Slepenība, IT un miljardi...: kā sabrūk valsts institūcijas un kā nepazaudēt valsti

Autori: Sanda Liepiņa, Ivo Rollis, Līga Stafecka
16.aprīlis, 2026.

Ievads

Latvijā kārtējais IT iepirkumu skandāls vairs neizskatās pēc atsevišķa "nejauka gadījuma". Tas drīzāk izskatās pēc simptomiem tam, ka institūcija, kurai bija jābūt valsts digitālās attīstības flagmanim, pati ir kļuvusi par risku – gan nodokļu maksātāju naudas, gan valsts reputācijas, gan 2026. gada demokrātisku vēlēšanu norises ziņā.

Šādā brīdī politiskais vilinājums ir meklēt vienkāršus risinājumus – nomainīt vadītāju, pamainīt dažus iekšējos noteikumus, publiski apsolīt "stingrāku kontroli" un sniegt ļoti virspusēju informāciju par izpildē esošajiem IT sistēmu izstrādes līgumiem un plānoto darbu pie vēlēšanu norises. Tieši tas ir noticis mēneša laikā kopš 2026. gada 18. marta ziņas par Eiropas Prokuratūras veikto izmeklēšanu Latvijā. [7] **Taču citu Eiropas valstu piemēri parāda, ka arī Latvijā šoreiz ar to nepietiks. Ir brīži, kad godīgāk ir atzīt: konkrētā iestāde kā sistēma ir izgāzusies.** Uzreiz gan jābrīdina, ka tikai ar vienas iestādes nomaiņu vien arī nepietiks. Jaunā struktūra pati par sevi nebūs izolēta no vecās sistēmas, ja netiks mainīta pārvaldības pieeja, kas nosaka prioritātes, kas koordinē iesaistītās institūcijas, kurš politiski atbild par gala rezultātu un kā tiek uzraudzīts, lai kritiskas digitālās sistēmas nekļūtu par pašplūsmā vadītiem tehniskiem projektiem.

Dānijas nodokļu dienesta SKAT stāsts ir viens no spilgtākajiem piemēriem. Tas palīdz saprast, kādi scenāriji Latvijai patiesībā ir uz galda – un kādas kļūdas nevajadzētu atkārtot. [34][35][37][32]

Pašreizējais skandāls parāda ne tikai konkrētus likumpārkāpumus, bet arī to, kas notiek, kad kritiski svarīga valsts iestāde gadiem ilgi strādā "ārpus radara". Lielie IT līgumi, riska ziņojumi un iekšējie auditi tiek klasificēti kā "iekšējai lietošanai vai ierobežotas pieejamības", Saeimai un sabiedrībai tiek piedāvāta tikai virspusēja informatīva līmeņa informācija. Šādā informācijas vakuumā nav brīnums, ka brīdinājuma signāli nav laicīgi pamanāmi un neseko savlaicīga rīcība. Problēma gan nav tikai caurskatāmības trūkumā. Tā ir arī tajā, ka valstij pašai bieži nav pietiekamas iekšējās kapacitātes noturēt sistēmu, definēt prasības, pārbaudīt specifikācijas un ilgtermiņā kontrolēt piegādātājus. Tad sanāk, ka valsts formāli pasūta, bet saturiski projektu arvien vairāk nosaka ārējie spēlētāji.

Lai definētu rīcību šo situāciju un risināmās problēmas ir vērts sadalīt četros atsevišķos, bet savstarpēji saistītos virzienos: **1) 2026. gada vēlēšanu nodrošināšana, 2) valsts digitālo**

risinājumu arhitektūra un pārvaldība, 3) izmeklēšana un atbildība, 4) slepenības laušana. Tikai kopā tie veido jēgpilnu atbildi uz notikušo.

Pirms izvēršam četrus Latvijas rīcības virzienu, īss ieskats Latvijas publisko IT iepirkumu risku hronoloģijā un Dānijas, Igaunijas, Somijas, Zviedrijas un Itālijas pieredzēs.

1. Latvijas publisko IT iepirkumu risku hronoloģija

Latvijas publisko IT iepirkumu risku hronoloģija – skaidri parāda, ka problēmas nav pēkšņas, tās ir uzkrājušās ilgstoši un ilgstoši ir ignorēta riska signālu ķēde. Tieši tāpēc šodienas krīze nav tikai atsevišķu amatpersonu vai viena konkursa stāsts, bet arī valsts nespēja gadiem apkopot, salīdzināt un politiski izsvērt atkārtotus brīdinājumus par publiskajiem IT projektiem.

Gads / periods	Riska signāls	Reakcija
2009	Valsts kontrole konstatē pārkāpumus LVRTC darbībā, kas rāda agrīnas bažas par pārvaldību valsts komunikāciju infrastruktūrā.[16]	Publiska revīzijas ietekme, bet bez redzamas visaptverošas IT pārvaldības reformas.[16]
2010	Revīzijā par "E-pārvaldes portfeli" secināts, ka projekts nav īstenots mērķtiecīgi un efektīvi un daļa līdzekļu izlietota nelietderīgi.[10]	Revīzijas secinājumi iesniegti valdībai un Saeimai, taču vēlāk līdzīgas problēmas atkārtojas citos projektos.[10][17]
2015–2018	E-veselības un veselības informācijas sistēmu revīzijās konstatēta fragmentēta vadība, nepietiekama uzraudzība un neizpildīti mērķi.[31]	Izteikti ieteikumi un veikti uzlabojumi atsevišķās jomās, taču būtiska daļa mērķu netika sasniegta arī vēlāk.[13][14]
2015–2016	Revīzijā par valsts pārvaldes uzkrātās informācijas izmantošanu uzsvērta vāja sadarbspēja un koordinācija starp iestādēm.[11]	Strukturāls brīdinājums par pārvaldības modeli, ne tikai atsevišķu projektu problēmām.[11]
2016–2020	Platjoslas projektā konstatēts, ka ieguldīti vairāk nekā 60 miljoni eiro, bet "pēdējā jūdze" līdz lietotājiem nav nodrošināta.[2][18]	Kritika par investīciju lietderību; vēlāk apturēti atsevišķi ES maksājumi un sākta policijas pārbaude.[2][12]
2020–2023	IR "E-neveiksmes" apvieno E-lietas, E-veselības un citu projektu problēmas: sadrumstalotība, kompetenču trūkums, neskaidra pārvaldība.[1]	Turpināti uzlabojumu plāni, bet neparādās pilnīgs valdības mēroga pārvaldības pārbūves modelis.[1]
2021–2024	OECD un ES materiāli uzsver skaidrāku institucionālo lomu, koordinācijas un iepirkumu kapacitātes nepieciešamību Latvijā.[3][5][6]	Starptautisks reformu pamatojums, bet publiskie rezultāti praksē joprojām ierobežoti.[3][5][6]

2025–2026	EPPO un Latvijas iestādes sāk plaša mēroga IT iepirkumu kriminālprocesu par vismaz sešiem ES fondu projektiem vismaz 1,5 miljonu eiro apmērā.[7][8]	Aizturētas 21 personas, sākti auditi, atstādinātas amatpersonas, iespējami jauni kriminālprocesi citās iestādēs.[7][8]

2. Dānijas SKAT: no "veiksmes stāsta" līdz institucionālam bankrotam

Dānijas SKAT tika veidots kā moderns, centralizēts nodokļu dienests, apvienojot iepriekšējos struktūras līmeņus vienā lielā iestādē. Gadu gaitā tas kļuva par milzīgu, sarežģītu "superaģentūru", kas apstrādāja teju visus nodokļu un muitas procesus vienuviet. Ideja – efektivitāte un vienots serviss – uz papīra izskatījās pārliecinoši. [37][34][32]

Taču vairāk nekā desmit gadu garumā uzkrājās problēmas: nesakārtota nodokļu parādu uzskaite, nesekmīga parādu piedziņa, nekvalitatīvas IT sistēmas un nepilnības datu kvalitātē. Visbeidzot, atklājās milzīgs starptautisks nodokļu krāpšanas skandāls ar dividenžu nodokļa atmaksām, kurā Dānijas nodokļu administrācija krāpniekiem samaksāja apmēram 12 miljardus DKK (vairāk kā 1,5 miljardi EUR), balstoties uz trausliem un vājiem kontroles mehānismiem. [40][24][34][32]

Īpaši zīmīgs ir fakts, ka arī vēlākās tiesvedībās britu tiesa kritizēja Dānijas SKAT sistēmu kā "tik vāju, ka to gandrīz nevarētu saukt par sistēmu vispār", uzsverot, ka procedūras bijušas "gandrīz neeksistējošas". Brīdī, kad kļuva skaidrs, ka vairs nevar runāt par "atsevišķiem gadījumiem", bet gan par iestādes nespēju kontrolēt procesus kopumā, politiskā reakcija bija neizbēgami radikāla. [35][12][40][32]

2017. gadā Dānijas valdība pieņēma lēmumu SKAT kā institūciju slēgt. Nevis "reformēt", bet tieši slēgt un tās vietā izveidot jaunu nodokļu administrācijas arhitektūru ar vairākām specializētām aģentūrām, atsevišķu vadību un pārdalītām funkcijām. Tā bija skaidra atzīšana – vecā iestāde vairs nav reformējama bez pārstartēšanas. [34][35][37][32]

3. Kāpēc dāņi nesamierinājās ar "kosmētisko remontu"

Kas Dānijas piemērā ir īpaši svarīgi Latvijai?

Pirmkārt, SKAT problēmas nebija tikai par nepareiziem IT iepirkumiem vai nepietiekamu kontroli. Būtiska loma bija ilgstošai politiskai izvēlei taupīt uz nodokļu administrācijas cilvēkkapitāla rēķina, masveidā samazinot darbinieku skaitu un vienlaikus uzticot vienai iestādei aizvien sarežģītākus uzdevumus. [35][34][32]

Otrkārt, centralizācija bez pietiekamas specializācijas un iekšējās kontroles padarīja SKAT par vienu lielu "kļūmes punktu". Ja kļūdījās sistēma – kļūdījās viss. Ja kādā posmā bija caurums kontroles mehānismos, tas skāra milzīgu nodokļu maksātāju loku. [13][35][32]

Treškārt, politiskā atbildība. Brīdī, kad sabiedrība saprata, ka zaudējumi ir mērāmi miljardos un iestāde gadiem nav bijusi spējīga to novērst, tikai vadītāja nomaiņa vairs nebūtu uztverama kā nopietna reakcija. Institucionāls bankrots prasīja drosmi pietiekami ātri atzīt šo faktu un piedāvāt tiešām nopietnu institucionālu pārmaiņu risinājumu – SKAT likvidāciju un jauna modeļa izveidi. [40][35][32]

Latvijas mācība no šīs pieredzes būtu, ka Latvijai šajā situācijā nav tikai divas izvēles - automātiski "decentralizēt visu" vai, tieši otrādi, "centralizēt vēl vairāk". Galvenais jautājums ir par koordināciju un atbildību. Kritiskās valsts IT funkcijas nevar būt sadrumstalotas tā, ka katrs redz tikai savu daļu, bet nevar arī tikt saliktas vienā institūcijā bez pietiekamas specializācijas, neatkarīgas kontroles un skaidras politiskas atbildības. Risinājums ir nevis mehāniska centralizācija, bet skaidri sadalītas funkcijas, valdības līmenī noteikts koordinācijas mehānisms starp pasūtītāju, uzraugu, tehnisko arhitektūru un ieviešanu, kā arī viens redzams politiski atbildīgais par gala rezultātu.

Papildus Dānijas pieredzei, Igaunijas 2019. gada Valsts kontroles izvērtējums par neveiksmīgiem IT projektiem rāda, ka arī digitalizācijas veiksmes stāsta valstī var izgāzties projekti neskaidru lomu, pārlieku optimistiskas plānošanas un sadarbības trūkuma dēļ. [20] Somijas piemērs savukārt parāda, ka ar formālu publisko IT projektu un iepirkumu priekšizvērtēšanas mehānismu vien nepietiek risku vadībai, ja tas praksē netiek konsekventi izmantots. [23] Savukārt Apvienotās Karalistes lielo projektu luksofora sistēma piedāvā noderīgu agrīnā brīdinājuma modeli, kas ļauj publiski agregēt un salīdzināt riskus starp projektiem. [9, 15, 25]

4. Slepenības cena: kā klusums baro korupciju un neprofesionalitāti

Ilgstoša slepenības pieeja ir kopīga iezīme daudziem šāda veida skandāliem. Tā nav tikai drošības prasību blakne – tā kļūst par korupcijas un neprofesionalitātes infrastruktūru. [33][32]

Slepenība kā korupcijas un "iekšējo karjeru" aizsargslānis

Ja lielie IT līgumi, to grozījumi un tehniskie risinājumi ir pieejami tikai šauram cilvēku lokam, tad šis loks kontrolē milzīgus resursus ar minimālu ārējo pārbaudi. Slepenību lielākoties nosaka pašas iestādes, kuras sevi tādā veidā liedz uzraudzīt - šajā gadījumā VDAA un VARAM un abas tā var paslēpt savu neizdarību un vai bezdarbību. Itālijas SOGEI ((Società Generale d'Informatica S.p.A.) ir Itālijas Ekonomikas un finanšu ministrijai piederošs IT uzņēmums, kas nodrošina valsts publiskās pārvaldes digitalizāciju) gadījumā izmeklētāji tieši pēta saiknes starp valsts IT uzņēmumu un piegādātājiem, tajā

skaitā iespējamu informācijas noplūdi par lēmumiem ministriju iekšējās sanāksmēs, kas varētu būt izmantota komerciāla labuma gūšanai (publiski ziņojumi par apjomīgiem arestiem 2024. gadā un 2026. gadā). [17] [18] Šādā vidē karjeras un līgumi veidojas nevis caur atklātu konkurenci un profesionāliem kritērijiem, bet gan "uzticamu cilvēku" tīklojumu. Slepenība te nav blakusefekts, bet funkcionāls priekšnoteikums – bez tās šādas shēmas vienkārši nebūtu iespējamas. [36][38][32]

Slepenība kā valsts ienaidnieks

Zviedrijas Transporta aģentūras skandāls ap tās pārziņā esošo sensitīvo datu nonākšanu nepiederošu cilvēku rokās ir klasisks piemērs tam, kā, apejot publisku un starpinstitucionālu diskusiju, tiek pieņemti lēmumi, kas vēlāk izrādās bīstami valsts drošībai. Lēmums ārpakalpojumā nodot kritiskās datubāzes uzturēšanu, neievērojot drošības likumus un drošības dienestu iebildumus, tika pieņemts šaurā lokā. Rezultātā sensitīva informācija par aizsargātām personām un operatīvo dienestu darbiniekiem nonāca pie cilvēkiem bez atbilstošas pielaides. [39][32] Divus gadus vēlāk 2017. gadā šie notikumi izraisīja apjomīgu valdības krīzi Zviedrijā. [19] Ja projekti un līgumi tiek paslēpti aiz "komercnoslēpuma", "ierobežotas pieejamības" un pārspīlētas drošības retorikas, kvalitatīvi ārējie viedokļi – no akadēmiskās vides, pilsoniskās sabiedrības vai neatkarīgiem IT ekspertiem – nepienāk. Iekšējiem profesionāļiem ir grūti cīnīties ar politiskajiem vai ekonomiskajiem motīviem, ja viņiem nav sabiedrotā "ārpusē". [32]

Slepenība kā politiskās nezināšanas mehānisms

Slepenība ļauj politiskajam līmenim ilgi turēties pie frāzes "mēs nezinājām". Ja ministram un Saeimai tiek piegādāta tikai rūpīgi atlasīta, pozitīvi tonēta informācija par projektu gaitu, tad politiskas sekas par bezdarbību iestājas tikai tad, kad skandāls jau ir publisks. Zviedrijas gadījumā ministra atkāpšanās un uzticības krīze nāca tikai pēc tam, kad datu noplūde bija kļuvusi par publiski zināmu faktu. [39] [32]

Rezultātā nevienai politiskai partijai nav īsta stimula savlaicīgi rakties cauri IT projektiem – daudz izdevīgāk ir gaidīt krīzi un tad skaļi pieprasīt "izmeklēšanu" un "sodus". Ilgstoša slepenība padara prevenciju politiski neizdevīgu un atlīdzina tikai reakciju brīdī, kad jau ir par vēlu. [32]

5. Četri Latvijas rīcības virzieni: 2026. gada vēlēšanas, valsts digitālo risinājumu arhitektūra un pārvaldība, izmeklēšana, slepenības laušana

Šo ārvalstu pieredzi var pārnest uz Latviju, sadalot nepieciešamo rīcību četros atsevišķos, bet savstarpēji saistītos virzienos.

5.1. 2026. gada Saeimas vēlēšanu nodrošināšana: jāatsien no skandāla

Pirmais un neatliekamais jautājums ir, kā nodrošināt godīgas un drošas vēlēšanas, neievelkot tās IT iepirkumu skandālā. Vēlēšanās nedrīkst iestāties tehnisks vai uzticības vakuums tikai tāpēc, ka centrālā IT aģentūra un tās darbinieki ir kompromitēti. [33] Saeima 26. martā spēra pirmo soli, pieņemot grozījumus likumā, nosakot manuālu balsu skaitīšanu 2026. gada Saeimas vēlēšanās. Skandāla pamatā ir pārvaldības un iepirkumu problēmas, nevis vēlēšanas pašas par sevi. Tāpēc sabiedrībai šis nodalījums jānotur ļoti skaidri, citādi ēna pār IT pārvaldību tiek uzmesta pašām vēlēšanām. Publiskajā komunikācijā šobrīd ir svarīgi norādīt uz pasākumiem, kas tiek veikti lai būtu garantija, ka vēlēšanu godīgums nav apdraudēts. **Mums visiem svarīgi zināt, ka vēlētāju balsis tiks godīgi saskaitītas un 2026. gada 3. oktobrī jānāk uz vēlēšanām.**

Izmeklēšana, tiesas procesi un politiskās batālijas ap šiem skandāliem turpināsies mēnešiem un gadiem. Vēlēšanu cikli tam nepielāgojas. Tāpēc Centrālās vēlēšanu komisijas atbildība ir šobrīd skaidri un nepārprotami nodalīt vēlēšanu tehnisko un institucionālo nodrošinājumu, tāpat arī iesaistītos darbiniekus no sasaistes ar šīs krīzes epicentru.

5.2. valsts digitālo risinājumu arhitektūra un pārvaldība: kosmētiskas pārmaiņas vairs neder

Otrais jautājums – ko darīt ar informācijas tehnoloģiju sistēmu attīstības organizēšanu Latvijā, ņemot vērā, ka esošā sistēma sevi ir izsmēlusi. Šeit runa nav par kosmētisku remontu, bet, visticamāk, par esošās aģentūras demontāžu un arī atbildīgās ministrijas pārvērtēšanu. [33] Jautājums nav tikai par to, vai viena konkrēta aģentūra vai ministrija ir ‘salabojama’, bet par to, kā organizēt kritiski svarīgu valsts digitālo sistēmu pārvaldību tā, lai būtu skaidras lomas, profesionāla kontrole un redzama politiskā atbildība.

Papildus tam jāatzīst vēl viena problēma - Latvijas IT pārvaldībā sistēma bieži ir pārāk fragmentēta. Pasūtītāji, uzraugi, tehniskie cilvēki, politiskais līmenis un piegādātāji strādā katrs pēc savas izpratnes, bez skaidri noteikta koordinācijas mehānisma starp pasūtītāju, uzraudzību, tehnisko arhitektūru un ieviešanu. Rezultātā sistēma formāli kustas, bet faktiski nesarunājas. Katrs redz savu daļu, bet neviens līdz galam neuzņemas kopējo risku un gala rezultātu. To vēl pastiprina profesionālā kodola trūkums pašā valsts pārvaldē. Ja iestādēs ir augsta darbinieku mainība un vāja institucionālā atmiņa, tad specifikācijas top formāli, bez pietiekamas satura pārvaldības, bet ārējie konsultanti un piegādātāji sāk aizstāt iekšējās kompetences. Rezultātā valsts vairs nav patstāvīgs un kritisks pasūtītājs, bet kļūst atkarīga no tiem, kuriem pašiem pēc tam jāizpilda un jāuzrauga risinājums.

Dānijas SKAT stāsts parāda vienu iespējamo ceļu: kad kļuva skaidrs, ka “superiestāde” nespēj vairs nodrošināt kontroli un kvalitāti, valdība pieņēma lēmumu to slēgt un sadalīt vairākās specializētās aģentūrās ar skaidrām atbildībām. Zviedrijā pēc Transporta aģentūras IT skandāla netika likvidēta

pati iestāde, bet tika būtiski pārveidota kopējā drošības un ārpakalpojumu regulēšana visā valsts pārvaldē. Itālijā šobrīd notiek plaša izmeklēšana par valsts IT iepirkumiem un centrālā IT uzņēmuma SOGEI lomu, bet lēmumi par arhitektūru vēl priekšā. [38][36][37][39][34][35][32][33]

Svarīga ir arī pati pieeja IT sistēmu veidošanai: valsts pārvaldē pārāk bieži mēģina vienā piegājienā uzbūvēt lielas, smagas sistēmas, nevis iet caur mazākiem, modulāriem un ātrāk testējamiem risinājumiem. Tas padara kļūdas dārgākas, riskus lielākus un atbildību vēl grūtāk noturamu.

Latvijai tas nozīmē: ir jāizvēlas ne tikai, vai esošā centrālā IT aģentūra ir salabojama, vai arī jārunā par pilnīgi jaunu arhitektūru un arī kādā veidā sistēma tiktu pārvaldīta. Galvenais jautājums nav tikai, ko likvidēt vai sadalīt, bet kā nodrošināt skaidru funkciju sadalījumu starp pasūtītāju, uzraudzību, tehnisko arhitektūru un ieviešanu, profesionālu kontroli un redzamu politisko atbildīgo par kritiski svarīgām valsts digitālajām sistēmām. No minēto valstu piemēriem Latvijai izriet vēl viens praktisks secinājums: nepietiek tikai ar pēcskandāla izmeklēšanu un auditiem. Digitālajām reformām nepietiek ar īsu politisko impulsu - tām vajag ilgstošu politisko atbildīgo, kas spēj novadīt reformu līdz konkrētam plānotajām rezultātam. Nepieciešams pastāvīgs valdības mēroga mehānisms, kas laikus identificē augsta riska IT projektus, ļauj tos salīdzināt un piespiež politisko līmeni reaģēt, pirms problēmas pāraug kriminālprocesos vai pilnā institucionālā krīzē.

5.3. Izmeklēšana un atbildība: jāļauj strādāt, bet reformu nedrīkst atlikt

Trešais virziens ir izmeklēšana un atbildības iestāšanās. Mums ir jāpaļaujas, ka tiesībsargājošās iestādes spēs objektīvi, vispusīgi un pietiekami ātri izmeklēt šos nodarījumus un saukt pie atbildības negodprātīgās amatpersonas, uzņēmējus un iesaistītos darbiniekus abās pusēs. LTV 1 intervijā 31.03.2026. Eiropas prokurors Gatis Doniks norādīja, ka izmeklēšana sākta gandrīz pirms trim gadiem, sākotnēji balstoties kriminālizlūkošanā, informācijas ievākšanā un grupas dalībnieku lomu noskaidrošanā; kriminālprocess ierosināts tikai pēc ilgstoša analītiskā darba. Doniks norādīja, ka šobrīd ir aizdomas par iespējamu krāpšanu sešos Eiropas fondu projektos vismaz 1,5 miljonu eiro apmērā, bet izmeklēšana var paplašināties arī uz citiem iepirkumiem un citām iestādēm. [22]

No EPPO, Latvijas prokuratūras un LSM materiāliem izriet šāda iespējamā shēma: [7][8]

1. Tiek identificēti ES fondu vai valsts finansēti IT projekti ar lielu līgumu vērtību un sarežģītu tehnisko saturu. [7][8]
2. Organizēta grupa ar skaidri sadalītām lomām ietekmē iepirkuma vidi tā, lai konkrēts uzņēmums vai uzņēmumu loks iegūtu uzdevumu. [7]
3. Grupai pietuvināti cilvēki valsts iestādēs tiek nozīmēti amatos, kas saistīti ar iepirkumu organizēšanu, uzraudzību vai piekļuvi sensitīvai informācijai.
4. Līgumi tiek nelikumīgi nodrošināti ar amatpersonu palīdzību, radot konkurences imitāciju vai piešķirot priekšrocības iepriekš izvēlētiem uzņēmumiem. [7][8]

5. Pēc projektu uzdevumu piešķiršanas nelikumīgi iegūtā peļņa tiek sadalīta starp līdzdalībniekiem. [7][8]
6. Izmeklēšanas gaitā iegūtie datu nesēji un terabaitos mērāmi dati var atklāt papildu projektus, iesaistītās personas un citus kriminālprocesus.

EPPO un OLAF materiāli rāda, ka iepirkumu manipulācija, fiktīva konkurence, amatpersonu un uzņēmēju sadarbība, interešu konflikti un uzpūstas izmaksas ir atkārtots modelis ES fondu lietās. [26][27][28] Eiropas Parlamenta pētījumā par korupciju publiskajā iepirkumā uzsvērts, ka īpaši ievainojami ir iepirkuma sākumposmi – vajadzību definēšana, tehnisko specifikāciju rakstīšana un atlases kritēriju noteikšana. [29]

Eucrim analīze par augsta riska korupcijas jomām ES publisko iepirkumu izceļ kā vienu no sešiem īpaša riska sektoriem, uzsverot tieši piedāvājumu saskaņošanu, uzvarētāja iepriekšēju noteikšanu un interešu konfliktus (Eucrim ir tiešsaistes platforma ES krimināltiesību jautājumos, to līdzfinansē Eiropas Komisija un Eiropas Birojs krāpšanas apkarošanai (OLAF)). [30] Tādēļ Latvijas IT iepirkumu lietu var pamatoti skatīt kā daļu no plašāka ES tipa riska modeļa, nevis kā unikālu vietējo anomāliju. [30][26][29][28]

Lai gan nedēļas laikā publiski jau pieejamas diezgan skaidras situācijas aprises - tomēr ir jābūt godīgiem – šis noteikti nebūs ātrs izmeklēšanas process. Lieli IT iepirkumi, sarežģītas līgumu ķēdes, starptautiski elementi, gadiem ilgas prakses – to visu nav iespējams atšķetināt dažu mēnešu laikā, to parāda gan Dānijas SKAT tiesvedības, gan Itālijas plašā izmeklēšana IT jomā. Tieši tāpēc strukturālās reformas nedrīkst “iesaldēt”, gaidot pēdējo tiesas spriedumu. Institucionālās slimības pazīmes – pārlieka koncentrācija, vāja kontrole, slepenības kultūra – ir redzamas jau tagad un ir pietiekams pamats rīkoties politiskā līmenī. [24][33][38][40]

Latvijas gadījums rāda pāreju no ilgstoši publiski redzamiem pārvaldības brīdinājumiem uz iespējamu krimināli organizētu shēmu ar ES fondu līdzekļu izkrāpšanas pazīmēm. [1][2][7][8] Centrālais secinājums nav tikai tas, ka bija “slikti IT projekti”, bet gan tas, ka vāja pārvaldība, zema caurspīdība un koncentrēta ietekme uz iepirkumiem rada vidi, kurā no sistēmiskas nekompetences var izaugt sistēmiska korupcija. [5][6][30][29]

No citu valstu pieredzes izriet trīs praktiskas mācības. Pirmkārt, agrīniem riska signāliem jābūt publiski apkopotiem un salīdzināmiem starp projektiem, kā to dara Lielbritānijas lielo projektu vērtēšanas sistēma. [9][15] Otrkārt, formāla kontrole bez reālas izpildes nestrādā, kā rāda Somijas piemērs. [23] Treškārt, digitālās valsts reputācija pati par sevi nepasargā no ievainojamiem projektiem vai tādiem, kas izgāžas, kā rāda Igaunijas un Zviedrijas gadījumi. [21][20][22]

Vienlaikus ir svarīgi skaidri nošķirt krimināltatbildību, administratīvu vai disciplināru atbildību un politisko atbildību. Kriminālprocess var ilgt gadiem, taču politiskais jautājums rodas jau tagad: kāpēc

šāda vide vispār tika pieļauta, kāpēc riski netika pamanīti agrāk un kāpēc kritiskas valsts sistēmas kvalitāte netika nodrošināta pirms izgāšanās, nevis tikai pēc tās. Ja šo nošķirumu nesaglabā, politiskā atbildība riskē pazust procesuālajā valodā. Papildu risks ir arī tas, ka sabiedrības un mediju spiediens šādos gadījumos parasti ir intensīvs, bet īslaicīgs. Ja tas netiek pārvērsts noturīgā politiskā pieprasījumā pēc strukturālām reformām, sistēma pēc publiskā skandāla norimšanas lielā mērā atgriežas iepriekšējā stāvoklī.

5.4. Slepenības laušana: problēmas sakne, nevis detaļa

Ceturtā, bet patiesībā šķērsgriezumā vissvarīgākā tēma ir slepenības plīvurs. Mums ir jāspēj atzīt, ka tieši ilgstoša slepenības kultūra ir viena no šodienas problēmu saknēm. [33] Šeit runa nav tikai par atsevišķu dokumentu statusu. Ilgstoša necaurskatāmība pati par sevi kļūst par sistēmas uzturēšanas mehānismu. Ja līgumi, grozījumi, riska ziņojumi, testēšanas rezultāti un iekšējie brīdinājumi paliek ārpus nopietnas ārējas pārbaudes, politiskajai sistēmai kļūst ļoti ērti dzīvot ar sajūtu, ka problēmu nav. Tad nezināšana kļūst ērta, bet prevencija politiski neizdevīga.

Šobrīd jebkurā valsts iestādē bieži vien ir vieglāk dokumentu pasludināt par "ierobežotas pieejamības", nekā to neizdarīt. Tas attiecas uz iepirkumu dokumentāciju, iekšējiem auditiem un riska ziņojumiem. Rezultāts – neliels iekšējais loks kontrolē milzīgus līdzekļus ar minimālu ārējo pārbaudi. Tieši šādos apstākļos var izveidoties slēgti tīklojumi un interešu grupas, kuras gadiem darbojas nepamanītas. [33]

Papildu problēma ir tā, ka Latvijā trūkst arī sistemātisku ex post izvērtējumu jau ieviestām digitālajām sistēmām. Rezultātā valsts ne tikai slikti uzbūvē jaunas sistēmas, bet arī pārāk reti pārskata, vai iepriekšējie risinājumi vispār strādā, kādi riski tajos uzkrājušies un kur nepieciešama savlaicīga pārbūve.

Lai jebkura strukturāla reforma būtu jēgpilna, slepenības prakses ir jāmaina. Lielie IT iepirkumi un to grozījumi jāpadara pēc iespējas publiski; iekšējo auditu rezultāti regulāri jāapspriež Saeimas komisijās ar skaidri nodalītu publisko un konfidenciālo daļu; un ierobežotas pieejamības statuss jāpamato ar valsts drošību, nevis reputācijas bažām. Pretējā gadījumā mēs vienkārši nomainīsim nosaukumus un struktūras, bet atstāsim neskartu to pašu slepenību, kurā šodienas problēmas varēja izaugt. [32][33]

6. Citas mācības no Eiropas IT skandāliem

Dānijas piemērs nav vienīgais, kas Latvijai būtu jāņem vērā.

Igaunijas Valsts kontrole 2019. gadā izvērtēja deviņus valsts IT projektus un četrus no tiem atzina par neveiksmīgiem, minot pārlieku optimistisku plānošanu, neskaidras lomas, lietotāju vajadzību

ignorēšanu, prasību maiņu un sadarbības problēmas. [20] Tas nav identisks kriminālprocess, bet tas ir ļoti līdzīgs sistēmisku pārvaldības vājumu piemērs. [20]

Zviedrijas Transporta aģentūras IT skandāls parādīja, ka ārpakalpojumu, drošības kontroles un politiskās atbildības sabrukums var kļūt par valsts līmeņa krīzi, ja sensitīvi dati nonāk nepietiekami kontrolētā vidē nevis un rada tiešus draudus demokrātijas pamatiem. [9][5][1][21][22] Šis gadījums ir būtisks Latvijai, jo parāda, ka publiskā IT iepirkuma problēmas nav tikai izmaksu vai termiņu jautājums, bet arī drošības un demokrātiskās uzticamības jautājums. [21][22]

Somijas Valsts kontrole secināja, ka formāli pastāvošs ICT līgumu priekšizvērtēšanas mehānisms praksē nav devis vajadzīgo sadarbspējas efektu, jo to nepietiekami izmantojušas pašas iestādes. [23] Šis piemērs rāda, ka nepietiek ar normatīvu prasību vien; nepieciešama institucionāli spēcīga un reāli piemērota "vārtsarga" funkcija. [23]

Savukārt Itālijas gadījums ar SOGEI – valsts ekonomikas un finanšu ministrijas IT uzņēmumu, kas nonācis plašas korupcijas un naudas atmazgāšanas izmeklēšanas centrā – izgaismo riskus, kas rodas, ja centrāla IT institūcija darbojas kā saikne starp lēmumu pieņēmējiem un piegādātājiem bez pietiekamiem caurspīdības un kontroles mehānismiem. Nupat 2026. gadā veiktās kratīšanas Itālijā vairākos valsts uzņēmumos un institūcijās (tai skaitā publiskā mākoņa infrastruktūras pārvaldītājā) norāda, ka iespējamās shēmas var aptvert plašu valsts sektora daļu. [6][8][1]

Lielbritānijā joprojām pastāv valdības lielo projektu "luksofora" sistēma, kas parāda novērtējumu par projekta īstenošanas iespējamību apstiprinātajā budžetā, laikā un plānotajā kvalitātē – Delivery Confidence Assessment ar Red, Amber un Green vērtējumiem, ko 2024.–2025. gadā turpina uzturēt jau jaunā institūcija NISTA. [24][9][15] Agrākie starpvērtējumi ir atcelti, bet sistēma nav pazudusi; tā joprojām kalpo kā publisks agrīnā brīdinājuma mehānisms par projektiem ar augstu neveiksmes risku. [9][25]

Šie stāsti kopā nozīmē divas lietas. Pirmkārt, IT iepirkumi ir politikas un drošības jautājums, nevis "tehniķu iekšējā lieta". Otrkārt, jebkura centrāla IT aģentūra vai uzņēmums jāuztver kā sistēmisks risks – un jāveido tā, lai tas nekad nekļūtu par vienu neaizvietojamu, nekontrolējamu mezglu. [38] [36][32]

7. Ko vajadzētu darīt: konkrēti virzieni (ar slepenības laušanu kā centrālo elementu)

Kad runājam par reformām, slepenības laušana nav "skaists, bet otršķirīgs" jautājums – tas ir centrālais nosacījums, lai jebkura struktūras reforma vispār strādātu. [32][33]

- **Stratēģiska politiskā atbildība**: jānosaka konkrēts ministrs un ministrijas līmenis, kas saturiski atbild par digitālās pārvaldes integritāti, kritisko sistēmu noturību un pārresoru koordināciju. Tas nozīmē pienākumu regulāri skaidroties Saeimai un sabiedrībai par kritiski svarīgu sistēmu stāvokli, ne tikai reaģēt uz skandāliem. [32] IT projektu izgāšanās gadījumos nedrīkst aizstāt politisko atbildību ar procesuālu valodu par izmeklēšanām, auditiem un statusiem (VDAA 01.04.2026. publiski izplatītais aicinājums veikt neatkarīgu aģentūras iepirkumu procesa auditu ir tieši šāds solis – protams nepieciešams, bet nepietiekams šajā situācijā).
- **Institucionālā arhitektūra un koordinācija**: jāizvērtē, kuras funkcijas patiešām jāglabā vienā digitālās attīstības aģentūrā un kuras būtu racionāli nodalīt atsevišķās vienībās ar skaidrām atbildībām un atšķirīgu uzraudzību – līdzīgi kā Dānija sadalīja SKAT vairākās specializētās aģentūrās. [37][34][35][32][33] Risinājums nav mehāniska centralizācija vai decentralizācija, bet skaidri sadalītas funkcijas starp pasūtītāju, uzraudzību, tehnisko arhitektūru un ieviešanu, valdības līmenī noteikts koordinācijas mehānisms starp šīm funkcijām un viens redzams politiski atbildīgais par gala rezultātu, kā arī regulārs un atklāts monitorings.
- **Valsts kā pasūtītāja stiprināšana:** kritiski svarīgās valsts IT sistēmās valstij pašai jāspēj noteikt vajadzību, definēt prasības, uzturēt tehnisko arhitektūru, neatkarīgi pārbaudīt risinājumu kvalitāti un profesionāli uzraudzīt piegādātāju darbu. Tas nozīmē stiprināt iekšējo IT, arhitektūras, analītisko un projektu vadības kapacitāti valsts pusē, kā arī mazināt pārmērīgu atkarību no ārējiem konsultantiem, lai valsts nevis tikai formāli administrētu iepirkumu, bet būtu reāls un kritisks pasūtītājs visā sistēmas dzīves ciklā. Tas līdz šim nav izdevies.
- **Caurspīdīga informācija par projektiem un slepenības ierobežošana**: lielie IT iepirkumi un to grozījumi, testēšanas rezultāti un veiktie auditi jāpublicē tādā detalizācijas līmenī, lai tos varētu reāli izvērtēt nozares eksperti un pilsoniskās sabiedrības organizācijas, izslēdzot tikai patiesi sensitīvus drošības elementus. [32][33] Ierobežotas pieejamības statuss nedrīkst tikt izmantots reputācijas aizsardzībai vai institucionālajai pašsaglabāšanai.
- **Iekšējā un ārējā kontrole**: iekšējo auditu rezultāti, riska ziņojumi un būtiskāko sistēmu ex post izvērtējumi regulāri jāprezentē Saeimas komisijām, nodalot publisko daļu no patiesi konfidenciālās daļas, kur to patiešām prasa valsts drošība, nevis reputācijas bažas. [32][33] Valstij jāveido regulārs mehānisms, kas liek pārskatīt ne tikai jaunus projektus, bet arī jau ieviestu digitālo sistēmu darbību, uzkrātos riskus un nepieciešamās pārbūves. Iespējams jāapsver Lielbritānijas publiskā agrīnā brīdinājuma mehānisma analogs par projektiem ar augstu neveiksmes risku (attiecas uz visiem lielajiem projektiem).
- **Piegādātāju un saistīto personu tīklu analīze:** KNAB un IUB būtu jāveic sistemātiska lielo IT iepirkumu piegādātāju, konsultantu, ekspertu un saistīto personu loku analīze vairāku gadu

griezumā, jo tieši atkārtojošos variantos visbiežāk veidojas riski, ko atsevišķa iepirkuma ietvaros nevar pilnībā ieraudzīt. Jānodrošina pilna publisko iepirkumu līgumu izpildes informācijas atklātība.

- **Personāls un rotācija**: jāpārskata Latvijas civildienesta un valsts IT projektu cilvēkresursu politika, lai vadības līmenī gan ministrijās, gan iestādēs un iepirkumu funkcijā nevarētu izveidoties situācija, kur vieni un tie paši cilvēku gadu desmitiem saglabā tās pašās pozīcijās un tos pašus neformālos tīklus. [32] Vienlaikus rotācija nedrīkst nozīmēt profesionālās atmiņas zaudēšanu. Tāpēc nepieciešama gan pārdomāta rotācija augsta riska amatos, gan stiprāks profesionālais kodols valsts pusē.

Lai nebūtu jāslēdz iestādes pēc gadiem ilgas degradācijas, problemātiskajām institūcijām regulāri jāsatiekas ar sabiedrības un parlamenta jautājumiem. Ja šis kontakts tiek pārrauts, slepenība lēnām, bet neizbēgami pārtop par korupcijas un neprofesionalitātes infrastruktūru – līdz brīdim, kad vienīgais godīgais risinājums ir pilnīgs "restart". [32][33]

Ja Latvija kā risinājumu tomēr izvēlēsies tikai iestādes vadītāju nomaiņu, jaunu nosaukumu vai vēl vienu "stingrākas kontroles" un "papildus auditu" solījumu, bet neatrisinās valsts kā pasūtītāja vājumu, sistēmas fragmentāciju, slepenības kultūru un neskaidro politisko atbildību, tad pat jebkāda jaunā struktūra, ja tāda tiks veidota, ļoti ātri sāks atkārtot vecās sistēmas kļūdas.

Avotu saraksts

1. Civil Service World par red-rated projektiem – https://www.civilserviceworld.com/professions/article/government-major-projects-portfolio-redrated-projects-now-worth-198bn [25]
2. EPPO, “Latvia: 20 suspects detained over €1.5 million IT procurement fraud” – https://www.eppo.europa.eu/en/media/news/latvia-20-suspects-detained-over-eu15-million-it-procurement-fraud [7]
3. EPPO, “Latvia: Three convicted in EPPO investigation into procurement fraud involving agricultural funds” – https://www.eppo.europa.eu/en/media/news/latvia-three-convicted-eppo-investigation-procurement-fraud-involving-agricultural-fund [27]
4. European Commission, “Latvia – public procurement capacity profile” – https://ec.europa.eu/regional_policy/sources/policy/how/improving-investment/public-procurement/study/country_profile/lv.pdf [5]
5. European Parliament study, “Political and other forms of corruption in the attribution of public procurement contracts” – https://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/490676/IPOL-JOIN_ET(2013)490676_EN.pdf [29]
6. Eucrim, “High-Risk Areas of Corruption in the EU” – https://eucrim.eu/news/high-risk-areas-of-corruption-in-the-eu-in-depth-report-highlights-six-vulnerable-sectors/ [30]
7. Government Major Projects Portfolio – https://www.gov.uk/government/publications/government-major-projects-portfolio [15]
8. Igaunijas Valsts kontroles atreferējums ERR – https://news.err.ee/979157/national-audit-office-fails-four-state-it-projects un pilns ziņojums: Archived Page: Audit reports [20]
9. IR, “E-neveiksmes” – https://ir.lv/rubrika/tema/e-neveiksmes.210043 [1]
10. LRP, “Latvija: Aizdomās par 1,5 miljonu eiro izkrāpšanu IT iepirkumos” – https://www.prokuratura.lv/lv/aktualitates/2026/informacija-par-aktualitatem/latvija-aizdomas-par-15-miljonu-eiro-izkrapsanu-it- [8]
11. LSM, “Pirms aizgāja LVRTC valde, apturēti ES projekta maksājumi; policija sāk pārbaudi” – https://www.lsm.lv/raksts/zinas/latvija/14.04.2019-pirms-aizgaja-lvrtc-valde-aptureti-es-projekta-maksajumi-policija-sak-parbaudi.a315991/ [12]
12. LSM, “Valsts kontrole: Projekts ‘E-pārvaldes portfelis’ nav mērķtiecīgi un…” – https://www.lsm.lv/raksts/dzive--stils/tehnologijas-un-zinatne/valsts-kontrole-projekts-e-parvaldes-portfelis-nav-merktiecigi-un-pamatoti-planots-un-ieviests.a16470/ [10]
13. LSM, “Valsts kontrole konstatē pārkāpumus LVRTC darbībā” – https://www.lsm.lv/raksts/zinas/latvija/valsts-kontrole-konstate-parkapumus-lvrtc-darbiba.a8453/ un https://www.lrvk.gov.lv/lv/revizijas/revizijas/noslegtas-revizijas/vas-latvijas-valsts-radio-un-televizijas-centrs-ienemumu-izlietojuma-likumiba-un-atbilstiba-vas-latvijas-valsts-radio-un-televizijas-centrs-darbibas-merkiem [16]
14. NISTA Annual Report 2024-25 – https://www.gov.uk/government/publications/nista-annual-report-2024-2025/nista-annual-report-2024-25 [9]
15. NRA, “Valsts kontrole atsakās turpmāk kontrolēt e-veselību bezjēdzīguma dēļ” – https://nra.lv/neatkariga/izpete/381219-valsts-kontrole-atsakas-turpmak-kontrolet-e-veselibu-bezjedziguma-del.htm un Valsts kontrole, publiskais gada pārskats un ieteikumu ieviešanas platforma – https://lrvk.gov.lv/lv/ieteikumu-ieviesana/ieteikumu-platforma/ieteikumu-parskats [14]

16. OECD, “Digitalizācija Latvijā / Going Digital in Latvia” – https://www.oecd.org/lv/publications/digitalizacija-latvija_a58d1c1a-lv.html [3]
17. OECD, “Going Digital in Latvia” (EN PDF) – https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/02/going-digital-in-latvia_0cf1d1d6/8eec1828-en.pdf [6]
18. OECD, “Interagency Coordination in Economic Crime Investigations in Latvia” – https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/interagency-coordination-in-economic-crime-investigations-in-latvia_86d9eeda/4e30b5e1-en.pdf [4]
19. OLAF annual findings / fraud and irregularities – https://anti-fraud.ec.europa.eu/media-corner/news/olaf-investigations-find-over-eu12-billion-affected-fraud-and-irregularities-2023-2024-06-17_en [26]
20. OLAF, “Serious irregularities in EU-funded procurement in Poland” – https://anti-fraud.ec.europa.eu/media-corner/news/olaf-completes-investigation-suspected-serious-irregularities-eu-funded-procur-2025-02-17_en [28]
21. Somijas Valsts kontrole, “Interoperability in government ICT contracts” – https://vtv.fi/en/report/interoperability-in-government-ict-contracts/ [23]
22. Sveriges Radio, “Government under fire after Transport Agency data breach” – https://www.sverigesradio.se/artikel/6740394 [21]
23. Valsts kontrole, “Informācijas sistēmas veselības aprūpē” – https://lrvk.gov.lv/lv/revizijas/revizijas/noslegtas-revizijas/informacijas-sistemas-veselibas-aprupe [31]
24. Valsts kontrole, “Vai ieguldījumi elektroniskās sakaru infrastruktūras pieejamības uzlabošanā ir veikti lietderīgi?” – https://lrvk.gov.lv/lv/revizijas/revizijas/noslegtas-revizijas/vai-ieguldijumi-elektroniskas-sakaru-infrastrukturas-pieejamibas-uzlabosana-ir-veikti-lietderigi [2]
25. Valsts kontrole, “Vai valsts pārvalde efektīvi rīkojas ar uzkrāto informāciju?” – https://www.lrvk.gov.lv/lv/getrevisionfile/uploads/reviziju-zinojumi/2016/2.4.1-12_2016/zinojums.pdf [11]
26. Jauns.lv, “Valsts kontrole: e-veselības jomā jānovērš virkne problēmu” – https://jauns.lv/raksts/zinas/255317-valsts-kontrole-e-veselibas-joma-janovers-virkne-problemu un Valsts kontrole, publiskais gada pārskats un ieteikumu ieviešanas platforma – https://lrvk.gov.lv/lv/ieteikumu-ieviesana/ieteikumu-platforma/ieteikumu-parskats [13]
27. https://cphpost.dk/2017-06-13/news/so-long-min-skat-denmark-restructuring-its-tax-authority/ [32]
28. https://gatehouselaw.co.uk/commercial-court-dismisses-in-its-entirety-the-danish-governments-claims-in-skatteforvaltningen-the-danish-customs-and-tax-administration-v-solo-capital-partners-llp-in-special-administrat/ [24]
29. https://iclg.com/news/23133-dreadful-day-in-court-for-the-danish-tax-authority [38]
30. https://jp.reuters.com/article/world/denmark-launches-major-overhaul-of-tax-authority-after-scandals-idUSKBN1941FZ/ [33]
31. https://replay.lsm.lv/lv/skaties/ieraksts/ltv/373857/11-eiropas-prokurors-gatis-doniks [22]
32. https://uk.finance.yahoo.com/news/danish-tax-authority-loses-1-104956187.html [39]
33. https://www.computerweekly.com/news/450423272/Big-data-means-big-risk-Swedish-Transport-Agency-leak-shows [34]
34. https://www.devdiscourse.com/article/politics/3851820-italian-probe-uncovers-public-it-procurement-scandal [36]

35. https://www.gdf.gov.it/it/gdf-comunica/notizie-ed-eventi/comunicati-stampa/anno-2024/ottobre/reati-contro-la-pubblica-amministrazione [17]
36. https://www.judiciary.uk/wp-content/uploads/2025/10/Skatteforvaltningen-Danish-Customs-and-Tax-Administration-v-Solo-Capital-Partners.pdf [40]
37. https://www.lsm.lv/raksts/zinas/arzemes/drosibai-svarigas-informacijas-nopludes-del-atkapjas-divi-zviedrijas-ministri.a244734/ [19]
38. https://www.nytimes.com/2017/07/25/world/europe/ibm-sweden-data-outsourcing.html [37]
39. https://www.reuters.com/sustainability/society-equity/italian-tax-police-search-multiple-offices-it-contracts-probe-2026-03-26/ [18]
40. https://www.reuters.com/technology/italian-tax-police-raid-digital-value-olidata-offices-2024-10-15/ [35]