiciară;
- 3) altor autorități/instituții implicate în activitatea de expertiză, după caz.

16. Conturul funcțional „DOCUMENTE” include funcții de evidență a documentelor care circulă în cadrul SIGDEJ, după cum urmează:

- 1) documente de intrare în SIGDEJ;
- 2) documente tehnologice a SIGDEJ (inclusiv tehnice).
- 3) documente de ieșire a SIGDEJ.

IV. STRUCTURA ORGANIZAȚIONALĂ A SIGDEJ

17. Funcțiile de bază privind formarea și exploatarea RDEJ sunt divizate între:

- 1) proprietarul SIGDEJ;
- 2) posesorul SIGDEJ;
- 3) deținătorul SIGDEJ;
- 4) administratorul tehnic al SIGDEJ;
- 5) utilizatorii SIGDEJ.

18. Proprietarul SIGDEJ este statul, care își realizează dreptul de proprietate, de gestionare și de utilizare a datelor din sistem. Resursele financiare pentru dezvoltarea și exploatarea SIGDEJ sunt asigurate din bugetul de stat și din alte surse financiare conform actelor normative.

19. Posesorul SIGDEJ este Ministerul Justiției. Deținătorul SIGDEJ este Agenția Resurse Informaționale Juridice.

20. Posesorul SIGDEJ asigură condițiile organizatorice și financiare pentru funcționarea acestuia. Deținătorul SIGDEJ asigură crearea, administrarea, mentenanța și dezvoltarea acestuia.

21. Administratorul tehnic al SIGDEJ este Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică, care asigură administrarea tehnică și mentenanța acestuia.

22. Utilizatori ai SIGDEJ sunt:

- 1) registratorii;
- 2) furnizorii de date;
- 3) destinatarii.

23. Registratorii SIGDEJ sunt următoarele persoane juridice sau fizice:

- 1) Centrul Național de Expertize Judiciare;
- 2) Centrul Tehnico-Criminalistic și Expertize Judiciare al Inspectoratului General al Poliției;
- 3) Centrul de Medicină Legală;

4) subdiviziunea responsabilă de realizarea expertizei judiciare din cadrul Inspectoratului General al Poliției de Frontieră;

5) subdiviziunea responsabilă de realizarea expertizei judiciare din cadrul Centrului Național Anticorupție;

6) experții judiciari din cadrul birourilor de expertiză judiciară.

24. Furnizori de date pentru SIGDEJ sunt solicitanții de expertiză și autoritățile/instituțiile publice care prezintă registratorului, pe suport de hârtie sau în format electronic, date despre obiectele informaționale ale acestuia.

25. Destinatarii SIGDEJ sunt persoanele fizice și juridice mandatate conform legislației să primească datele conținute în RDEJ.

V. DOCUMENTELE SIGDEJ

26. În cadrul SIGDEJ se folosesc următoarele categorii de documente:

1) documente de intrare, care sunt fundamentale pentru introducerea datelor în sistem;

2) documente de ieșire, obținute în urma funcționării sistemului;

3) documente tehnologice.

27. Documentele de intrare ale SIGDJ sunt următoarele:

1) solicitările de expertize;

2) anexele la solicitările de expertize;

3) documente scanate în format PDF, JPG necesare desfășurării activității de expertiză;

4) scrisorile solicitanților adresate instituțiilor de expertiză judiciară, ce conțin orice clarificări privind solicitarea depusă.

28. Documentele de ieșire ale SIGDJ sunt următoarele:

1) rapoartele de expertiză;

2) scrisorile (notificările) de acceptare sau de refuz privind efectuarea expertizei;

3) rapoartele expertizei de laborator;

4) rapoartele statistice privind expertizele efectuate/respinse;

5) scrisorile de clarificare adresate solicitantului privind solicitarea serviciilor de expertiză a acestuia.

29. Documentele tehnologice ale SIGDJ sunt următoarele:

1) confirmarea plăților pentru serviciile de expertiză;

2) documente ce conțin alte informații necesare efectuării expertizei, care pot apărea pe parcursul desfășurării acesteia.

3) lista cu istoricul (log-ul) activităților aferente lucrului cu dosarele de expertiză în sistem.

VI. SPAȚIUL INFORMAȚIONAL AL SIGDEJ

30. Resursa informațională a SIGDEJ este reprezentată de un ansamblu de obiecte informaționale și interacțiunea acestora. Obiectele informaționale sunt determinate în funcție de destinația SIGDEJ și includ:

1) persoană fizică – obiect informațional împrumutat din Registrul de stat al populației (în continuare – *RSP*);

2) unitate de drept – obiect informațional împrumutat din Registrul de stat al unităților de drept (în continuare – *RSUD*). În SIGDEJ aceste obiecte se clasifică în:

a) instituție de expertiză judiciară, care reprezintă subiectul responsabil de organizarea efectuării expertizei și emiterea raportului de expertiză;

b) persoane juridice care solicită expertize judiciare;

3) document, care se clasifică în:

a) solicitare de expertiză, în sensul oferit la pct. 7 subpct. 6);

b) notificare de acceptare – mesaj emis de către SIGDEJ în adresa solicitantului, în care se conțin informații referitoare la acceptarea solicitării de expertiză;

c) notificare de refuz – mesaj emis de către SIGDEJ, în care se conțin informații referitoare la refuzul efectuării expertizei indicate în solicitarea de expertiză, cu indicarea motivului refuzului;

d) notificare privind statutul dosarului de expertiză – mesaj emis de către SIGDEJ în adresa solicitantului, în care se conțin informații privind statutul dosarului de expertiză inițiat în baza solicitării de expertiză;

e) raport de expertiză – document emis prin intermediul SIGDEJ, care reflectă rezultatul expertizei efectuate. Acesta poate fi raport de expertiză judiciară, raport de expertiză extrajudiciară, raport de constatare tehnico-științifică, raport de constatare medico-legală;

f) raport de cercetare de laborator – document emis de către laborator, în care se conțin informații referitoare la cercetările de laborator efectuate, relevante expertizei;

g) raport statistic – document generat de SIGDEJ care reflectă sinteza datelor stocate în acesta, organizate conform unei anumite structuri;

h) document de ieșire – document emis prin intermediul SIGDEJ, adresat către solicitant, în care se conțin informații privind solicitarea de expertiză depusă, precum și chestiuni de clarificare privind obiectul de expertizat sau privind activitățile de expertiză;

i) document de intrare – document emis de către solicitant, înregistrat și stocat ulterior în SIGDEJ, în care se conțin orice clarificări sau informații

referitoare la solicitarea de expertiză și la obiectul de expertizat, oferită de către solicitant.

4) eveniment – obiect informațional intersistemic. Un eveniment în sistem reprezintă un anumit punct în cadrul derulării programului software în care are loc execuția unei sarcini identificabile.

Obiectele informaționale împrumutate „persoană fizică” și „unitate de drept” sunt inițial înregistrate și identificate în alte sisteme, respectiv, RSP și RSUD, pentru care nemijlocit în SIGDEJ se mențin numai numerele de identificare (IDNP sau IDNO) și în acest caz nu se admite modificarea identificatorului. Toate datele suplimentare necesare sunt accesibile din RSP sau RSUD, iar în caz de necesitate pot fi completate.

31. În SIGDEJ se utilizează următorii identificatori ai obiectelor informaționale:

1) „persoană fizică” – numărul de identificare de stat al persoanei fizice (IDNP);

2) „unitate de drept” – numărul de identificare de stat al unității de drept (IDNO) din RSUD;

3) „solicitare de expertiză” – codul unic de identificare, generat și atribuit de sistem, care are următoarea structură:

„REQUEST”+YYMMDDNNNN, solicitării de expertiză depuse, unde:

YY – ultimele cifre ale anului curent;

MM – luna, exprimată în cifre;

DD – data, exprimată în cifre;

NNNN – numărul de ordine al solicitării de expertiză, generat de sistem conform înregistrării pentru ziua respectivă;

4) „raport de expertiză” – numărul unic generat și atribuit de sistem, care are următoarea structură:

„EXPERTREP”+YYMMDDNNNN raportului emis, unde:

YY – ultimele cifre ale anului curent;

MM – luna, exprimată în cifre;

DD – data, exprimată în cifre;

NNNN – numărul de ordine al raportului de expertiză, conform înregistrării pentru ziua respectivă;

5) „notificare de acceptare” – numărul generat și atribuit de sistem, care are următoarea structură:

„NOTIF_ACCEPT”+YYMMDDNNNN notificării de acceptare, unde:

YY – ultimele cifre ale anului curent;

MM – luna, exprimată în cifre;

DD – data, exprimată în cifre;

NNNN – numărul de ordine al notificării de acceptare, conform înregistrării pentru ziua respectivă;

6) „notificare de refuz” – numărul de ordine al rutei înregistrate, generat și atribuit de sistem, care are următoarea structură:

„NOTIF_REFUZ”+YYMMDDNNNN notificării de refuz, unde:

YY – ultimele cifre ale anului curent;

MM – luna, exprimată în cifre;

DD – data, exprimată în cifre;

NNNN – numărul de ordine al notificării de refuz, conform înregistrării pentru ziua respectivă;

7) „notificarea privind statutul dosarului de expertiză” – codul unic de identificare, generat și atribuit de sistem, care are următoarea structură:

„NOTIF_STATUT”+YYMMDDNNNN notificării privind statutul solicitării de expertiză, unde:

YY – ultimele cifre ale anului curent;

MM – luna, exprimată în cifre;

DD – data, exprimată în cifre;

NNNN – numărul de ordine al notificării privind statutul solicitării de expertiză, conform înregistrării pentru ziua respectivă;

8) „raport de cercetare de laborator” – codul unic de identificare, generat și atribuit de sistem, care are următoarea structură:

„LABREPORT”+YYMMDDNNNN raportului de cercetare, unde:

YY – ultimele cifre ale anului curent;

MM – luna, exprimată în cifre;

DD – data, exprimată în cifre;

NNNN – numărul de ordine al documentului raport de încercări de laborator încărcat în sistem, conform înregistrării pentru ziua respectivă;

9) „raport statistic” – codul unic de identificare, generat și atribuit de sistem, care are următoarea structură:

„Titlul raportului” + YYMMDDHHLLSS, unde:

YY – ultimele cifre ale anului curent;

MM – luna, exprimată în cifre;

DD – data, exprimată în cifre;

HH – ora generării raportului;

LL – timpul generării raportului în minute;

SS – timpul generării raportului în secunde.

10) „eveniment” – codul unic de identificare, generat și atribuit de sistem, care are următoarea structură:

„EVENT” + YYMMDDHHLLSS, unde:

YY – ultimele cifre ale anului curent;

MM – luna, exprimată în cifre;

DD – data, exprimată în cifre;

HH – ora generării raportului;

LL – timpul când a avut loc evenimentul;

SS – timpul când a avut loc evenimentul în secunde.

32. În SIGDEJ se utilizează următoarele scenarii de bază:

1) scenariul privind depunerea și înregistrarea în SIGDEJ a solicitărilor de expertiză. Acest scenariu este utilizat de către solicitantul de expertiză și presupune parcurgerea următorilor pași:

a) recepționarea solicitării de expertiză de către utilizatorul instituției de expertiză judiciară responsabil de activitatea de secretariat cu rol de registrator;

b) accesarea SIGDEJ prin intermediul unui navigator web și autentificarea, utilizând serviciul electronic guvernamental de autentificare și control al accesului (MPass). În cazul autentificării cu succes, sistemul redirecționează registratorul către pagina principală, care reprezintă spațiul de lucru al acestuia;

c) selectarea din meniul principal a funcționalității de adăugare a unei noi solicitări de expertiză în sistem. Ca răspuns, sistemul afișează forma electronică care oferă registratorului posibilitatea de a introduce orice informație referitoare la solicitarea de expertiză depusă;

d) scanarea filelor solicitării de expertiză și încărcarea acestora în sistem, completând totodată toate câmpurile obligatorii ale formularului electronic – metadatele solicitării de expertiză. Completarea formularului electronic al unui nou dosar reprezintă transpunerea formularelor în format electronic, care sunt personalizate în funcție de specificul instituției de expertiză judiciară și rolul utilizatorului;

e) validarea de către sistem a datelor introduse. Acest proces implică atât mecanisme de validare de tip *Client-Side*, cât și de tip *Server-Side*. În cazul depistării unor date introduse eronat, sistemul afișează mesajul corespunzător de eroare și evidențiază câmpurile care urmează a fi editate/corectate;

f) salvarea datelor și a solicitării de expertiză scanate în baza de date a sistemului și crearea dosarului electronic, totodată generând și atribuind codurile unice de identificare (ID unic) atât pentru dosarul electronic nou-creat, cât și pentru solicitarea de expertiză recepționată.

g) notificarea prin mijloacele disponibile (de exemplu, e-mail, SMS, dashboardul utilizatorului, inclusiv cabinetul virtual al solicitantului) a tuturor utilizatorilor relevanți despre inițierea unui nou dosar de expertiză;

h) imprimarea recipisei privind confirmarea recepționării solicitării de expertiză și transmiterea acesteia solicitantului;

2) scenariul privind recepționarea și înregistrarea în SIGDEJ a obiectelor de expertizat:

a) recepționarea obiectului de expertizat de către utilizatorul instituției de expertiză judiciară responsabil de activitatea de secretariat cu rol de registrator;

b) accesarea sistemului și selectarea solicitării deja înregistrate;

c) completarea metadatelor necesare privind obiectul de expertizat recepționat;

d) validarea de către sistem a datelor introduse. Acest proces implică atât mecanisme de validare de tip *Client-Side*, cât și de tip *Server-Side*. În cazul

depistării unor date introduse eronat, sistemul afișează mesajul corespunzător de eroare și evidențiază câmpurile care urmează a fi editate/corectate;

e) salvarea datelor completate în baza de date a sistemului și generarea codului de bare unic și irepetabil pentru obiectul de expertizat;

f) imprimarea stickerului cu codul de bare și aplicarea acestuia pe ambalajul obiectului recepționat;

3) scenariul privind acceptarea și repartizarea dosarului în lucru:

a) accesarea sistemului prin intermediul serviciului electronic guvernamental de autentificare și control al accesului (MPass) de către utilizatorul instituției de expertiză judiciară cu rol de conducător;

b) accesarea listei de dosare în așteptare nou-înregistrate în sistem și selectarea unui dosar;

c) vizualizarea informațiilor din dosar și analizarea solicitării de expertiză în vederea luării deciziei referitoare la admisibilitatea și cursul de mai departe al acestuia;

d) setarea statutului privind acceptarea dosarului în lucru;

e) indicarea în sistem a subdiviziunii responsabile și/sau a expertului judiciar/expertilor judiciari, responsabil/responsabili de efectuarea expertizei solicitate. În cazul în care expertul indicat în solicitare nu este disponibil pentru a efectua expertiza, conducătorul propune un alt expert, oferind totodată în sistem toate explicațiile de rigoare. În cazul substituirii expertului, sistemul generează și o scrisoare de ieșire adresată solicitantului, pentru a cere acordul acestuia privind desemnarea altui expert;

f) setarea termenului de efectuare a expertizei, inclusiv în cazul prelungirii acestuia;

g) salvarea datelor completate de către utilizator;

h) notificarea tuturor utilizatorilor relevanți despre faptul distribuirii dosarului și statutul acestuia în sistem;

4) scenariul privind refuzul expertizei:

a) accesarea sistemului de către conducătorul instituției de expertiză judiciară prin intermediul serviciului electronic guvernamental de autentificare și control al accesului (MPass);

b) accesarea listei de dosare în așteptare nou-înregistrate în sistem și selectarea unui dosar;

c) vizualizarea informațiilor din dosar și analizarea solicitării de expertiză în vederea luării deciziei referitor la cursul de mai departe al acestuia;

d) setarea în sistem a statutului de refuz pentru dosarul respectiv, precum și indicarea tuturor explicațiilor și referințelor la cadrul legal privind refuzul efectuării expertizei solicitate;

e) generarea de către sistem a scrisorii de refuz conform datelor oferite de către utilizator la pasul precedent;

f) redactarea, după caz, a scrisorii de refuz de către utilizator și aplicarea semnăturii electronice utilizând serviciul electronic guvernamental integrat de semnătură electronică (MSign);

g) generarea și atribuirea numărului unic de identificare pentru scrisoarea de refuz și expedierea acesteia către solicitant prin intermediul cabinetului virtual și e-mail;

h) imprimarea, după caz, a scrisorii de refuz și expedierea acesteia solicitantului;

5) scenariul privind procesarea documentelor de ieșire:

a) accesarea sistemului prin intermediul serviciului electronic guvernamental de autentificare și control al accesului (MPass) de către utilizatorul din cadrul instituției de expertiză;

b) accesarea funcționalității de creare a unui document nou. Ca răspuns, sistemul afișează la ecran forma de document de tip *blank*, conform șabloanelor preconfigurate în sistem, incluzând antet și subsol conforme specificului instituției de expertiză judiciară;

c) indicarea dosarului de expertiză la care se referă documentul, dacă este cazul;

d) utilizatorul completează conținutul documentului, salvând versiuni intermediare ori de câte ori are nevoie, pentru a putea ulterior reveni la procesul de redactare a documentului;

e) aplicarea semnăturii electronice asupra versiunii finale a documentului;

f) expedierea documentului către conducătorul responsabil conform fluxului de lucru intern al instituției;

g) aplicarea semnăturii electronice de către conducătorul instituției și generarea numărului unic de înregistrare a documentului de ieșire;

h) expedierea în regim electronic a documentului de ieșire către adresat prin intermediul mijloacelor disponibile ale sistemului, cum ar fi cabinetul virtual și e-mail;

i) imprimarea, dacă este cazul, a documentului de ieșire pe suport de hârtie și expedierea acestuia către adresat;

6) scenariul privind procesarea documentelor de intrare:

a) accesarea sistemului prin intermediul serviciului electronic guvernamental de autentificare și control al accesului (MPass) de către utilizatorul responsabil de activitățile de secretariat din cadrul instituției de expertiză;

b) accesarea funcționalității de înregistrare a unui document de intrare. Ca răspuns, sistemul afișează la ecran forma electronică privind înregistrarea și încărcarea documentului de intrare;

c) scanarea documentului recepționat, dacă este pe suport de hârtie, și încărcarea acestuia în sistem;

d) indicarea dosarului de expertiză din cadrul sistemului, în cazul în care documentul de intrare se referă la un anumit dosar de expertiză deja înregistrat în sistem;

e) completarea metadatelor referitoare la document conform câmpurilor obligatorii și opționale ale formei electronice privind documentul de intrare;

f) validarea de către sistem a datelor introduse despre documentul de intrare. Acest proces implică atât mecanisme de validare de tip *Client-Side*, cât și de tip *Server-Side*. În cazul depistării unor date introduse eronat, sistemul afișează mesajul corespunzător de eroare și evidențiază câmpurile care urmează a fi editate/corectate;

g) salvarea documentului și a tuturor metadatelor asociate în baza de date a sistemului, totodată, generând și atribuind numărul de înregistrare unic și irepetabil al documentului;

h) notificarea tuturor utilizatorilor relevanți privind înregistrarea noului document de intrare în cadrul sistemului;

7) scenariul privind procesul de efectuare a expertizei și finalizarea dosarului:

a) accesarea sistemului prin intermediul serviciului electronic guvernamental de autentificare și control al accesului (MPass) de către expertul instituției de expertiză judiciară;

b) accesarea listei de sarcini în așteptare ale expertului și selectarea dosarului distribuit către acesta;

c) verificarea de către sistem prin intermediul serviciului guvernamental de plăți electronice (MPay), dacă serviciile de expertiză au fost achitate și respectiv dacă este posibil să se purceadă nemijlocit la activitățile de expertiză. Pentru cazurile în care nu este posibilă verificarea prin intermediul serviciului guvernamental de plăți electronice (MPay), utilizatorul din cadrul instituției de expertiză va avea posibilitatea să indice în regim manual faptul achitării sau depunerii garanțiilor în acest sens;

d) vizualizarea informațiilor din dosar și analizarea solicitării de expertiză în vederea luării deciziei referitoare la posibilitatea efectuării acesteia;

e) setarea statutului privind luarea dosarului în lucru sau refuzul de efectuare a expertizei, însă oferind obligatoriu toate explicațiile de rigoare în sistem;

f) completarea formelor electronice ale dosarului conform procesului de lucru privind efectuarea expertizelor;

g) atașarea la dosar și a altor documente, dacă este cazul;

h) accesarea funcționalității de generare a raportului de expertiză. Ca răspuns, sistemul va afișa la ecran forma de raport de expertiză de tip *blank*, conform șabloanelor preconfigurate în sistem, incluzând compartimente de document cu antet, subsol și alte elemente conforme specificului instituției de expertiză judiciară;

i) expertul va completa conținutul raportului și va salva versiuni intermediare ori de câte ori este nevoie pentru a putea reveni ulterior la procesul de redactare;

j) salvarea documentului ca versiune prefinală și notificarea supervisorului (șeful de subdiviziune) privind sarcina de verificare a raportului de expertiză;

k) verificarea raportului de expertiză de către supervisor și oferirea comentariilor de rigoare, dacă este cazul;

l) notificarea expertului privind rezultatul verificării, inclusiv punerea la dispoziție a comentariilor oferite de către supervisor;

m) revizuirea versiunii prefinale a raportului de expertiză și notificarea repetată a supervisorului privind necesitatea de verificare a acestuia. Secvența pașilor j) – l) se repetă ciclic până în momentul obținerii rezultatului pozitiv al verificării din partea supervisorului – atunci când va fi setat statutul de versiune finală a raportului de expertiză;

n) semnarea raportului de expertiză de către expert și de alți experți în cazul unei expertize în comisie sau complexe;

o) generarea scrisorii de însoțire a raportului de expertiză, precum și atribuirea numărului de înregistrare unic și irepetabil acesteia;

p) aplicarea semnăturii electronice a conducătorului instituției de expertiză judiciară;

q) expedierea și/sau înmânarea raportului de expertiză solicitantului și restituirea obiectului de expertizat cu indicarea mențiunilor corespunzătoare în sistem;

r) declanșarea procesului de arhivare a dosarului de expertiză;

8) scenariul privind solicitarea cercetărilor de laborator:

a) accesarea sistemului prin intermediul serviciului electronic guvernamental de autentificare și control al accesului (MPass) de către expertul instituției de expertiză judiciară;

b) selectarea și accesarea dosarului de expertiză;

c) accesarea funcționalității de solicitare a cercetării de laborator. Ca răspuns, sistemul afișează la ecran forma precompletată privind solicitarea de efectuare a cercetării de laborator;

d) completarea de către expert a tuturor câmpurilor obligatorii și, dacă este cazul, a celor opționale, cum ar fi tipul cercetării solicitate, laboratorul, termenul-limită de realizare a cercetării și alte date relevante;

e) salvarea solicitării de efectuare a cercetării de laborator în baza de date a sistemului;

f) notificarea tuturor utilizatorilor relevanți, inclusiv a specialistului de laborator, privind solicitarea nouă;

9) scenariul privind procesarea rezultatelor cercetărilor de laborator:

a) accesarea sistemului prin intermediul serviciului electronic guvernamental de autentificare și control al accesului (MPass) de către specialistul de laborator al instituției de expertiză judiciară;

b) selectarea și accesarea solicitării de cercetare de laborator;

c) accesarea funcționalității privind documentarea rezultatului cercetării de laborator. Ca răspuns, sistemul afișează la ecran forma precompletată privind rezultatul cercetării de laborator efectuate;

d) completarea de către specialistul de laborator a tuturor câmpurilor obligatorii și, dacă este cazul, a celor opționale și încărcarea raportului de cercetare de laborator;

e) aplicarea semnăturii electronice a specialistului de laborator care a efectuat cercetarea;

f) salvarea înregistrării și a raportului în baza de date a sistemului;

g) notificarea tuturor utilizatorilor relevanți, inclusiv a expertului care a solicitat cercetarea de laborator;

10) scenariul privind arhivarea dosarului de expertiză:

a) pentru toate dosarele de expertiză finalizate, adică cele în care raportul de expertiză și obiectul de expertizat au fost recepționate de către solicitant, procesul de arhivare se declanșează în mod automat de către sistem;

b) toate documentele și informațiile din dosarul de expertiză ce urmează a fi arhivat se transferă în baza de date a arhivei digitale a sistemului, iar accesul pentru oricare utilizator este restricționat, inclusiv pentru utilizatorii care au participat la procesul de efectuare a expertizei;

c) dosarul căpăta statutul „arhivat” în sistem, iar metadatele acestuia pot participa doar în cadrul procesului de raportare statistică, fără a dezvălui alte informații, documente sau alt tip de conținut din dosar, având un regim de păstrare și arhivare stabilit în actele normative din domeniul expertizei judiciare.

33. Obiectele informaționale reprezintă totalitatea de date care le caracterizează, și anume:

1) date privind obiectul informațional „solicitare de expertiză”:

a) ID – numărul unic de identificare al solicitării de expertiză;

b) titlul;

c) data și timpul depunerii solicitării;

d) data și timpul înregistrării în sistem a solicitării;

e) date privind solicitantul (IDNO/IDNP al persoanei fizice/juridice, nume și prenume/denumire, domiciliu/sediu etc.);

f) tipul expertizei solicitate;

g) expertul solicitat;

h) termenul-limită solicitat pentru efectuarea expertizei;

i) alte documente însoțitoare, dacă este cazul – anexe la solicitarea de expertiză;

j) referința la obiectul de expertizat;

- k) descrierea;
- 2) date privind obiectul informațional „obiect de expertizat”:
 - a) ID – numărul unic de identificare al obiectului de expertizat;
 - b) denumirea;
 - c) date privind solicitantul (IDNO/IDNP al persoanei fizice/juridice, nume și prenume/denumire, domiciliu/sediu etc.);
 - d) descrierea;
 - e) date despre ambalaj, dacă este cazul;
 - f) referință la solicitarea de expertiză depusă;
 - g) alte mențiuni;
- 3) date privind obiectul informațional „document de intrare”:
 - a) ID – numărul de înregistrare și identificare al documentului de intrare;
 - b) tipul documentului;
 - c) titlul;
 - d) data și timpul emiterii documentului;
 - e) date privind autoritatea/instituția emitentă (IDNO, denumire, sediu etc.);
 - f) date privind autoritatea/instituția destinatară (IDNO, denumire, sediu etc.);
 - g) date privind persoana executor al documentului din cadrul autorității/instituției emitente (IDNP, nume, prenume, funcție deținută);
 - h) ID al dosarului de expertiză;
 - i) conținutul documentului;
- 4) date privind obiectul informațional „document de ieșire”:
 - a) ID – numărul de înregistrare și identificare al documentului de ieșire;
 - b) tipul documentului;
 - c) titlul;
 - d) data și timpul emiterii documentului;
 - e) date privind autoritatea/instituția emitentă (IDNO, denumire, sediu etc.);
 - f) date privind autoritatea/instituția destinatară (IDNO, denumire, sediu etc.);
 - g) date privind persoana executor al documentului din cadrul autorității/instituției emitente (IDNP, nume, prenume, funcție deținută);
 - h) ID al dosarului de expertiză;
 - i) conținutul documentului;
- 5) date privind obiectul informațional „notificarea de acceptare”:
 - a) ID – numărul de identificare al notificării de acceptare;
 - b) data și timpul emiterii notificării;
 - c) ID al dosarului de expertiză;
 - d) date privind solicitantul (IDNO/IDNP al persoanei fizice/juridice, nume și prenume/denumire, domiciliu/sediu etc.) cărui îi este adresată notificarea de acceptare;
 - e) ID al autorității/instituției emitente;

f) date privind utilizatorul care a acceptat efectuarea expertizei (IDNP, nume, prenume, funcția deținută);

6) date privind obiectul informațional „notificarea de refuz”:

a) ID – număr de identificare al notificării de refuz;

b) data și timpul emiterii notificării;

c) ID al dosarului de expertiză;

d) date privind solicitantul (IDNP/IDNO al persoanei fizice/juridice, nume și prenume/denumire, domiciliu/sediu etc.) cărui îi este adresată notificarea de refuz;

e) date privind utilizatorul care a refuzat efectuarea expertizei (IDNP, nume, prenume, funcția deținută);

f) motivele refuzului;

7) date privind obiectul informațional „notificarea privind statutul dosarului de expertiză”:

a) ID – număr de identificare al notificării privind statutul dosarului de expertiză;

b) data și timpul emiterii notificării;

c) ID al dosarului de expertiză;

d) datele privind solicitantul (IDNP/IDNO al persoanei fizice/juridice, nume și prenume/denumire, domiciliu/sediu etc.) cărui îi este adresată notificarea privind statutul dosarului de expertiză;

e) date privind autoritatea/instituția emitentă (IDNO, denumire, sediu etc.);

f) date privind statutul dosarului;

g) date privind statutul precedent al dosarului;

h) date privind statutul următor, conform fluxului de expertiză judiciară.

8) date privind obiectul informațional „raport de cercetare de laborator”:

a) ID – numărul de identificare al raportului de cercetare de laborator;

b) tipul raportului;

c) titlul;

d) data și timpul înregistrării raportului;

e) data și timpul efectuării cercetării de laborator;

f) laboratorul care a efectuat cercetarea;

g) date privind persoana responsabilă care a întocmit raportul de cercetare de laborator (IDNP, nume și prenume, funcție deținută etc.);

h) ID al dosarului de expertiză;

i) date privind solicitantul cercetării de laborator (IDNP/IDNO al persoanei fizice/juridice, nume și prenume/denumire, domiciliu/sediu, funcție deținută etc.);

j) rezultatul sau concluziile încercărilor de laborator (mențione în sistem, document Word sau PDF);

9) date privind obiectul informațional „raport statistic”:

a) ID – numărul de identificare al raportului statistic;

b) tipul raportului;

- c) titlul;
- d) data și timpul înregistrării raportului;
- e) perioada selectată de raportare;
- 10) date privind obiectul informațional „evenimentul”:
 - a) ID al evenimentului;
 - b) tipul evenimentului;
 - c) statutul;
 - d) data și timpul înregistrării evenimentului;
 - e) tipul operațiunii efectuate de către utilizator;
 - f) utilizatorul care a efectuat operațiunea (IDNP, nume și prenume, funcția deținută).

34. Pentru a asigura autenticitatea și pentru a reduce volumul de informații stocate în sistem, se utilizează sistemul de clasificatoare. Clasificatoarele se grupează în: internațional, național și departamental.

În cadrul SIGDEJ se folosesc cel puțin următoarele clasificatoare naționale:

- 1) CUATM – Clasificatorul unităților administrativ-teritoriale;
- 2) CFOJ – Clasificatorul formelor organizațional-juridice ale agenților economici.

35. Clasificatoarele departamentale urmează să fie elaborate și utilizate în cadrul SIGDEJ numai în absența clasificatoarelor naționale și internaționale aprobate.

36. Pentru asigurarea formării corecte a resursei informaționale a SIGDEJ, este necesară organizarea accesului la resursele informaționale ale următoarelor sisteme informaționale:

- 1) sistemele informaționale partajate:
 - a) serviciul electronic guvernamental de autentificare și control al accesului (MPass) – în vederea autentificării utilizatorilor în sistem;
 - b) serviciul electronic guvernamental integrat de semnătură electronică (MSign);
 - c) serviciului guvernamental de plăți electronice (MPay) – în vederea efectuării și verificării plăților, unde este cazul;
 - d) serviciul electronic guvernamental de jurnalizare (MLog);
 - e) serviciul electronic guvernamental de notificare (MNotify);
- 2) sistemul informațional „Registrul de stat al unităților de drept”, care conține date despre toate categoriile de unități de drept constituite în bază legală – în scopul preluării și validării datelor despre persoanele juridice privind corectitudinea combinațiilor de IDNO, denumire, cod CUATM, cod CAEM etc., necesare înregistrărilor, modificărilor sau radierilor care conțin date despre persoane juridice;

3) sistemul informațional „Registrul de stat al populației”, care include date despre persoanele fizice – în vederea preluării și validării înregistrărilor, modificărilor sau radierilor care conțin date despre persoane fizice și a verificării acestora privind corectitudinea combinațiilor de IDNP, nume, prenume, act de identitate;

4) sistemul informațional „Registrul de stat al unităților administrativ-teritoriale și al adreselor”, care cuprinde date cu privire la unitățile teritorial-administrative, străzi, clădiri, amplasarea imobilelor etc.;

5) programul Integrat de Gestionare a Dosarelor „PIGD”, implementat în instanțele de judecată;

6) sistemul informațional „Urmărire penală: E-Dosar” al Procuraturii Generale.

37. Interoperabilitatea dintre SIGDEJ și resursele informaționale de stat se asigură prin intermediul platformei de interoperabilitate (MConnect) în conformitate cu prevederile cadrului normativ ce reglementează domeniul interoperabilității și schimbului de date.

VII. SPAȚIUL TEHNOLOGIC AL SIGDEJ

38. SIGDEJ urmează a fi găzduit pe platforma tehnologică guvernamentală comună (MCloud) în conformitate cu Hotărârea Guvernului nr. 128/2014 privind platforma tehnologică guvernamentală comună (MCloud).

39. Arhitectura SIGDEJ urmează să fie SOA (Service-Oriented Architecture), ceea ce permite ca SIGDEJ să fie integrat cu toate sistemele informaționale partajate precum: serviciului guvernamental de plăți electronice (MPay), serviciul electronic guvernamental integrat de semnătură electronică (MSign), serviciul electronic guvernamental de autentificare și control al accesului (MPass), serviciul electronic guvernamental de jurnalizare (MLog) și serviciul electronic guvernamental de notificare (MNotify), precum și cu alte sisteme informaționale de stat.

40. Datorită faptului că interfața de client al SIGDEJ este preconizat să fie navigatorul (browser) web, nu sunt necesare resurse hardware și software adăugătoare semnificative.

41. Platforma tehnologică a SIGDEJ are următoarele funcții:

1) asigură formate unice de prezentare a datelor și protocoale comune de schimb de date;

2) oferă mecanisme de asigurare a concordanței bazelor de date ale SIGDEJ cu cele ale sistemelor informaționale ale altor autorități publice.

Concordanța este respectată în termeni de clasificatoare, nomenclatoare, completitudine etc.;

3) pune la dispoziția dezvoltatorilor de software un cadru formal și metodologic propice creării și implementării sistemului de management al securității informaționale.

42. Produsele programului și echipamentele SIGDEJ trebuie să satisfacă următoarele cerințe:

- 1) să asigure posibilitatea stocării unor volume mari de informații;
- 2) să asigure posibilitatea extinderii funcționale și a puterii de calcul (extensibilitate și scalabilitate);
- 3) să susțină prelucrarea distribuită a datelor, accesul la resurse atât în rețeaua locală, cât și în internet;
- 4) să utilizeze un sistem unic de clasificare și codificare;
- 5) să funcționeze pe diferite platforme hardware;
- 6) să asigure fiabilitate înaltă;
- 7) să asigure consistența și completitudinea informației;
- 8) să susțină posibilitatea de modernizare în timpul procesului de exploatare.

43. Posesorul SIGDEJ urmează să asigure găzduirea acestuia pe platforma tehnologică guvernamentală comună (MCloud).

VII. ASIGURAREA SECURITĂȚII INFORMAȚIONALE A SIGDEJ

44. Securitatea informațională presupune protecția SIGDEJ la toate etapele proceselor de creare, procesare, stocare și transmitere a datelor de acțiuni accidentale sau intenționate cu caracter artificial sau natural, care au ca rezultat cauzarea prejudiciului posesorului și utilizatorilor resurselor și infrastructurii informaționale.

45. Asigurarea securității informaționale va fi realizată în conformitate cu Cerințele minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr. 201/2017. Pentru gestiunea riscurilor de securitate va fi implementată o politică generală de securitate. Personalul implicat în utilizarea și administrarea SIGDEJ va fi instruit în ceea ce privește riscurile de securitate la care poate fi expus. Politica de securitate va include prevederi referitoare la organizarea auditurilor periodice de securitate pentru a verifica politica și conformitatea cu regulile de securitate, precum și pentru a stabili domeniile care necesită îmbunătățiri.

46. Posesorul, deținătorul și registratorii vor proteja SIGDEJ de pericolul cauzării prejudiciilor resurselor sau infrastructurii informaționale. Principalele pericole pentru securitatea informațională a SIGDEJ sunt:

- 1) colectarea și utilizarea ilegală a datelor;
- 2) încălcarea tehnologiei de prelucrare a datelor;
- 3) implementarea în produsele software și hardware a componentelor care realizează funcții neprevăzute în documentația care însoțește aceste produse;
- 4) elaborarea și răspândirea programelor ce pot afecta funcționarea normală a sistemelor informaționale și de comunicații, precum și a sistemelor de protecție a informației;
- 5) nimicirea, deteriorarea, suprimarea radioelectronică sau distrugerea mijloacelor hardware și/sau software de prelucrare a informației;
- 6) influențarea sistemelor cu parolă-cheie de protecție a sistemelor automatizate de prelucrare și transmitere a datelor;
- 7) compromiterea cheilor și a mijloacelor de protecție criptografică a informației;
- 8) scurgerea de informație prin canale tehnice;
- 9) implementarea dispozitivelor electronice de interceptare a informației în mijloacele tehnice de prelucrare, păstrare și transmitere a datelor prin canalele de comunicații, precum și în încăperile de serviciu ale registratorilor sistemului;
- 10) nimicirea, deteriorarea, distrugerea sau sustragerea suporturilor de informație mecanice sau de alt tip;
- 11) tentativele de interceptare a datelor în rețelele locale ale registratorilor sistemului și în liniile de comunicații, decodificarea și impunerea informației false;
- 12) utilizarea tehnologiilor informaționale necertificate, a mijloacelor de protecție a datelor, a mijloacelor de informatizare și comunicații la crearea și dezvoltarea infrastructurii informaționale;
- 13) accesul neautorizat la resursele informaționale care se află în băncile și bazele de date;
- 14) încălcarea restricțiilor legale ce țin de răspândirea informației;
- 15) încălcarea prevederilor Legii nr. 133/2011 privind protecția datelor cu caracter personal.

47. Protecția datelor cu caracter personal se asigură prin următoarele acțiuni:

- 1) posesorul, deținătorul și registratorii vor prelucra doar datele cu caracter personal strict necesare, neexcesive scopului prestabilit, conform competențelor atribuite, respectând principiile stabilite în actele normative din domeniul protecției datelor cu caracter personal;
- 2) posesorul și deținătorul vor asigura măsuri organizatorice și tehnice necesare pentru protecția datelor cu caracter personal împotriva distrugerii, modificării, blocării, copierii, răspândirii, precum și împotriva altor acțiuni

ilicite, măsuri menite să asigure un nivel de securitate adecvat în ceea ce privește riscurile prezentate de prelucrare și caracterul datelor prelucrate;

3) posesorul, deținătorul și administratorul tehnic în cazul incidentelor de securitate vor întreprinde măsuri necesare pentru depistarea sursei de producere a incidentului, vor efectua analiza acestuia și vor înlătura cauzele incidentului de securitate cu informarea Centrului Național pentru Protecția Datelor cu Caracter Personal;

4) posesorul, deținătorul și registratorii, în limitele responsabilităților, vor asigura respectarea drepturilor subiecților de date cu caracter personal în cadrul operațiunilor de prelucrare a datelor cu caracter personal efectuate conform prezentului Concept.

48. SIGDEJ asigură realizarea următoarelor obiective de securitate:

1) autentificarea – garantează că zonele restricționate ale SIGDEJ vor fi accesibile doar utilizatorilor cu o identitate verificată prin serviciul electronic guvernamental de autentificare și control al accesului (MPass);

2) autorizarea – garantează că utilizatorii autentificați prin serviciul electronic guvernamental de autentificare și control al accesului (MPass) pot accesa serviciile și datele care corespund drepturilor lor de acces;

3) confidențialitatea – garantează că datele înregistrate în RDEJ nu pot fi accesate de o parte terță neautorizată;

4) integritatea – garantează că datele înregistrate în RDEJ nu au fost modificate sau alterate de o parte terță neautorizată;

5) nonrepudierea – garantează că datele înregistrate în RDEJ nu pot fi negate mai târziu.

49. Pentru atingerea obiectivelor de securitate, SIGDEJ trebuie să dispună de mai multe mecanisme de securitate:

1) semnătura electronică – mecanism ce asigură integritatea și nonrepudierea datelor înregistrate în RDEJ;

2) firewall – filtrul firewall face parte din arhitectura tehnică a platformei tehnologice (MCloud) pentru a asigura un mecanism de apărare împotriva utilizatorilor externi neautorizați;

3) antivirus/antispam – soluțiile hardware și/sau software asigură protecția antivirus și antispam pentru toate serverele. Fișierele se scanează la încărcare în SIGDEJ. În cazul detectării unui fișier infectat, procedura de încărcare este oprită și fișierul – respins;

4) sistem de detectare a intruziunilor – sistem de detectare a accesului neautorizat la nivelul componentelor de sistem al SIGDEJ;

5) comunicare sigură (transferuri de date) între serverele web și utilizatori – schimbul de informații confidențiale este securizat;

6) backup sistematic al datelor păstrate – permite recuperarea rapidă și fiabilă a datelor în caz de incident care a dus la pierderea sau deteriorarea datelor;

7) instrument de înregistrare a evenimentelor de audit – toate activitățile desfășurate de către utilizatori, indiferent dacă au succes sau nu (cum ar fi conectările încercate, dar nereușite), sunt monitorizate și înregistrate în jurnalele SIGDEJ, cu acces limitat pentru utilizatorii neautorizați.

50. În cadrul SIGDEJ se asigură generarea și păstrarea înregistrărilor de audit ale securității pentru operațiile de prelucrare a datelor cu caracter personal în condițiile cadrului normativ în materie de protecție a datelor cu caracter personal. Înregistrările de audit ale operațiilor și rezultatele acestora pot fi accesate de către Centrul Național pentru Protecția Datelor cu Caracter Personal și puse la dispoziția acestuia în scopul investigării potențialelor încălcări ale regimului de prelucrare/protecție a datelor cu caracter personal. SIGDEJ va utiliza funcționalitatea de autentificare doar prin intermediul serviciului electronic guvernamental de autentificare și control al accesului (MPass).

51. Utilizatorii SIGDEJ vor fi autorizați să acceseze doar blocurile funcționale și datele pentru care au permisiunile necesare conform rolurilor fiecăruia. Utilizatorii și rolurile acestora vor fi gestionate prin intermediul serviciului electronic guvernamental de autentificare și control al accesului (MPass). SIGDEJ va prelua rolurile utilizatorilor din serviciul electronic guvernamental de autentificare și control al accesului (MPass).

O necesitate importantă legată de securitate este păstrarea înregistrărilor de audit pentru analiza integrității SIGDEJ și pentru monitorizarea activității utilizatorilor. SIGDEJ se va baza pe un mecanism de înregistrări de audit dublu (intern și cu utilizarea serviciului electronic guvernamental de jurnalizare (MLog)), ce urmează practicile internaționale.

Notă informativă
la proiectul hotărârii Guvernului „Cu privire la aprobarea Conceptului
Sistemului informațional „Gestiunea Dosarelor de Expertiză Judiciară”

1. Denumirea autorului și, după caz, a participanților la elaborarea proiectului

Proiectul hotărârii Guvernului „Cu privire la aprobarea Conceptului Sistemului informațional „Gestiunea Dosarelor de Expertiză Judiciară” (în continuare – proiect) a fost elaborat de Ministerul Justiției cu suportul proiectului „Consolidarea Eficienței și Accesul la Justiție” al Programului Națiunilor Unite Pentru Dezvoltare din Moldova (în continuare – PNUD).

2. Condițiile ce au impus elaborarea proiectului actului normativ și finalitățile urmărite

Instituțiile de expertiză judiciară reprezintă o parte integrantă a sistemului de justiție din Republica Moldova, întrucât reprezintă forma organizatorică a activității experților judiciari, care, la rândul lor, contribuie la ameliorarea eficienței judiciare, oferind judecătorilor răspunsuri clare și argumentate asupra problemelor specifice și complexe cu care se confruntă aceștia la înfăptuirea justiției. Calitatea și acuratețea investigațiilor și expertizelor judiciare sau extrajudiciare au un impact imens asupra calității justiției și, implicit, asupra percepției generale a societății asupra sistemului de justiție în ansamblu.

Necesitatea elaborării și implementării unui sistem informațional în activitatea de efectuare a expertizei judiciare vine în contextul în care, instituțiile de expertiză judiciară necesită o asistență sporită, determinată de importanța lor pentru sectorul justiției.

Procedurile operaționale existente în procesul desfășurării activității instituțiilor de expertiză judiciară, cu mici excepții, sunt bazate pe hârtie. Aceasta determină existența unor riscuri și vulnerabilități care vizează siguranța și integritatea rapoartelor de expertiză, o durată mai mare de timp a procedurilor ce vizează interacțiunea cu alte autorități publice din sectorul justiției (procuratura, organele de urmărire penală, instanțele judecătorești, etc), existența unor proceduri interne care variază de la o instituție la alta, varietate determinată de sisteme proprii de evidență a dosarelor aflate pe rol.

În această ordine de idei menționăm că elaborarea și implementarea unui sistem informațional va permite eliminarea decalajelor cu procedurile altor actori ai sectorului justiției și integrarea activității de efectuare a expertizelor judiciare într-un proces coerent și coordonat.

Totodată, dezvoltarea și asigurarea funcționalității acestui sistem și asigurarea interoperabilității și schimbului de date a acestuia cu alte sisteme informaționale din sectorul justiției va consolida colectarea și prelucrarea datelor dezagregate și vor asigura accesibilitatea acestor informații pentru public, conducând la promovarea și asigurarea transparenței și eficacității procedurilor judiciare. Automatizarea procedurilor de efectuare a expertizei judiciare va permite, de asemenea, partajarea rapoartelor de expertiză judiciară cu alți actori relevanți din sectorul justiției în mod electronic și va asigura interoperabilitatea cu alte sisteme

informaționale de stat, accelerând astfel interacțiunea și comunicarea între actorii relevanți ai sectorului justiției în cauzele penale, civile și contravenționale.

De asemenea, subliniem faptul că elaborarea proiectului se înscrie în contextul de ansamblu al cadrului de politici și celui normativ atât în domeniul expertizei judiciare, cât și în domeniile informatizării, modernizării tehnologice a guvernării și a serviciilor guvernamentale.

Deși în prezent la nivel național nu există un document de politici care să abordeze separat problematica dezvoltării domeniului expertizei judiciare și a statutului experților judiciari. Preocupările pentru acest subdomeniu al sectorului justiției au fost abordate într-un context mai larg de implementare a Strategiei de reformă a sectorului justiției pentru anii 2011-2016 și a Planului de acțiuni pentru implementarea acesteia, a cărui executare a durat până la finele anului 2017.

În cadrul Ministerului Justiției a fost elaborat documentul de politici Strategia pentru asigurarea independenței și integrității sectorului justiției pentru anii 2022-2025, ulterior adoptată de către Parlamentul Republicii Moldova prin Legea nr. 211/2011. În această ordine de idei, de către minister a fost aprobat Planul de acțiuni pentru implementarea acesteia, care cuprinde, între altele, în contextul realizării obiectivului de consolidare a autoadministrării, independenței și responsabilității profesiilor conexe justiției, acțiunea de efectuare a unei analize privind instituirea conceptului unificării metodologiilor de efectuare a expertizelor judiciare.

În acest context, o abordare strategică pozitivă pe dimensiunea unificării procedurilor și metodologiei de efectuare a expertizelor judiciare constituie un argument în susținerea obiectivului de automatizare a procesului de gestiune a cazurilor de expertiză judiciară care va constitui o contribuție consistentă la realizarea obiectivelor politicii statului în acest domeniu. În situația dată, în Planul de acțiuni al Guvernului pentru anii 2021-2022 în compartimentul „Justiție și Anticorupție” își setează ca obiectiv (pct. 310.5.) – „Aprobarea Conceptului tehnic al Sistemului informațional automatizat „Gestiunea dosarelor de expertiză judiciară”.

Elaborarea proiectului este determinată de prevederile art. 7⁶ din Legea nr. 467/2003 cu privire la informatizare și resursele informaționale de stat, care reglementează obligativitatea documentării sistemelor și resurselor informaționale de stat. Astfel, potrivit alin. (2) lit. a) din acest articol unul din documentele care trebuie să stea la baza creării și implementării unui sistem informațional sau resurse informaționale este conceptul, care trebuie să determine spațiul funcțional, structura organizatorică, spațiul informațional, spațiul tehnologic, securitatea sistemului informațional și protecția informației.

Astfel, reieșind din cele menționate mai sus, a fost decisă crearea și implementarea unui sistem informațional în activitatea de efectuare a expertizei judiciare și, în acest scop, a fost elaborat proiectul hotărârii Guvernului „Cu privire la aprobarea Conceptului Sistemului informațional „Gestiunea Dosarelor de Expertiză Judiciară”.

3. Principalele prevederi ale proiectului și evidențierea elementelor noi

Proiectul cuprinde prevederi care stabilesc statutul și locul sistemului informațional în spectrul de resurse și sistemele informaționale ale statului,

obiectivele, principiile și cadrul normativ în baza cărora sistemul urmează a fi creat și implementat, spațiul funcțional, structura organizatorică, spațiul informațional și tehnologic, precum și aspectele relevante de asigurare a securității informaționale a sistemului.

Astfel, reprezintă o soluție informatică din categoria Guvern pentru Guvern (G2G) și constituie totalitatea mijloacelor software, hardware și infrastructurii utilizatorului, destinate pentru procesarea informației și formarea resursei informaționale cu privire la dosarele de expertiză judiciară – Registrul dosarelor de expertiză judiciară.

Registrul dosarelor de expertiză judiciară va fi un registru de stat, ținut în scopul înregistrării rapoartelor de expertiză întocmite de către sau cu participarea experților judiciari care activează în cadrul instituțiilor de expertiză judiciară înregistrate în Republica Moldova și formării dosarelor de expertiză judiciară în conformitate cu prevederile art. 39 alin. (2) din Legea nr. 68/2016 cu privire la expertiza judiciară și statutul expertului judiciar.

Obiectivele de bază ale sistemului informațional ce se preconizează a fi creat sunt:

- a) crearea resursei informaționale a activității de expertiză judiciară desfășurată de către instituțiile de expertiză judiciară înregistrate în Republica Moldova, în vederea creării și păstrării dosarelor de expertiză judiciară prin stocarea, sistematizarea și actualizarea informațiilor ce sunt procesate de către acestea și asigurării unui nivel adecvat de protecție a datelor;
- b) eficientizarea lucrului personalului din cadrul instituțiilor de expertiză judiciară, prin minimizarea utilizării hârtiei în activitatea de stocare și prelucrare a informațiilor;
- c) asigurarea lanțului de trasabilitate și custodie a obiectelor de expertizat;
- d) asigurarea calității și veridicității informației vehiculate în cadrul proceselor de efectuare a expertizelor;
- e) identificarea unică și asigurarea gestiunii și trasabilității documentelor;
- f) eliminarea poverii de completare în regim manual a diferitor registre și rapoarte pe suport de hârtie;
- g) centralizarea tuturor datelor și informațiilor referitoare la dosarele de expertiză judiciară într-o bază de date unică și oferirea accesului la informații atât agregate, cât și în detaliu, de diferite forme de prezentare;
- h) asigurarea protecției datelor și a altor aspecte de securitate informațională referitoare la expertiza judiciară;
- i) reducerea timpului necesar colectării datelor necesare și a timpului pentru elaborarea și consolidarea rapoartelor integrate prin utilizarea unui instrument tehnologic modern de raportare;
- j) minimizarea interacțiunii fizice între solicitanții de expertize și instituțiile de expertiză judiciară;
- k) crearea unui mecanism pentru ca solicitanții de expertize să poată urmări evoluția solicitărilor lor;
- l) contribuirea la diminuarea volumului de documente procesate pe suport de hârtie în cadrul instituțiilor de expertiză judiciară.

De asemenea proiectul delimitează subiecții raporturilor juridice în domeniul creării, dezvoltării și utilizării sistemului informațional, reglementând competența acestora. Astfel, în conformitate cu prevederile art. 11 – art. 15 din Legea nr.71/2007 cu privire la registre și art. 7² – 7⁶ din legea nr. 467/2003 cu privire la informatizare și resursele informaționale de stat, posesor al sistemului se propune a fi desemnat Ministerul Justiției, deținător - Agenția Resurse Informaționale Juridice, iar ca administrator tehnic – Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică”.

Arhitectura sistemului este concepută după schema-tip a infrastructurii informaționale a sistemului informațional.

Din perspectiva spațiului tehnologic, menționăm că sistemul va avea o arhitectură orientată pe servicii, ceea ce-i va permite integrarea cu și utilizarea serviciilor guvernamentale de platformă (MPass, MSign, Mpay, MLog, MNotify) și găzduirea pe platforma tehnologică guvernamentală MCloud. Sistemul se va interconecta în vederea schimbului de date și cu alte sisteme informaționale sau resurse informaționale prin intermediul platformei de interoperabilitate MConnect.

Proiectul de asemenea, propune reglementarea expresă a măsurilor de asigurare a protecției și securității informației conținute în sistem, identificând obiectele ce necesită a fi protejate și metodele de protecție, inclusiv cele de contracarare a pericolelor informaționale. În acest context, securitatea informațională a sistemului va trebui să se conformeze cerințelor stabilite de către legislația Republicii Moldova, precum și de standardele internaționale care nu contravin legii și permit sporirea gradului de securitate, astfel asigurând:

- a) confidențialitatea informației, care presupune limitarea accesului la informație pentru persoanele fără drepturi și împuterniciri corespunzătoare;
- b) integritatea logică a informației, adică prevenirea introducerii, modificării, copierii, actualizării și nimicirii neautorizate a informației;
- c) integritatea fizică a informației;
- d) protecția infrastructurii informaționale împotriva deteriorării și încercărilor de modificare a funcționării.

Pentru îndeplinirea sarcinilor privind asigurarea securității informaționale și a protecției datelor cu caracter personal, în sistem vor fi utilizate mecanismele de autentificare și autorizarea utilizatorilor prin intermediul serviciului MPass și mijloacele proprii ale sistemului; management al accesului și înregistrarea acțiunilor și auditul prin utilizarea serviciului MLog.

4. Fundamentarea economico-financiară

Pentru identificarea și estimarea beneficiilor și costurilor proiectului a fost efectuată analiza de impact în conformitate cu prevederile Metodologiei de analiză a impactului în procesul de fundamentare a proiectelor de acte normative, aprobată prin Hotărârea Guvernului nr. 23/2019.

Astfel, pe de o parte, cele mai importante **beneficii** cuantificabile în urma revizuirii proceselor din cadrul sistemului de expertiză judiciară, digitizarea fluxului de documente și implementarea SIGDEJ se referă în special la economia considerabilă de timp, cheltuieli pentru transport și pentru purtători de informație

(hîrtie). Aceste economii sunt estimate, conform analizei de impact, la o cifră minimă de circa **17 592,3 mii lei pe an**.

Pe de altă parte **costurile** opțiunii recomandate în analiza de impact sunt de aproximativ **298,7 mii lei anual**, care include costul anual de mentenanță, estimat la 236,1 mii lei și cheltuielile legate de utilizarea semnăturii electronice de circa 62, 6 mii lei. În context menționăm că costurile dezvoltării și punerii în aplicare a SIGDEJ (de circa 127-200 mii USD) este suportat de către proiectul PNUD „Consolidarea eficienței și accesului la justiție în Moldova”, existând posibilitatea unei finanțări suplimentare pentru asigurarea mentenanței sistemului nou creat din contul resurselor PNUD până la finele anului 2022.

Ulterior, pentru mentenanța sistemului informațional menționat vor fi alocate sume din contul și în limita bugetului anual al Ministerului Justiției.

5. Modul de încorporare a actului în cadrul normativ în vigoare

Conform prevederilor art.7⁶ din *Legea nr. 467/2003 cu privire la informatizare și resursele informaționale de stat*, sistemele și resurselor informaționale de stat se supun documentării în mod obligatoriu. Adică, pentru dezvoltarea și punerea în aplicare a unui sistem informațional automatizat în calitate de resursă informațională de stat, este obligatoriu ca să fie elaborate și aprobate un șir de documente aferente acestui sistem informațional, conform cadrului normativ metodologic privind crearea, administrarea, mentenanța, dezvoltarea și scoaterea din exploatare a sistemelor informaționale de stat. Documentele sistemelor și resurselor informaționale de stat sunt:

a) conceptul sistemului informațional, în care să fie definite: spațiul funcțional, structura organizatorică, spațiul informațional, spațiul tehnologic, securitatea sistemului informațional și protecția informației;

b) caietul de sarcini al sistemului informațional, care include cerințele funcționale și tehnice în conformitate cu care se creează sistemul informațional;

c) regulamentul resursei informaționale, care să cuprindă: reglementări privind drepturile și obligațiile subiecților raporturilor juridice aferente creării și ținerii resursei informaționale; modalitatea de ținere a resursei informaționale; procedura de înregistrare, modificare, completare și radiere a datelor; procedura de interacțiune cu furnizorii de date; măsuri privind asigurarea securității resursei informaționale.

Prin urmare, după adoptarea proiectului de Concept al SIGDEJ, urmează să fie aprobate de către posesor cerințele tehnice ale sistemului și, după elaborarea nemijlocită a sistemului informațional, până la punerea în acestuia în exploatare, urmează a fi aprobat Regulamentului de organizare și funcționare a resursei informaționale – Registrul dosarelor de expertiză judiciară.

La același capitol ținem să relevăm faptul că, în conformitate cu proiectul de Concept al SIGDEJ, acest sistem la o primă etapă va oferi o flexibilitate funcțională, ceea ce va permite păstrarea și pe suport de hîrtie a anumitor etape ale procedurii de efectuare a expertizei judiciare. Totuși, într-o perioadă de timp previzibilă, pentru a elimina barierele existente în legislația actuală, astfel încât să fie posibilă

digitalizarea absolută a procedurii de efectuare a expertizei judiciare vor fi necesare o serie de modificări ale cadrului legal.

Astfel, în Legea nr. 68/2016 cu privire la expertiza judiciară și statutul expertului judiciar va fi necesară:

a) completarea legii cu prevederi prin care va fi reglementată posibilitatea utilizării unui sistem informațional în activitatea de efectuare a expertizei judiciare;

b) modificarea prevederilor legii care reglementează „forma scrisă” a oricărui document. În acest sens este necesar de specificat că această formă (scrisă) presupune atât documente pe suport de hârtie, cât și documente electronice, iar sintagmele care se referă la semnătură să reglementeze expres că poate fi aplicată și semnătura electronică. În mod special, art. 37, care reglementează forma și conținutul raportului de expertiză judiciară, trebuie să stabilească expres că „forma scrisă” a raportului presupune atât forma unui document electronic, cât și forma unui document pe suport de hârtie. Aceste modificări sunt necesare, deoarece raportul de expertiză judiciară se încadrează în categoria actelor cu caracter administrativ, distincția clară de formă electronică și formă scrisă, ca două forme separate, așa cum prevede Codul Civil, nefiind aplicabilă în privința raportului.

c) La art. 39 este necesar de specificat că arhiva se ține doar în formă electronică.

În *Codul de procedură penală*, la art. 151 alin. (1), urmează a se exclude prevederea conform căruia raportul este în formă „tipărită” și complementar după cuvintele „în formă scrisă” de completat „ca document electronic sau pe suport de hârtie” și la alin. (6) trebuie de specificat complementar că raportul se semnează cu semnătură electronică avansată calificată de expert, în cazul în care se emite în formă de document electronic.

În aceeași ordine de idei, este recomandabil ca și în *Codul de procedură civilă* să fie incluse completări în urma cărora cel puțin se vor echivala raportului de expertiză pe suport de hârtie cu raportul de expertiză în formă de document electronic.

De asemenea, odată cu darea în exploatare a sistemului informațional, va fi necesară ajustarea actelor departamentale, în mod special cele ale instituțiilor de expertiză judiciară, având ca obiectiv asigurarea implementării corespunzătoare a acestui instrument în procedurile interne specifice fiecărei instituții.

În aceeași ordine de idei, în contextul necesității asigurării integrării sistemului cu alte sisteme informaționale guvernamentale, inclusiv cele partajate, va fi necesară semnarea unor acte juridice cu posesorii acestor sisteme în conformitate cu mecanismele prevăzute de actele normative ale Guvernului prin care se reglementează modul de organizare și funcționare ale acestora.

6. Avizarea și consultarea publică a proiectului

În scopul respectării prevederilor *Legii nr. 239/2008 privind transparența în procesul decizional*, proiectul hotărârii este plasat pe pagina web oficială a Ministerului Justiției www.justice.gov.md, compartimentul *Transparența decizională*, directoriul *Proiecte de acte normative remise spre coordonare*.

De asemenea, conform prevederilor art. 20 al *Legii nr. 100/2017 cu privire la actele normative*, elaborarea prezentului proiect de lege a fost demarată odată cu publicarea

pe pagina web oficială a Ministerului Justiției la compartimentul *Transparența decizională*, directoriul *Anunțuri privind inițierea elaborării actelor normative*, a anunțului de inițiere a procesului de elaborare.

Proiectul a fost înregistrat la Cancelaria de Stat cu **nr. unic 514/MJ/2021** și prezentat în cadrul ședinței Secretarilor Generali. Ulterior, proiectul menționat a fost remis la avizare instituțiilor interesate, iar avizele recepționate au fost incluse în tabelul de sinteză.

Ulterior, prin scrisoarea cu nr. 03/1666 din 21 februarie 2022 proiectul menționat a fost remis la avizare repetată, fiind recepționate avizele instituțiilor interesate și incluse în tabelul de sinteză.

7. Constatările expertizei anticorupție

Prin scrisoarea cu nr. 06/2-1252 din 3 martie 2022, a fost recepționat expertiza anticorupție. În urma expertizei s-a constatat că proiectul respectă rigorile de transparență impuse de *Legea nr. 239/2008 privind transparența în procesul decizional*, autorul a asigurat informarea publicului despre inițierea elaborării proiectului de decizie, precum și consultarea publică a acestuia.

Prevederile proiectului corespund scopului declarat de către autor în nota informativă și acesta este în conformitate cu interesul public.

În normele formulate prin proiectul supus expertizei anticorupție n-au fost identificați careva factori de riscuri de corupție.

Ministru



Sergiu LITVINENCO