III

(Sagatavošanā esoši tiesību akti)

EIROPAS CENTRĀLĀ BANKA

EIROPAS CENTRĀLĀS BANKAS ATZINUMS

(2021. gada 4. jūnijs)

par priekšlikumu Eiropas Parlamenta un Padomes regulai par finanšu sektora digitālās darbības noturību

(CON/2021/20)

(2021/C 343/01)

Ievads un tiesiskais pamats

Eiropas Centrālā banka (ECB) 2020. gada 22., 23. un 29. decembrī saņēma Eiropas Savienības Padomes un Eiropas Parlamenta lūgumus sniegt atzinumu par priekšlikumu Eiropas Parlamenta un Padomes regulai par finanšu sektora digitālās darbības noturību un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014 un (ES) Nr. 909/2014 ([1]) (turpmāk – "ierosinātā regula"), kā arī par priekšlikumu direktīvai, ar ko groza Direktīvas 2006/43/EK, 2009/65/EK, 2009/138/ES, 2011/61/ES, 2013/36/ES, 2014/65/ES, (ES) 2015/2366 un (ES) 2016/2341 ([2]) (turpmāk – "ierosinātā grozījumu direktīva", vai, norādot uz to kopā ar ierosināto regulu – "ierosinātie tiesību akti").

ECB kompetence sniegt atzinumu pamatojas uz Līguma par Eiropas Savienības darbību 127. panta 4. punktu un 282. panta 5. punktu, jo ierosinātajos tiesību aktos ietverti noteikumi, kas ir ECB kompetences jomās, jo īpaši tādās kā monetārās politikas noteikšana un īstenošana, maksājumu sistēmu raitas darbības veicināšana, palīdzība kompetentām iestādēm sekmīgi īstenot politiku, kas attiecas uz finanšu tirgus sistēmas stabilitāti, un ECB uzdevumi kredītiestāžu prudenciālās uzraudzības jomā saskaņā ar Līguma 127. panta 2. punkta pirmo un ceturto ievilkumu, 127. panta 5. punktu un 127. panta 6. punktu. ECB Padome šo atzinumu ir pieņēmusi saskaņā ar Eiropas Centrālās bankas reglamenta 17.5. panta pirmo teikumu.

1. Vispārīgi apsvērumi

1.1 ECB atzinīgi vērtē ierosināto regulu, kuras mērķis ir uzlabot kiberdrošību un finanšu sektora darbības noturību. ECB īpaši atzinīgi vērtē ierosinātās regulas mērķi novērst šķēršļus finanšu pakalpojumu iekšējam tirgum un uzlabot tā izveidi un darbību, saskaņojot noteikumus, kas piemērojami informācijas un komunikācijas tehnoloģiju (IKT) riska pārvaldībai, paziņošanai, testēšanai un ar trešo personu saistītajam IKT riskam. Turklāt ECB atzinīgi vērtē ierosinātās regulas mērķi racionalizēt un saskaņot visas tās regulatīvās prasības vai prognozes uzraudzības jomā, kuras savstarpēji pārklājas un kuras finanšu vienībām pašlaik piemēro saskaņā ar Savienības tiesību aktiem.

1.2 ECB saprot, ka attiecībā uz finanšu vienībām, kas noteiktas kā pamatpakalpojumu sniedzēji ([3]), ierosinātā regula ir tiesību akts konkrētai nozarei (*lex specialis*) tādā izpratnē, kas noteikta Eiropas Parlamenta un Padomes Direktīvas (ES) 2016/1148 ([4]) (turpmāk – "TID direktīva") 1. panta 7. punktā; tas nozīmē, ka ierosinātajā regulā paredzētajām prasībām principā būtu noteicošs spēks pār TID direktīvu. Praksē finanšu vienības, kas identificētas kā pamatpakalpojumu sniedzēji ([5]), cita starpā paziņotu par incidentiem saskaņā ar ierosināto

([1]) COM(2020) 595 *final*.
([2]) COM(2020) 596 *final*.
([3]) Sk. ierosinātās regulas 1. panta 2. punktu.
([4]) Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (OV L 194, 19.7.2016., 1. lpp.).
([5]) Sk. TID direktīvas 5. pantu.

regulu, nevis TID direktīvu. Lai gan ECB atzinīgi vērtē to, ka tiek samazinātas tādas prasības finanšu vienībām, kuras attiecas uz incidentu paziņošanu un, iespējams, savstarpēji pārklājas, būtu papildus jāizvērtē ierosinātās regulas un TID direktīvas mijiedarbība. Piemēram, saskaņā ar ierosināto regulu uz trešo personu, kas sniedz IKT pakalpojumus ([6]), varētu attiekties ieteikumi, kurus sniedzis galvenais pārraugs ([7]). Vienlaikus tā pati trešā persona, kas sniedz IKT pakalpojumus, var tikt klasificēta kā pamatpakalpojumu sniedzējs saskaņā ar TID direktīvu, un uz to varētu attiekties saistoši norādījumi, kurus izdevusi kompetentā iestāde ([8]). Šādā gadījumā uz trešo personu, kas sniedz IKT pakalpojumus, varētu attiekties pretrunīgi ieteikumi, kas sniegti saskaņā ar ierosināto regulu, un saistoši norādījumi, kas izdoti saskaņā ar TID direktīvu. ECB ierosina Savienības likumdevējām iestādēm turpināt apsvērt iespējamās neatbilstības starp ierosināto regulu un TID direktīvu, kas var kavēt tādu prasību saskaņošanu un samazināšanu, kuras noteiktas finanšu vienībām, kā arī savstarpēji pārklājas un ir pretrunīgas.

1.3 ECB arī saprot, ka saskaņā ar priekšlikumu Eiropas Parlamenta un Padomes direktīvai, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā un ar ko atceļ Direktīvu (ES) 2016/1148 ([9]) (turpmāk –"ierosinātā TID2 direktīva"), uz "gandrīz notikušu notikumu" ([10]) attieksies ziņošanas pienākumi ([11]). Lai gan ierosinātās TID2 direktīvas 39. apsvērumā ir atsauce uz termina "gandrīz noticis notikums" nozīmi, nav skaidrs, vai pastāv nodoms noteikt prasību, ka ierosinātās regulas 2. pantā uzskaitītajām finanšu vienībām jāziņo par gandrīz notikušiem notikumiem. Šajā sakarā, kā arī ņemot vērā to, ka gandrīz notikušus notikumus var konstatēt tikai pēc tam, kad tie ir notikuši, ECB labprāt savlaicīgi saņemtu paziņojumu par būtiskiem gandrīz notikušiem notikumiem, kā tas pašlaik notiek kiberincidentu gadījumā. ECB ierosina uzlabot ierosinātās regulas un ierosinātās TID2 direktīvas saskaņotību, lai konkretizētu precīzu ziņošanas tvērumu, kas saskaņā ar šiem diviem atšķirīgajiem, bet saistītajiem Savienības tiesību aktiem var attiekties uz jebkuru finanšu vienību. Vienlaikus būtu jādefinē "gandrīz noticis notikums" un jāizstrādā noteikumi, kas precizētu tā nozīmi.

1.4 ECB atzinīgi vērtē to, ka finanšu vienības tiek mudinātas brīvprātīgi apmainīties ar izlūkošanas informāciju par kiberdraudiem, lai uzlabotu un stiprinātu to kibernoturības stāvokli. ECB ir sniegusi palīdzību, rosinot "Kiberdraudu izlūkošanas informācijas apmaiņas iniciatīvu" (*CIISI-EU*) tirgus dalībniekiem, un plānu šādas iniciatīvas veidošanai un veicināšanai ECB ir padarījusi pieejamu ikvienam ([12]).

1.5 ECB atbalsta sadarbību starp kompetentajām iestādēm ierosinātās regulas nolūkā, Eiropas uzraudzības iestādēm (EUI) un kiberdrošības incidentu reaģēšanas vienībām (*CSIRT*) ([13]). Ir būtiski apmainīties ar informāciju, lai nodrošinātu Savienības darbības noturību, jo informācijas apmaiņa un iestāžu sadarbība var palīdzēt novērst kiberuzbrukumus un mazināt IKT apdraudējumu izplatīšanos. Būtu jāveicina vienota izpratne par riskiem, kas saistīti ar IKT, un visā Savienībā būtu jānodrošina konsekventa šādu risku novērtēšana. Ir ārkārtīgi svarīgi, lai kompetentās iestādes ([14]) dalītos informācijā ar vienoto kontaktpunktu ([15]) un valstu *CSIRT* tikai tad, ja ir skaidri noteikti klasifikācijas un informācijas apmaiņas mehānismi, kā arī pienācīgi aizsardzības pasākumi konfidencialitātes nodrošināšanai.

1.6 Visbeidzot, ECB atzinīgi novērtētu, ja ierosinātajā regulā iekļautu noteikumus par personas datiem un datu saglabāšanu. Saglabāšanas perioda ilguma vajadzībām būtu jāņem vērā izmeklēšana, pārbaude, informācijas pieprasīšana, paziņošana, publicēšana, izvērtēšana, pārbaude, novērtēšana un pārraudzības vai uzraudzības plānu sagatavošana, kas kompetentajām iestādēm varētu būt jāveic, pildot savas attiecīgās saistības un

([6]) Sk. ierosinātās regulas 3. panta 15) punktu.
([7]) Sk. ierosinātās regulas 31. panta 1. punkta d) apakšpunktu.
([8]) Sk. TID direktīvas 15. panta 3. punktu.
([9]) COM(2020) 823 *final*.
([10]) Notikums, kurš būtu varējis izraisīt kaitējumu, bet kura pilnīga izvēršanās tika veiksmīgi novērsta; sk. TID2 direktīvas 39. apsvērumu.
([11]) Sk. TID2 direktīvas 11. pantu.
([12]) *Cyber threat Intelligence Information Sharing Initiative* (*CIISI-EU*), kas pieejama ECB interneta vietnē www.ecb.europa.eu.
([13]) Sk. ierosinātās regulas 42. pantu.
([14]) Sk. arī TID2 direktīvas 11., 26. un 27. pantu.
([15]) Sk. TID direktīvas 8. panta 3. punktu.

pienākumus saskaņā ar ierosināto regulu. Šajā ziņā būtu piemērots 15 gadu saglabāšanas periods. Atkarībā no vajadzības konkrētos gadījumos, šo datu saglabāšanas periodu varētu saīsināt vai pagarināt. Šajā sakarā ECB ierosina Savienības likumdevējām iestādēm, formulējot attiecīgo noteikumu par personas datiem un datu saglabāšanu, ņemt vērā arī datu minimizēšanas principu, kā arī turpmāku apstrādi arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos vai statistikas nolūkos ([16]).

2. Īpaši apsvērumi par pārraudzību un vērtspapīru tīrvērti un norēķiniem

2.1 *ECBS un Eurosistēmas pārraudzības kompetence*

2.1.1 Līgums un Eiropas Centrālo banku sistēmas un Eiropas Centrālās bankas Statūti (turpmāk – "ECBS Statūti") ciešā saistībā ar Eurosistēmas monetārās politikas pamatuzdevumiem paredz, ka Eurosistēma veic tīrvērtes un maksājumu sistēmu pārraudzību. Saskaņā ar Līguma 127. panta 2. punkta ceturto ievilkumu, kas atspoguļots ECBS Statūtu 3.1. pantā, viens no pamatuzdevumiem, ko veic ar Eiropas Centrālo banku sistēmas (ECBS) palīdzību, ir veicināt maksājumu sistēmu raitu darbību. Pildot šo pamatuzdevumu, ECB un valstu centrālās bankas var dot iespējas, un ECB var izdot regulas, lai Savienībā un attiecībās ar citām valstīm nodrošinātu efektīvas un stabilas tīrvērtes un maksājumu sistēmas ([17]). Pildot savu pārraudzības funkciju, ECB pieņēma Eiropas Centrālās bankas Regulu (ES) Nr. 795/2014 (ECB/2014/28) (turpmāk – "SNMS regula") ([18]). Ar SNMS regulu ir detalizēti ieviesti 2012. gada aprīļa "Finanšu tirgus infrastruktūru principi", kurus izstrādājusi Maksājumu un norēķinu sistēmu komiteja (*Committee on Payment and Settlement Systems*) un Starptautiskā Vērtspapīru komisiju organizācija (*International Organisation of Securities Commissions*) ([19]), un šie principi ir juridiski saistoši un attiecas gan uz sistēmiski nozīmīgām liela apjoma maksājumu sistēmām, gan arī uz sistēmiski nozīmīgām neliela apjoma maksājumu sistēmām, kuras nodrošina vai nu Eurosistēmas centrālā banka, vai arī privāta struktūra. Eurosistēmas pārraudzības politikas regulējumā ([20]) noteikts, ka maksājumu instrumenti ir "maksājumu sistēmu neatņemama daļa", un tādējādi tie iekļauti tās pārraudzības tvērumā. Pašlaik tiek pārskatīts maksājumu instrumentu pārraudzības regulējums ([21]). Šajā regulējumā maksājumu instruments (piemēram, karte, kredīta pārvedums, tiešais debets, e-naudas pārvedums un digitālo maksājumu tokens ([22])) tiek definēts kā tāda personalizēta ierīce (vai ierīču kopums) un/vai tāds procedūru kopums saskaņā ar maksājumu pakalpojumu lietotāja un maksājumu pakalpojumu sniedzēja vienošanos, ar kuru iniciē vērtības nodošanu ([23]).

2.1.2 Ņemot vērā iepriekš minēto, ECB atzinīgi vērtē to, ka no ierosinātās regulas darbības jomas ir izslēgti sistēmas operatori, kā definēts Eiropas Parlamenta un Padomes Direktīvas 98/26/EK ([24]) 2. panta p) punktā, maksājumu sistēmas (tostarp centrālo banku pārvaldītās sistēmas), maksājumu shēmas un maksājumu pasākumi, ņemot

([16]) Sk. 4. panta 1. punkta b) apakšpunktu un 13. pantu Eiropas Parlamenta un Padomes Regulā (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK (OV L 295, 21.11.2018., 39. lpp.).

([17]) Sk. ECBS Statūtu 22. pantu.

([18]) Eiropas Centrālās bankas Regula (ES) Nr. 795/2014 (2014. gada 3. jūlijs) par sistēmiski nozīmīgu maksājumu sistēmu pārraudzību (ECB/2014/28) (OV L 217, 23.7.2014., 16. lpp.).

([19]) Pieejami Starptautisko norēķinu bankas interneta vietnē www.bis.org.

([20]) Eurosistēmas pārraudzības politikas regulējums (*Eurosystem oversight policy framework*), pārskatītā versija (2016. gada jūlijs), kas pieejama ECB interneta vietnē www.ecb.europa.eu.

([21]) Sk. pārskatīto un konsolidēto 2020. gada oktobra Eurosistēmas elektronisko maksājumu instrumentu, shēmu un pasākumu pārraudzības regulējumu (*PISA* regulējums) (*Eurosystem oversight framework for electronic payment instruments, schemes and arrangements (PISA framework)*), kas pieejams ECB interneta vietnē www.ecb.europa.eu.

([22]) Digitālo maksājumu tokens ir digitāls vērtības atspoguļojums, kas nodrošināts ar prasījumiem vai aktīviem, kuri reģistrēti citur, un ļauj nodot vērtību starp galalietotājiem. Atkarībā no digitālo maksājumu tokenu funkcionālajiem elementiem, ar tiem var būt iespējama vērtības nodošana, neiesaistot centrālo trešo personu un/vai neizmantojot maksājumu kontus.

([23]) "Vērtības nodošana". "Maksātāja vai maksājuma saņēmēja, kas rīkojas maksātāja uzdevumā, iniciēts naudas līdzekļu vai digitālo maksājumu tokenu pārvedums vai skaidras naudas iemaksa lietotāja kontā vai izņemšana no tā neatkarīgi no pamatā esošām maksātāja un maksājuma saņēmēja saistībām. Pārveduma veikšanā būt iesaistīts viens vai vairāki maksājumu pakalpojumu sniedzēji." Šī "vērtības nodošanas" definīcija *PISA* regulējumā atšķiras no "naudas līdzekļu" pārveduma definīcijas saskaņā ar Eiropas Parlamenta un Padomes Direktīvu (ES) 2015/2366 (2015. gada 25. novembris) par maksājumu pakalpojumiem iekšējā tirgū, ar ko groza Direktīvas 2002/65/EK, 2009/110/EK un 2013/36/ES un Regulu (ES) Nr. 1093/2010 un atceļ Direktīvu 2007/64/EK (OV L 337, 23.12.2015., 35. lpp.). "Vērtības nodošana" minētajā direktīvā definētā "maksājumu instrumenta" kontekstā var nozīmēt tikai "naudas līdzekļu" pārvedumu. Saskaņā ar minēto direktīvu "naudas līdzekļi" neietver digitālo maksājumu tokenus, izņemot gadījumus, kad tokenus var klasificēt kā elektronisko naudu (vai hipotētiski – kā naudu ieraksta veidā).

([24]) Eiropas Parlamenta un Padomes Direktīva 98/26/EK (1998. gada 19. maijs) par norēķinu galīgumu maksājumu un vērtspapīru norēķinu sistēmās (OV L 166, 11.6.1998., 45. lpp.).

vērā iepriekš minēto pārraudzības regulējumu piemērošanu. Šo iemeslu dēļ ierosinātās regulas apsvērumos būtu nepārprotami jāatspoguļo ECBS kompetence saskaņā ar Līgumu un Eurosistēmas kompetence saskaņā ar SNMS regulu.

2.1.3 Tāpat ECB atzinīgi vērtē to, ka ierosinātajā regulā noteikto pārraudzības sistēmu nav paredzēts piemērot attiecībā uz tādām trešām personām, kas sniedz IKT pakalpojumus, kurām piemēro Līguma par Eiropas Savienības darbību 127. panta 2. punktā minēto uzdevumu atbalstam izveidotās pārraudzības sistēmas ([25]). Šajā sakarā ECB vēlas uzsvērt, ka ierosinātās regulas pants par darbības jomu neattiecas uz ECBS centrālajām bankām, kad tās rīkojas kā monetāras iestādes ([26]), un Eurosistēmu, kad tā sniedz pakalpojumus, izmantojot *TARGET2*, *TARGET2* vērtspapīriem (T2V) ([27]) un *TARGET* ātro maksājumu norēķinus (*TIPS*) ([28]), kā arī tās nevar uzskatīt par trešām personām, kas sniedz IKT pakalpojumus, un tādēļ ierosinātās regulas vajadzībām tās nevarētu klasificēt kā kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus. Eurosistēma pārrauga T2V saistībā ar tās pilnvarām nodrošināt efektīvas un stabilas tīrvērtes un maksājumu sistēmas. Turklāt EVTI ir precizējusi, ka T2V nav būtisku pakalpojumu sniedzējs ([29]) Eiropas Parlamenta un Padomes Regulas (ES) Nr. 909/2014 ([30]) (turpmāk – "CVD regula") izpratnē. Tāpēc T2V organizatoriskā un darbības drošība, efektivitāte un noturība tiek nodrošināta, izmantojot piemērojamo juridisko, tiesisko un darbības regulējumu un saskaņotos pārvaldības pasākumus jeb T2V, nevis CVD regulu.

2.1.4 Turklāt Eurosistēmas pārraudzības politikas regulējums ([31]) attiecas uz tādiem būtiskiem pakalpojumu sniedzējiem kā Vispasaules Starpbanku finanšu telekomunikāciju sabiedrība (*Society for Worldwide Interbank Financial Telecommunication*; *SWIFT*). *SWIFT* ir Beļģijā reģistrēta kooperatīvā sabiedrība ar ierobežotu atbildību, kas sniedz drošas ziņojumapmaiņas pakalpojumus starptautiskā mērogā. *Nationale Bank van België*/*Banque Nationale de Belgique* rīkojas kā *SWIFT* vadošais pārraugs un, uzmantojot sadarbībā balstītu pārraudzības mehānismu, veic *SWIFT* pārraudzību sadarbībā ar pārējām G10 centrālajām bankām, tostarp ECB. G10 pārraugi atzīst, ka pārraudzības galvenais mērķis ir *SWIFT* operacionālais risks, jo to uzskata par primāro riska kategoriju, ar kuru *SWIFT* varētu radīt sistēmisku risku Savienības finanšu sistēmai. Šajā sakarā Sadarbībā balstītā *SWIFT* pārraudzības grupa ir izstrādājusi *SWIFT* piemērojamus konkrētus principus un augsta līmeņa prognozes, piemēram, attiecībā uz riska apzināšanu un pārvaldību, informācijas drošību, uzticamību un noturību, tehnoloģiju plānošanu un saziņu ar lietotājiem. G10 pārraugi sagaida, ka *SWIFT* ievēros Maksājumu un tirgus infrastruktūru komitejas (*CPMI*) un Starptautiskās Vērtspapīru komisiju organizācijas (*IOSCO*) "Norādījumus par kibernoturību" (*Guidance on cyber resilience*) ([32]), kā arī citus starptautiskos IKT drošības standartus, kuri kopumā pārsniedz ierosinātajā regulā noteiktās prasības.

2.1.5 Uz *SWIFT* un, iespējams, uz citiem pakalpojumu sniedzējiem, kuriem piemērojams Eurosistēmas pārraudzības politikas regulējums, ierosinātā regula varētu attiekties kā uz trešām personām, kas sniedz IKT pakalpojumus, ja tie sniegtu pakalpojumus, uz kuriem neattiecas Līguma 127. panta 2. punkts. Tāpēc ECB ļoti atzinīgi vērtē to, ka pakalpojumu sniedzēji, uz kuriem jau attiecas Eurosistēmas pārraudzības politikas regulējums, tostarp *SWIFT*, ir izslēgti no ierosinātajā regulā noteiktā pārraudzības regulējuma piemērošanas jomas.

([25]) Sk. ierosinātās regulas 28. panta 5. punktu.

([26]) Sk. 1.3. punktu Eiropas Centrālās bankas Atzinumā (2021. gada 19. februāris) par priekšlikumu regulai par kriptoaktīvu tirgiem un ar ko groza Direktīvu (ES) 2019/1937 (CON/2021/4). Visi ECB atzinumi tiek publicēti *EUR-Lex*.

([27]) Sk. IIA pielikumu Eiropas Centrālās bankas Pamatnostādnei ECB/2012/27 (2012. gada 5. decembris) par Eiropas automatizēto reālā laika bruto norēķinu sistēmu (*TARGET2*) (OV L 30, 30.1.2013., 1. lpp.). Eiropas Centrālās bankas Pamatnostādne ECB/2012/13 (2012. gada 18. jūlijs) par *TARGET2* vērtspapīriem (OV L 215, 11.8.2012., 19. lpp.); Eiropas Centrālās bankas Lēmums ECB/2011/20 (2011. gada 16. novembris), ar ko nosaka detalizētus noteikumus un procedūras atbilstības kritēriju ieviešanai attiecībā uz centrālo vērtspapīru depozitāriju piekļuvi *TARGET2* vērtspapīriem pakalpojumiem (OV L 319, 2.12.2011., 117. lpp.). Sk. arī T2V Pamatlīgumu un Koplīgumu.

([28]) Sk. Pamatnostādnes ECB/2012/27 IIB pielikumu.

([29]) Sk. 30. panta 5. punktu Eiropas Parlamenta un Padomes Regulā (ES) Nr. 909/2014 (2014. gada 23. jūlijs) par vērtspapīru norēķinu uzlabošanu Eiropas Savienībā, centrālajiem vērtspapīru depozitārijiem un grozījumiem Direktīvās 98/26/EK un 2014/65/ES un Regulā (ES) Nr. 236/2012 (OV L 257, 28.8.2014., 1. lpp.) un 68. pantu Komisijas Deleģētajā regulā (ES) 2017/392 (2016. gada 11. novembris) ar ko Eiropas Parlamenta un Padomes Regulu (ES) Nr. 909/2014 papildina attiecībā uz regulatīvajiem tehniskajiem standartiem par atļauju izsniegšanas, uzraudzības un operacionālajām prasībām centrālajiem vērtspapīru depozitārijiem (OV L 65, 10.3.2017., 48. lpp.).

([30]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 909/2014 (2014. gada 23. jūlijs) par vērtspapīru norēķinu uzlabošanu Eiropas Savienībā, centrālajiem vērtspapīru depozitārijiem un grozījumiem Direktīvās 98/26/EK un 2014/65/ES un Regulā (ES) Nr. 236/2012 (OV L 257, 28.8.2014., 1. lpp.).

([31]) Eurosistēmas pārraudzības politikas regulējums (*Eurosystem oversight policy framework*), pārskatītā versija (2016. gada jūlijs), kas pieejama ECB interneta vietnē www.ecb.europa.eu.

([32]) Pieejami Starptautisko norēķinu bankas interneta vietnē www.bis.org.

2.2 *ESCB kompetence vērtspapīru tīrvērtes jomā*

2.2.1 Centrālie vērtspapīru depozitāriji (CVD) ir finanšu tirgus infrastruktūras (FTI), ko stingri regulē un uzrauga dažādas iestādes saskaņā ar CVD regulu, kurā noteiktas prasības attiecībā uz norēķiniem par finanšu instrumentiem, kā arī noteikumi par CVD organizatorisko struktūru un darbību. CVD arī jāņem vērā *CPMI-IOSCO* "Norādījumi par kibernoturību", kuru īstenošanai ir izstrādātas "Kibernoturības pārraudzības prognozes attiecībā uz FTI" (*Cyber resilience oversight expectations for financial market infrastructures*; 2018. gada decembris) ([33]). Papildus uzraudzības pilnvarām, kas saskaņā ar CVD regulu uzticētas nacionālajām kompetentajām iestādēm (NKI), ECBS dalībnieki rīkojas kā "attiecīgās iestādes", kas ir CVD uzturēto vērtspapīru norēķinu sistēmu pārraugi, kā centrālās bankas, kas emitē svarīgākās valūtas, kurās tiek veikti norēķini, un kā centrālās bankas, kuru reģistros tiek veikti naudas posma norēķini ([34]). Šajā sakarā CVD regulas 8. apsvērumā norādīts, ka regula būtu jāpiemēro, neskarot ECB un nacionālo centrālo banku pienākumus nodrošināt efektīvas un stabilas tīrvērtes un maksājumu sistēmas Savienībā un citās valstīs. CVD regulas 8. apsvērumā arī norādīts, ka tai nevajadzētu novērst ECBS dalībnieku piekļuvi informācijai, kas ir svarīga to pienākumu pildīšanā ([35]), tostarp CVD un citu finanšu tirgus infrastruktūru pārraudzībā ([36]).

2.2.2 Turklāt ECBS dalībnieki bieži rīkojas kā norēķinu iestādes vērtspapīru darījumu naudas posmā, un Eurosistēma ar T2V starpniecību piedāvā norēķinu pakalpojumus CVD. Eurosistēmas veiktā T2V pārraudzība ir saistīta ar tās pilnvarām nodrošināt efektīvas un stabilas tīrvērtes un maksājumu sistēmas, savukārt CVD kompetento iestāžu un attiecīgo iestāžu mērķis ir nodrošināt to raitu darbību, norēķinu drošību un efektivitāti, kā arī finanšu tirgu pareizu darbību to attiecīgajās jurisdikcijās.

2.2.3 Saskaņā ar ierosināto regulu ([37]) ECBS centrālās bankas nav iesaistītas tehnisko standartu izstrādē attiecībā uz IKT risku noteikšanu. Tāpat saskaņā ar ierosināto regulu ([38]) attiecīgās iestādes netiek informētas par incidentiem, kas saistīti ar IKT. ECBS centrālajai bankai būtu jāsaglabā tāds pats iesaistes līmenis, kāds pašlaik paredzēts CVD regulā, un attiecīgās iestādes būtu jāinformē par incidentiem, kas saistīti ar IKT. Eurosistēma ir attiecīgā iestāde visiem euro zonas CVD un vairākiem citiem ES CVD. ECBS centrālās bankas būtu jāinformē par incidentiem, kas saistīti ar IKT un kas attiecas uz to pienākumu izpildi, tostarp CVD un citu FTI pārraudzību. Riski, kuriem pakļauti CVD, tostarp IKT riski, var apdraudēt CVD stabilu darbību. Tādēļ IKT riski ir svarīgi attiecīgajām iestādēm, kurām būtu jāgūst pilnīgs un detalizēts pārskats par šiem riskiem, lai novērtētu tos un ietekmētu CVD riska pārvaldības pieeju. Ierosinātajā regulā nevajadzētu paredzēt mazāk ierobežojošas prasības attiecībā uz IKT riskiem salīdzinājumā ar prasībām, kas noteiktas CVD regulā un spēkā esošajos regulatīvajos tehniskajos standartos.

2.2.4 Turklāt Savienības likumdevējām iestādēm būtu jāprecizē mijiedarbība starp ierosināto regulu ([39]) un regulatīvajiem tehniskajiem standartiem, kas papildina CVD regulu. It īpaši nav skaidrs, vai CVD ir jāatbrīvo no pienākuma izveidot savu rezerves apstrādes vietu, ja trešā persona, kas sniedz IKT pakalpojumus CVD, uztur šādu vietu ([40]). Ja CVD tiktu atbrīvots no pienākuma uzturēt rezerves apstrādes vietu, nav skaidrs, kāds

([33]) Pieejami ECB interneta vietnē www.ecb.europa.eu.

([34]) Sk. Regulas (ES) Nr. 909/2014 12. pantu.

([35]) Sk. arī Regulas (ES) Nr. 909/2014 13. pantu, 17. panta 4. punktu un 22. panta 6. punktu.

([36]) Sk. 7.3. punktu Eiropas Centrālās bankas Atzinumā (2017. gada 6. aprīlis) par kritiski svarīgās infrastruktūras identifikāciju informācijas tehnoloģiju drošības vajadzībām (CON/2017/10), 7.2. punktu Eiropas Centrālās bankas Atzinumā (2018. gada 8. novembris) par to, kā apstiprina pamatpakalpojumus un pamatpakalpojumu sniedzējus tīkla un informācijas sistēmu drošības vajadzībām (CON/2018/47), 3.5.2. punktu Eiropas Centrālās bankas Atzinumā (2019. gada 2. maijs) par tīkla un informācijas sistēmu drošību (CON/2019/17) un 3.5.2. punktu Eiropas Centrālās bankas Atzinumā (2019. gada 11. novembris) par tīkla un informācijas sistēmu drošību (CON/2019/38).

([37]) Sk. ierosinātās regulas 54. panta 5. punktu un Regulas (ES) Nr. 909/2014 45. panta 7. punktu.

([38]) Sk. ierosinātās regulas 54. panta 4. punktu un Regulas (ES) Nr. 909/2014 45. panta 6. punktu.

([39]) Sk. ierosinātās regulas 11. panta 5. punktu.

([40]) Sk. 78. panta 3. punktu Komisijas Deleģētajā regulā (ES) 2017/392 (2016. gada 11. novembris), ar ko Eiropas Parlamenta un Padomes Regulu (ES) Nr. 909/2014 papildina attiecībā uz regulatīvajiem tehniskajiem standartiem par atļauju izsniegšanas, uzraudzības un operacionālajām prasībām centrālajiem vērtspapīru depozitārijiem (OV L 65, 10.3.2017., 48. lpp.).

būtu šīs prasības juridiskais spēks. Tāpat ierosinātajā regulā ([41]) ir atsauce uz katras funkcijas atgūšanas laika mērķi un atgūšanas punkta mērķiem ([42]), savukārt attiecīgais regulatīvais tehniskais standarts izšķir svarīgās funkcijas ([43]) un svarīgās darbības ([44]) saistībā ar CVD svarīgajām darbībām noteikto darbības atgūšanas laikposmu. Lai novērstu pretrunīgu prasību risku, Savienības likumdevējām iestādēm vajadzētu precizēt un turpināt apsvērt mijiedarbību starp ierosināto regulu un regulatīvajiem tehniskajiem standartiem, kas papildina CVD regulu. Visbeidzot, būtu jāprecizē, ka ar ierosināto regulu tiek paplašināti atbrīvojumi, kas saskaņā ar CVD regulu ([45]) ir piešķirti dažu publisko struktūru uzturētiem CVD.

2.3 *ECBS kompetence vērtspapīru tīrvērtes jomā*

2.3.1 ECBS centrālajām bankām ir uzticētas pārraudzības pilnvaras attiecībā uz centrālajiem darījumu partneriem (CDP). Šajā sakarā Eurosistēmas nacionālās centrālās bankas bieži sadarbojas ar attiecīgajām nacionālajām kompetentajām iestādēm CDP pārraudzības un uzraudzības funkciju veikšanā un piedalās attiecīgās CDP kolēģijā, kas izveidota saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 648/2012 ([46]) (turpmāk – "ETIR"). Attiecīgie Eurosistēmas dalībnieki ([47]) piedalās ETIR kolēģijās kā pārraugi un pārstāv Eurosistēmu kā emisijas centrālā banka CDP, kam euro ir nozīmīgākā valūta, kurā denominēti finanšu instrumenti, kam veic tīrvērti (un ārvalstu CDP, kas veic tīrvērti nozīmīgam euro denominētu darījumu apjomam). ECB ir ārpus euro zonas esošo CDP emisijas centrālā banka.

2.3.2 Saskaņā ar ierosināto regulu ([48]) ECBS centrālās bankas nav iesaistītas tehnisko standartu izstrādē attiecībā uz IKT risku noteikšanu. Turklāt ierosinātajā regulā ([49]) nav nevienas atsauces uz atgūšanas laika mērķa un atgūšanas punkta mērķa prasībām saskaņā ar ETIR ([50]). Ierosinātajai regulatīvajai sistēmai nevajadzētu paredzēt prasības attiecībā uz IKT riskiem, kuras ir mazāk ierobežojošas kā pašlaik pastāvošās prasības. Tādēļ ir ļoti svarīgi noteikt skaidrus atgūšanas laika un atgūšanas punkta mērķus, lai izveidotu stabilu darbības nepārtrauktības pārvaldības sistēmu. Konkrētu atgūšanas laika un atgūšanas punkta mērķu uzturēšana ir ietverta arī *CPMI-IOSCO* "Finanšu tirgus infrastruktūru principos" ([51]). Būtu jāsaglabā pašreizējais ETIR noteikums, un ierosinātā regula būtu attiecīgi jāpielāgo. ECBS centrālās bankas būtu jāiesaista jebkādu sekundāro tiesību aktu sagatavošanā, kā arī Savienības likumdevējām iestādēm būtu jāprecizē un jāturpina apsvērt mijiedarbība starp ierosināto regulu un to papildinošajiem regulatīvajiem tehniskajiem standartiem, lai novērstu prasību savstarpēju pārklāšanos vai to pretrunas.

3. **Īpaši apsvērumi par prudenciālās uzraudzības aspektiem**

3.1 Padomes Regulā (ES) Nr. 1024/2013 ([52]) (turpmāk – "VUM regula") ir noteikti konkrēti uzdevumi ECB attiecībā uz kredītiestāžu prudenciālo uzraudzību euro zonā un ir paredzēts, ka ECB atbild par Vienotā uzraudzības mehānisma (VUM), kurā ECB un iesaistītajām NKI tiek sadalīti konkrēti uzraudzības pienākumi, efektīvu un konsekventu darbību. ECB jo īpaši veic visu kredītiestāžu atļauju izsniegšanas un atsaukšanas uzdevumu. ECB uzdevums cita starpā ir arī nodrošināt atbilstību attiecīgajiem Eiropas Savienības tiesību aktiem, ar kuriem kredītiestādēm noteiktas prudenciālās prasības, tajā skaitā prasība ieviest stabilu pārvaldības kārtību, piemēram, drošus riska pārvaldības procesus un iekšējās kontroles mehānismus ([53]). Šajā nolūkā ECB piešķirtas visas tās funkciju izpildei

([41]) Sk. ierosinātās regulas 11. panta 6. punktu.
([42]) Sk. ierosinātās regulas 3. panta 17. punktu.
([43]) Sk. Komisijas Deleģētās regulas (ES) 2017/392 76. panta 2. punkta d) un e) apakšpunktu.
([44]) Sk. Komisijas Deleģētās regulas (ES) 2017/392 78. panta 2. un 3. punktu.
([45]) Sk. Regulas (ES) Nr. 909/2014 1. panta 4. punktu.
([46]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 648/2012 (2012. gada 4. jūlijs) par ārpusbiržas atvasinātajiem instrumentiem, centrālajiem darījumu partneriem un darījumu reģistriem (OV L 201, 27.7.2012., 1. lpp.).
([47]) Sk. ETIR 18. panta 2. punkta g) un h) apakšpunktu.
([48]) Sk. ierosinātās regulas 53. panta 2. punkta b) apakšpunktu un 53. panta 3. punktu, kā arī ETIR 34. panta 3. punktu.
([49]) Sk. ierosinātās regulas 53. panta 2. punkta a) apakšpunktu.
([50]) Sk. ETIR 34. pantu.
([51]) Sk. *CPMI-IOSCO* "Finanšu tirgus infrastruktūru principos", kas pieejami Starptautisko norēķinu bankas interneta vietnē www.bis.org.
([52]) Padomes Regula (ES) Nr. 1024/2013 (2013. gada 15. oktobris), ar ko Eiropas Centrālajai bankai uztic īpašus uzdevumus saistībā ar politikas nostādnēm, kas attiecas uz kredītiestāžu prudenciālo uzraudzību (OV L 287, 29.10.2013., 63. lpp.).
([53]) Sk. Regulas (ES) Nr. 1024/2013 4. panta 1. punkta e) apakšpunktu un 6. panta 4. punktu.

nepieciešamās uzraudzības pilnvaras iejaukties kredītiestāžu darbībā. Tādējādi ECB un attiecīgās NKI ir kompetentās iestādes, kas īsteno konkrētas prudenciālās uzraudzības pilnvaras saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 575/2013 ([54]) (turpmāk – "Kapitāla prasību regula") un Eiropas Parlamenta un Padomes Direktīvu 2013/36/ES ([55]) (turpmāk – "Kapitāla prasību direktīva").

3.2 Ierosinātajā regulā ir noteikts, ka būtu jāturpina pilnveidot vienoto noteikumu kopumu un uzraudzības sistēmu, lai aptvertu digitālās darbības noturību un IKT drošību, paplašinot finanšu stabilitātes un tirgus integritātes uzraudzībai un aizsardzībai norīkoto finanšu uzraudzības iestāžu pilnvaras ([56]). Mērķis ir veicināt visaptverošu IKT vai operacionālā riska sistēmu, saskaņojot galvenās digitālās darbības noturības prasības visām finanšu vienībām ([57]). Jo īpaši ierosinātās regulas mērķis ir konsolidēt un uzlabot IKT riska prasības, kas līdz šim dažādos tiesību aktos ir skatītas atsevišķi ([58]).

3.3 Prasības, kas saistītas ar IKT risku finanšu nozarē, pašlaik ir sadalītas vairākos Savienības tiesību aktos, tostarp Kapitāla prasību direktīvā, un ieteikuma tiesību instrumentos (piemēram, EBI pamatnostādnēs), un tās ir daudzveidīgas un dažkārt nepilnīgas. Dažos gadījumos IKT risks ir ietverts tikai netieši kā daļa no operacionālā riska, savukārt citos tas nav ietverts vispār. Tas būtu jānovērš, saskaņojot ierosināto regulu un minētos aktus. Šajā nolūkā ierosinātajā grozījumu direktīvā ir ietverts grozījumu kopums, kas šķiet nepieciešams, lai nodrošinātu juridisko skaidrību un konsekvenci attiecībā uz dažādu digitālās darbības noturības prasību piemērošanu. Tomēr ierosinātajā grozījumu direktīvā ([59]) pašlaik ietvertie Kapitāla prasību direktīvas grozījumi aptver tikai noteikumus par ārkārtas situāciju un darbības nepārtrauktības plāniem ([60]), kuru mērķis ir netieši kalpot par pamatu IKT riska pārvaldībai.

3.4 Turklāt ierosinātajā regulā ([61]) paredzēts, ka finanšu vienībām, tostarp kredītiestādēm, ir izveidotas iekšējās pārvaldības un kontroles sistēmas, kas nodrošina visu IKT risku efektīvu un prudenciālu pārvaldību. Ierosinātajā regulā ([62]) paredzēta tajā noteikto prasību piemērošana individuālā un konsolidētā līmenī, bet bez pietiekamas saskaņošanas ar minētajiem nozares tiesību aktiem. Visbeidzot, ierosinātajā regulā ([63]) ir paredzēts, ka, neskarot ierosinātās regulas noteikumus par kritisku svarīgu trešo personu, kas sniedz IKT pakalpojumus, pārraudzības sistēmu ([64]), kredītiestādēm regulā noteikto pienākumu izpildi nodrošina kompetentā iestāde, kas izraudzīta saskaņā ar Kapitāla prasību direktīvas 4. pantu, neskarot īpašos uzdevumus, kas ECB uzticēti ar VUM regulu.

3.5 Ņemot vērā iepriekš minēto, ECB saprot, ka, neskarot ierosinātās regulas noteikumus par kritisku svarīgu trešo personu, kas sniedz IKT pakalpojumus, pārraudzības sistēmu ([65]), ierosinātās regulas mērķis attiecībā uz kredītiestādēm ir izveidot prudenciālu iekšējās pārvaldības sistēmu IKT riska pārvaldībai, kas tiks integrēta vispārējā iekšējās pārvaldības sistēmā saskaņā ar Kapitāla prasību direktīvu. Turklāt, ņemot vērā ierosinātās sistēmas prudenciālās iezīmes, kompetentās iestādes, kas atbild par ierosinātajā regulējumā noteikto pienākumu izpildes uzraudzību, tostarp ECB, būs iestādes, kas atbild par banku uzraudzību saskaņā ar VUM regulu.

([54]) Eiropas Parlamenta un Padomes Regula (ES) Nr. 575/2013 (2013. gada 26. jūnijs) par prudenciālajām prasībām attiecībā uz kredītiestādēm un ieguldījumu brokeru sabiedrībām, un ar ko groza Regulu (ES) Nr. 648/2012 (OV L 176, 27.6.2013., 1. lpp.).

([55]) Eiropas Parlamenta un Padomes Direktīva 2013/36/ES (2013. gada 26. jūnijs) par piekļuvi kredītiestāžu darbībai un kredītiestāžu un ieguldījumu brokeru sabiedrību prudenciālo uzraudzību, ar ko groza Direktīvu 2002/87/EK un atceļ Direktīvas 2006/48/EK un 2006/49/EK (OV L 176, 27.6.2013., 338. lpp.).

([56]) Sk. ierosinātās regulas 8. apsvērumu.

([57]) Sk. ierosinātās regulas 11. apsvērumu.

([58]) Sk. ierosinātās regulas 12. apsvērumu.

([59]) Sk. ierosinātās grozījumu direktīvas 4. un 5. apsvērumu.

([60]) Sk. Kapitāla prasību direktīvas 85. pantu.

([61]) Sk. ierosinātās regulas 4. panta 1. punktu.

([62]) Sk. ierosinātās regulas 25. panta 3. un 4. punktu.

([63]) Sk. ierosinātās regulas 41. pantu.

([64]) Sk. ierosinātās regulas V nodaļas II iedaļu.

([65]) Sk. ierosinātās regulas V nodaļas II iedaļu.

3.6 Tādēļ Savienības likumdevējas iestādes varētu vēlēties ņemt vērā šādus ierosinājumus, lai uzlabotu ierosinātās regulas un Kapitāla prasību direktīvas skaidrību un saskaņotību. Pirmkārt, ierosinātās regulas prasības var nepārprotami uzskatīt par prudenciālām prasībām, kā tas cita starpā ir CVD regulā ([66]). Otrkārt, ņemot vērā to, ka ierosinātās regulas prasības neattiecas tikai uz ārkārtas situāciju un darbības nepārtrauktības plāniem, varētu paplašināt ierosinātās grozījumu direktīvas apsvērumu ([67]) formulējumus. Uz IKT riska pārvaldības pasākumiem attiecas stingrāku pārvaldības pasākumu kopums saskaņā ar Kapitāla prasību direktīvas ([68]) 74. pantu. Treškārt, ierosinātā regula ([69]) būtu jāgroza, lai apsvērumos atgādinātu ECB kompetenci attiecībā uz kredītiestāžu prudenciālo uzraudzību saskaņā ar Līgumu un VUM regulu. Ceturtkārt, atsauce uz tajā paredzēto prasību piemērošanu individuālā un konsolidētā līmenī ([70]) būtu jāpārskata, jo ierosinātajā regulā nav subkonsolidētā un konsolidētā līmeņa definīciju un konsolidētā uzraudzība saskaņā ar attiecīgajiem tiesību aktiem neattiecas uz dažu veidu starpniekiem (piemēram, maksājumu iestādēm). Turklāt ierosinātajā regulā paredzēto prasību piemērošanas līmenim vajadzētu būt atkarīgam tikai no tiesību aktiem, kas piemērojami katram finanšu vienības veidam. Attiecībā uz kredītiestādēm ir paredzēta skaidra saikne starp Kapitāla prasību direktīvu un ierosināto regulu, tāpēc ierosinātās regulas prasības tiktu automātiski piemērotas attiecīgi individuālā, subkonsolidētā vai konsolidētā līmenī ([71]). Visbeidzot, Savienības likumdevējas iestādes varētu apsvērt iespēju paredzēt pārejas režīmu, lai pārvaldītu laikposmu no ierosinātās regulas stāšanās spēkā līdz regulas priekšlikumā paredzēto regulatīvo tehnisko standartu stāšanās spēkā, jo uz dažiem starpniekiem, tostarp kredītiestādēm, jau attiecas noteikumi par IKT riskiem, kas ir piemērojami konkrētām nozarēm un ir detalizētāki nekā ierosinātās regulas vispārīgie noteikumi.

3.7 Saskaņā ar VUM regulu ECB ir uzticēts uzdevums nodrošināt kredītiestāžu atbilstību Savienības tiesību aktu prasībām, kas paredz, ka kredītiestādēm jābūt stabiliem riska pārvaldības procesiem un iekšējās kontroles mehānismiem ([72]). Tas nozīmē, ka ECB jānodrošina, lai nozīmīgajās uzraudzītajās iestādēs tiktu īstenota politika un procedūras, kas ļauj novērtēt un pārvaldīt to operacionālo risku, tostarp modeļa risku, ietverot notikumus ar zemu iestāšanās varbūtību un būtisku ietekmi. Kredītiestādēm ir jāprecizē, kas ir operacionālais risks šīs politikas un procedūru vajadzībām ([73]).

3.8 Eiropas Centrālās bankas (ECB) Padome 2017. gada jūlijā, pamatojoties uz Uzraudzības valdes priekšlikuma projektu saskaņā ar VUM regulas 26. panta 8. punktu un 6. panta 2. punktu un Eiropas Centrālās bankas Regulas (ES) Nr. 468/2014 (ECB/2014/17) ([74]) 21. panta 1. punktu, izveidoja VUM kiberincidentu paziņošanas sistēmu (turpmāk – "paziņošanas sistēma"). Sistēmas pamatā ir saistošs pieprasījums (individuāli lēmumi, kas adresēti kredītiestādēm) sniegt informāciju un/vai paziņot saskaņā ar VUM regulas 10. pantu ([75]). Dažās valstīs jau ir ieviests incidentu paziņošanas process, saskaņā ar kuru kredītiestādēm ir jāpaziņo savām NKI par visiem būtiskajiem kiberincidentiem. Šajās valstīs nozīmīgas kredītiestādes joprojām ziņos par incidentiem NKI, kuras pēc tam uzraudzīto iestāžu vārdā bez liekas kavēšanās pārsūtīs šos paziņojumus ECB. Tāpēc iepriekš minētie lēmumi ir adresēti arī šīm nacionālajām kompetentajām iestādēm, lai paziņošanas sistēmas ietvaros nosūtītu šo informāciju

([66]) Sk. CVD regulas II nodaļas 4. iedaļu "Prudenciālās prasības".

([67]) Sk. ierosinātās grozījumu direktīvas 4. apsvērumu.

([68]) Direktīvas 2013/36/ES 85. pantā noteikti tikai kritēriji. Šajā sakarā sk. arī 4., 11. un 37. lpp. Eiropas Banku iestādes 2019. gada 29. novembra Pamatnostādnēs par IKT un drošības risku pārvaldību (turpmāk – "EBI pamatnostādnes"), kurās skaidri noteikts, ka vispārējais juridiskais pamats ir Direktīvas 2013/36/ES 74. pants.

([69]) Sk. ierosinātās regulas 41. panta 1. punktu.

([70]) Sk. ierosinātās regulas 25. panta 3. un 4. punktu.

([71]) Sk. arī Kapitāla prasību direktīvas 109. pantu.

([72]) Sk. VUM regulas 4. panta 1. punktu.

([73]) Sk. Kapitāla prasību direktīvas 85. pantu.

([74]) Eiropas Centrālās bankas Regula (ES) Nr. 468/2014 (2014. gada 16. aprīlis), ar ko izveido Vienotā uzraudzības mehānisma pamatstruktūru Eiropas Centrālās bankas sadarbībai ar nacionālajām kompetentajām un norīkotajām iestādēm (VUM pamatregula) (ECB/2014/17) (OV L 141, 14.5.2014., 1. lpp.).

([75]) Konkrēti, par kiberincidentu (konstatētu iespējamu informācijas drošības pārkāpumu, neatkarīgi no tā, vai tas ir ļaunprātīgs vai nejaušs) ir jāziņo ECB, ja ir izpildīts vismaz viens no šādiem nosacījumiem: 1) potenciālās finansiālās ietekmes apjoms ir 5 milj. euro jeb 0,1% no 1. līmeņa pamatkapitāla (*CET1*); 2) par incidentu publiski sniegta informācija, un tas varētu nodarīt nozīmīgu kaitējumu reputācijai; 3) veikta kiberincidenta eskalācija līdz galvenajam informācijas speciālistam (*CIO*) ārpus regulārās paziņojumu sniegšanas; 4) par incidentu ziņots nacionālajam *CERT*/*CSIRT*, drošības aģentūrai vai policijai; 5) uzsāktas procedūras negadījuma seku novēršanai vai darbības nepārtrauktības nodrošināšanai, vai arī ir iesniegts kiberdrošības apdrošināšanas atlīdzības pieteikums; 6) noticis juridisko vai regulatīvo prasību pārkāpums; vai 7) banka izmanto iekšējus kritērijus vai ekspertu vērtējumu (tostarp par iespējamu sistēmisku ietekmi) un nolemj informēt ECB.

ECB. ECB atbalsta Savienības likumdevēju iestāžu centienus veicināt to, ka cita starpā tiek saskaņots un racionalizēts kredītiestādēm piemērojamo noteikumu un pienākumu kopums, kas attiecas uz incidentu paziņošanu. Ņemot to vērā, ECB ir gatava vajadzības gadījumā grozīt (un, iespējams, atcelt) paziņošanas sistēmu, ja tiktu pieņemta ierosinātā regula.

4. **Īpaši apsvērumi par IKT riska pārvaldību, incidentu paziņošanu, darbības noturības testēšanu un ar trešo personu saistīto IKT risku**

4.1 *IKT riska pārvaldība*

4.1.1 ECB atzinīgi vērtē to, ka ar ierosināto regulu tiek ieviesta stabila un visaptveroša IKT riska pārvaldības sistēma, kas ietver *CPMI-IOSCO* "Norādījumus par kibernoturību" un ir cieši saskaņota ar labāko praksi, tostarp Eurosistēmas "Kibernoturības pārraudzības prognozēm attiecībā uz FTI".

4.1.2 ECB atbalsta ideju, ka finanšu vienībām būtu jāveic riska novērtējumi par katru būtisku izmaiņu tīkla un informācijas sistēmas infrastruktūrā ([76]). Ņemot vērā iepriekš minēto, ierosinātajā regulā nav "būtisku izmaiņu" definīcijas, kas rada nevēlamu iespējamību, ka finanšu vienības varētu interpretēt tās atšķirīgi, kas galu galā varētu kavēt ierosinātās regulas saskaņošanas mērķu sasniegšanu. Juridiskās noteiktības nolūkā Savienības likumdevējas iestādes varētu apsvērt "būtisku izmaiņu" definīcijas ieviešanu ierosinātajā regulā.

4.1.3 ECB kopumā atbalsta ideju, ka finanšu vienības, kas nav mikrouzņēmumi, paziņo kompetentajām iestādēm par attiecīgajām izmaksām un zaudējumiem, ko izraisījuši IKT traucējumi un ar IKT saistītie incidenti ([77]). Tomēr, lai nodrošinātu sistēmas vispārējo efektivitāti un izvairītos no iespējas, ka kompetentajām iestādēm un finanšu vienībām jāapstrādā pārāk daudz ziņojumu, Savienības likumdevējām iestādēm būtu lietderīgi izpētīt iespēju ieviest attiecīgas robežvērtības, kas, iespējams, būtu kvantitatīvas.

4.1.4 ECB atzīst, ka pēc kompetento iestāžu apstiprinājuma finanšu vienības varētu deleģēt IKT riska pārvaldības prasību izpildes pārbaudes uzdevumus grupas iekšienē vai ārējiem uzņēmumiem ([78]). Vienlaikus ir svarīgi, lai Savienības likumdevējas iestādes precizētu, kā kompetento iestāžu apstiprinājums tiktu piešķirts gadījumos, ja finanšu vienība ir pakļauta vairākām kompetentajām iestādēm. Tas varētu notikt, ja finanšu vienība ir kredītiestāde, kriptoaktīvu pakalpojumu sniedzējs un/vai maksājumu pakalpojumu sniedzējs. Visbeidzot, attiecībā uz finanšu vienību identificēšanu un klasifikāciju, kas jāveic saskaņā ar ierosināto regulu ([79]), ECB uzskata, ka ierosinātajā regulā aktīvu klasifikācijas nolūkā būtu pamatoti prasīt finanšu vienībām ņemt vērā šādu aktīvu kritisko svarīgumu (proti, vai tie vajadzīgi kritiski svarīgām funkcijām).

4.2 *Incidentu paziņošana*

4.2.1 ECB atzinīgi vērtē ierosinātajā regulā izklāstītos centienus saskaņot IKT incidentu paziņošanas vidi Savienībā un strādāt pie tā, lai par būtiskiem ar IKT saistītiem incidentiem paziņotu centralizēti ([80]). Saskaņotas sistēmas ieviešana paziņošanai attiecīgajām kompetentajām iestādēm par būtiskiem ar IKT saistītiem incidentiem ([81]) principā racionalizētu un saskaņotu finanšu vienību, tostarp kredītiestāžu, paziņošanas pienākumu apjomu. Kompetentās iestādes gūtu labumu no plašākā incidentu tvēruma, kas neaprobežotos tikai ar kiberincidentiem, uz kuriem pašlaik attiecas spēkā esošās sistēmas ([82]). Lai nākotnē pieņemtu ierosināto regulu, būtu jāpārskata un, iespējams, jāatceļ spēkā esošās sistēmas, tostarp VUM kiberincidentu paziņošanas sistēma. Ņemot to vērā, lai panāktu patiesu racionalizēšanu un pilnīgu saskaņošanu visās sistēmās, ir ļoti svarīgi nodrošināt, ka ierosinātās regulas noteikumu, kas attiecas uz incidentu paziņošanu, darbības joma, tostarp visas attiecīgās definīcijas, robežvērtības un ziņošanas parametri, tiek pilnībā saskaņota ar attiecīgajām sistēmām. Jo īpaši ir ārkārtīgi svarīgi nodrošināt saskaņotību starp

([76]) Sk. ierosinātās regulas 7. panta 3. punktu.
([77]) Sk. ierosinātās regulas 10. panta 9. punktu.
([78]) Sk. ierosinātās regulas 5. panta 10. punktu.
([79]) Sk. ierosinātās regulas 7. pantu.
([80]) Sk. ierosinātās regulas 19. pantu.
([81]) Sk. ierosinātās regulas 3. panta 7. punktu, 17. pantu un 18. pantu.
([82]) Sk., piemēram, paziņošanas sistēmu.

ierosināto regulu, no vienas puses, un Eiropas Parlamenta un Padomes Direktīvu (ES) 2015/2366 ([83]) (turpmāk – "MPD2") un EBI Pamatnostādnēm par būtisku incidentu paziņošanu (turpmāk – "EBI pamatnostādnes"). Ierosinātajā grozījumu direktīvā ([84]) ir ietverti grozījumi MPD2, ar ko nošķir incidentu paziņošanu saskaņā ar ierosināto regulu un MPD2, kas galvenokārt ietekmētu maksājumu pakalpojumu sniedzējus, kuriem varētu būt arī kredītiestādes licence, kā arī kompetentās iestādes. Trūkst skaidrības par incidentu paziņošanas procesu, un pastāv pārklāšanās iespējamība attiecībā uz dažiem incidentiem, par kuriem jāpaziņo saskaņā ar ierosināto regulu un EBI pamatnostādnēm.

4.2.2 Procesi, kurus izmanto paziņošanai par būtiskiem incidentiem saskaņā ar attiecīgi ierosināto regulu ([85]), MPD2 un attiecīgajām EBI pamatnostādnēm, paredz, ka maksājumu pakalpojumu sniedzējiem jāiesniedz incidenta ziņojums savai attiecīgajai kompetentajai iestādei, tiklīdz incidents ir klasificēts. Sākotnējie ziņojumi faktiski neatspoguļo incidenta būtību, cēloni vai funkcionālo jomu, un maksājumu pakalpojumu sniedzēji var noteikt atšķirības tikai vēlāk, kad kļūst pieejama sīkāka informācija par incidentu. Rezultātā sākotnējos ziņojumus par incidentiem varētu iesniegt gan saskaņā ar ierosināto regulu, gan saskaņā ar EBI pamatnostādnēm, vai arī maksājumu pakalpojumu sniedzēji var nolemt lietot vienotu paziņošanas sistēmu un labot iesniegtos datus vēlāk. Tāda pati nenoteiktība (piemēram, attiecībā uz jebkura incidenta pamatcēloni) varētu atspoguļoties arī starpposma un nobeiguma ziņojumos. Arī tas palielinātu iespējamību, ka vienlaikus iesniedz ziņojumus kompetentajām iestādēm gan saskaņā ar ierosināto regulu, gan arī saskaņā ar MPD2.

4.2.3 Daži incidenti, kuri var tikt klasificēti kā ar IKT saistīti incidenti, var ietekmēt arī citas jomas, un tāpēc par tiem būtu jāziņo saskaņā ar EBI pamatnostādnēm. Tā tas var būt gadījumos, kad incidentam ir ietekme no IKT viedokļa, bet vienlaikus tas ir ietekmējis arī tiešu maksājumu pakalpojumu sniegšanu un/vai citas ar IKT nesaistītas funkcionālas jomas vai kanālus. Turklāt varētu būt gadījumi, kad nav iespējams nošķirt darbības incidentus un ar IKT saistītos incidentus. Turklāt gadījumā, ja viena un tā pati finanšu vienība ir nozīmīga kredītiestāde un maksājumu pakalpojumu sniedzējs, saskaņā ar ierosināto regulu vienai un tai pašai vienībai būtu divreiz jāziņo par ar IKT saistītu incidentu, jo tas būtu divu kompetento iestāžu kompetencē. Ņemot vērā iepriekš minēto, ierosinātajā regulā būtu skaidrāk jānosaka, kā MPD2 un EBI pamatnostādņu mijiedarbībai ir jādarbojas praksē. Turklāt ziņošanas pienākumu saskaņošanas un racionalizēšanas nolūkā būtu svarīgi, lai Savienības likumdevējas iestādes apsvērtu atlikušos divkāršās ziņošanas aspektus un precizētu, vai ierosinātā regula, no vienas puses, un MPD2 un EBI pamatnostādnes, no otras puses, pastāvētu paralēli, jeb tomēr vajadzētu pastāvēt vienotam prasību kopumam ziņošanai par incidentiem.

4.2.4. Ar ierosināto regulu tiek ieviesta prasība kompetentajām iestādēm ([86]) pēc paziņojuma saņemšanas apstiprināt paziņojuma saņemšanu un pēc iespējas ātrāk sniegt finanšu vienībai visas vajadzīgās atgriezeniskās saites vai norādījumus, jo īpaši, lai apspriestu korektīvos pasākumus vienības līmenī vai veidus, kā mazināt negatīvo ietekmi visās nozarēs. Tas nozīmētu, ka kompetentajām iestādēm būtu aktīvi jāpiedalās incidentu pārvaldībā un koriģējošajos pasākumos, vienlaikus novērtējot arī uzraudzītās struktūras reakciju uz kritiskiem incidentiem. ECB uzsver, ka par koriģējošiem pasākumiem būtu jāatbild, tie būtu jāīsteno un par incidenta sekām būtu jāatbild vienīgi attiecīgajai finanšu vienībai. Tāpēc ECB ierosina ierobežot atgriezenisko saiti un norādījumus, paredzot tikai augsta līmeņa prudenciālo atgriezenisko saiti un norādījumus. Ja atgriezeniskā saites saturs būtu plašāks, būtu vajadzīgi tādi specializēti profesionāļi ar ļoti ievērojamām tehniskām zināšanām, kādi parasti nav pieejami uzraudzības iestādēm pieejamajā talantu rezervē.

4.3 *Digitālās darbības noturības testēšana*

4.3.1 ECB atzinīgi vērtē prasības, kas ierosinātajā regulā ([87]) noteiktas attiecībā uz digitālās darbības noturības testēšanu finanšu vienībās, un to, ka katrai iestādei ir pašai sava testēšanas programma. Ierosinātajā regulā ([88]) norādītas dažādu veidu pārbaudes, kas īpaši attiecas uz finanšu vienībām. Testu veidi nav pārāk skaidri, un dažus testus, piemēram, saderības testus, anketas vai uz scenāriju balstītus testus, var interpretēt EUI, kompetentās iestādes vai

([83]) Eiropas Parlamenta un Padomes Direktīva (ES) 2015/2366 (2015. gada 25. novembris) par maksājumu pakalpojumiem iekšējā tirgū, ar ko groza Direktīvas 2002/65/EK, 2009/110/EK un 2013/36/ES un Regulu (ES) Nr. 1093/2010 un atceļ Direktīvu 2007/64/EK (OV L 337, 23.12.2015., 35. lpp.).

([84]) Sk. ierosinātās grozījumu direktīvas 7. panta 9. punktu.

([85]) Sk. ierosinātās regulas 17. panta 3. punktu.

([86]) Sk. ierosinātās regulas 20. pantu.

([87]) Sk. ierosinātās regulas 21. un 22. pantu.

([88]) Sk. ierosinātās regulas 22. panta 1. punktu.

finanšu vienības. Turklāt nav arī norādījumu par katra testa biežumu. Iespējamā pieeja varētu būt tāda, ka ierosinātajā regulā būtu izklāstītas vispārīgas testēšanas prasības, precīzāku testu veidu aprakstus nosakot regulatīvajos un īstenošanas tehniskajos standartos.

4.3.2 Draudu vadīti ielaušanās testi (DVIT) ir spēcīgs instruments drošības aizsardzības un sagatavotības testēšanai. Tāpēc ECB mudina finanšu vienības veikt DVIT. Ar šo rīku tiek pārbaudīti ne tikai tehniskie pasākumi, bet arī darbinieki un procesi. Šo testu rezultāti var ievērojami uzlabot pārbaudāmo struktūru augstākā līmeņa vadības informētību par drošību. Eiropas sistēma ētiskai ielaušanās simulācijai apdraudējuma izlūkošanas nolūkos (*European Framework for Threat Intelligence Based Ethical Red-teaming*; *TIBER-EU*) ([89]) un citi DVIT rīki, kas jau ir pieejami ārpus Eiropas Savienības, ir galvenie instrumenti, ar kuriem finanšu vienības pašas var novērtēt, testēt, praktizēt un uzlabot savu stāvokli un aizsardzību kibernoturības jomā.

4.3.3 Lielākajā daļā dalībvalstu, kurās ir īstenota *TIBER-EU*, pārraudzības un uzraudzības iestādes nav aktīvas dalībnieces lokalizēto *TIBER-XX* programmu īstenošanā, un *TIBER* kiberkomanda (*TIBER Cyber Team*; *TCT*) gandrīz visos gadījumos ir nošķirta no pārraudzības un uzraudzības funkciju izpildes. Šā iemesla dēļ padziļināta testēšana saskaņā ar ierosināto regulu ([90]), izmantojot DVIT, būtu jāīsteno kā instruments finanšu ekosistēmas stiprināšanai un finanšu stabilitātes uzlabošanai, nevis tikai kā uzraudzības instruments. Turklāt nav nepieciešams izstrādāt jaunu padziļinātas kibernoturības testēšanas sistēmu, jo dalībvalstis jau ir plaši pieņēmušas *TIBER-EU*, kas pašlaik ir vienīgā šāda sistēma ES.

4.3.4 Prasības testētājiem nevajadzētu iekļaut ierosinātās regulas pamattekstā, jo ar DVIT saistītā nozare joprojām attīstās, un konkrētas prasības var kavēt inovāciju. Ņemot to vērā, ECB uzskata, ka, lai nodrošinātu lielā mērā neatkarīgu testēšanu, finanšu vienībām nevajadzētu nodarbināt vai nolīgt tādas testētāju struktūras, kuras nodarbina vai nolīgst citas finanšu vienības attiecīgās finanšu vienības grupā vai kuras citādi pieder pārbaudāmajām finanšu vienībām un/vai kuras kontrolē attiecīgā finanšu vienība.

4.3.5 Lai samazinātu sadrumstalotības risku un nodrošinātu saskaņotību, ar ierosināto regulu būtu jānosaka viena DVIT sistēma, kas piemērojama finanšu sektoram visā Savienībā. Sadrumstalotība var izraisīt izmaksu pieaugumu, kā arī tehnisko, darbības un finanšu resursu vajadzību pieaugumu gan kompetentajām iestādēm, gan finanšu vienībām. Šīs pieaugošās izmaksas un prasības galu galā var negatīvi ietekmēt testu savstarpējo atzīšanu. Šis saskaņotības trūkums un no tā izrietošās problēmas saistībā ar savstarpēju atzīšanu ir īpaši svarīgas finanšu vienībām, kurām var būt vairākas licences un/vai kuras var darboties vairākās jurisdikcijās visā Savienībā. Regulatīvos un īstenošanas tehniskos standartus, kas jāizstrādā DVIT vajadzībām saskaņā ar ierosināto regulu, vajadzētu saskaņot ar *TIBER-EU*. Turklāt ECB atzinīgi vērtē iespēju sadarbībā ar EUI iesaistīties šo regulatīvo un īstenošanas tehnisko standartu sagatavošanā.

4.3.6 Kompetento iestāžu aktīva iesaistīšanās testos varētu radīt potenciālu interešu konfliktu ar citu funkciju, ko tās pilda, proti, ar finanšu vienības testēšanas sistēmas novērtēšanu. Ņemot vērā iepriekš minēto, ECB ierosina ierosinātajā regulā svītrot jebkādu kompetento iestāžu pienākumu apstiprināt dokumentus un izsniegt DVIT testa apliecinājumus.

4.4 Ar trešo personu saistīts IKT risks

4.4.1 ECB atzinīgi vērtē visaptveroša galveno principu kopuma un stabilas pārraudzības sistēmas ieviešanu tādu IKT risku identificēšanai un pārvaldībai, ko rada trešās personas, kas sniedz IKT pakalpojumus, neatkarīgi no tā, vai tās pieder vienai un tai pašai finanšu vienību grupai. Ņemot vērā iepriekš minēto, lai panāktu efektīvu IKT risku apzināšanu un pārvaldību, ir svarīgi pareizi identificēt un klasificēt cita starpā kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus. Šajā sakarā, lai gan ir atzinīgi vērtējama tādu deleģēto aktu ([91]) ieviešana, kas papildinās klasifikācijas vajadzībām izmantojamos kritērijus ([92]), pirms šādu deleģēto aktu pieņemšanas būtu jāapspriežas ar ECB.

([89]) Pieejama ECB interneta vietnē www.ecb.europa.eu.
([90]) Sk. ierosinātās regulas 23. un 24. pantu.
([91]) Sk. ierosinātās regulas 28. panta 3. punktu.
([92]) Sk. ierosinātās regulas 28. panta 2. punktu.

4.4.2 Attiecībā uz pārraudzības sistēmas struktūru ([93]) ir nepieciešams sīkāks skaidrojums par lomu, kas jāuzņemas Apvienotajai komitejai. Vienlaikus ECB atzinīgi vērtē tās iekļaušanu Pārraudzības forumā kā novērotāju, jo šī loma nodrošinās ECB tādu pašu piekļuvi dokumentācijai un informācijai kā balsstiesīgajiem locekļiem ([94]). ECB vēlas vērst Savienības likumdevēju iestāžu uzmanību uz to, ka ECB kā novērotāja sniegtu ieguldījumu Pārraudzības foruma darbā gan kā emisijas centrālā banka, kas atbild par tirgus infrastruktūru uzraudzību, gan kā kredītiestāžu prudenciālās uzraudzības iestāde. Turklāt ECB atzīmē, ka ECB kā kompetentā iestāde ne tikai būs novērotāja Pārraudzības forumā, bet arī piedalīsies kopīgajā pārbaudes grupā. Šajā sakarā Savienības likumdevējas iestādes varētu turpināt apsvērt kopīgo pārbaudes grupu sastāvu ([95]), lai nodrošinātu pienācīgu attiecīgo kompetento iestāžu iesaisti. Tāpat ECB uzskata, ka būtu jāpalielina maksimālais dalībnieku skaits kopīgajās pārbaudes grupās, ņemot vērā trešo personu sniegto IKT pakalpojumu kritisko svarīgumu, sarežģītību un darbības jomu.

4.4.3 ECB norāda, ka saskaņā ar ierosināto regulu vadošais pārraugs var liegt kritiski svarīgām trešajām personām, kas sniedz IKT pakalpojumus, slēgt tālākus apakšuzņēmuma līgumus, ja i) paredzētais apakšuzņēmējs ir trešā valstī reģistrēta trešā persona, kas sniedz IKT pakalpojumus, vai trešā valstī reģistrēts IKT apakšuzņēmējs, un ii) apakšuzņēmuma līgums attiecas uz kritiski svarīgu vai svarīgu finanšu vienības funkciju. ECB vēlas uzsvērt, ka šīs pilnvaras vadošais pārraugs var īstenot tikai saistībā ar apakšuzņēmuma līgumu slēgšanu, ja kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus, slēdz apakšuzņēmuma līgumu par kritiski svarīgas vai svarīgas funkcijas izpildi ar atsevišķu juridisku personu, kas reģistrēta trešā valstī. ECB saprot, ka vadošais pārraugs nevarētu īstenot līdzvērtīgas pilnvaras, lai nepieļautu, ka kritiski svarīga trešā persona, kas sniedz IKT pakalpojumus, finanšu vienības kritiski svarīgo vai svarīgo funkcijas izpildi nodod ārpakalpojumu sniedzējam, kas atrodas trešā valstī. Šāds gadījums varētu būt, piemēram, ja no darbības viedokļa kritiski svarīgus datus un/vai informāciju glabātu vai apstrādātu iekārtās, kas atrodas ārpus Eiropas Ekonomikas zonas (EEZ). Šādā gadījumā vadošā pārrauga pilnvaras nebūtu pietiekošas, lai pilnvarotu kompetentās iestādes piekļūt visai informācijai, telpām, infrastruktūrai un personālam, kas saistīti ar visu kritiski svarīgo vai svarīgo finanšu vienības funkciju veikšanu. Lai nodrošinātu, ka kompetentās iestādes spēj netraucēti veikt savus uzdevumus, ECB ierosina piešķirt vadošajam pārraugam pilnvaras ierobežot arī to, ka kritiski svarīgas trešās personas, kas sniedz IKT pakalpojumus, izmanto iekārtas, kuras atrodas ārpus EEZ. Šīs pilnvaras varētu īstenot konkrētos gadījumos, kad nav noslēgtas administratīvas vienošanās ar attiecīgajām trešo valstu iestādēm, kā paredzēts ierosinātajā regulā ([96]), vai kritiski svarīgu trešo personu, kas sniedz IKT pakalpojumus, pārstāvji nesniedz pietiekamus apliecinājumus attiecīgās trešās valsts sistēmas ietvaros par piekļuvi informācijai, telpām, infrastruktūrai un personālam, kas ir nepieciešams pārraudzības vai uzraudzības uzdevumu veikšanai.

4.4.4 Visbeidzot, prasība kompetentajām iestādēm ievērot vadošā pārrauga ieteikumus ([97]) varētu izrādīties neefektīva, jo kompetentajām iestādēm var nebūt visaptverošas izpratnes par riskiem, ko rada katra kritiski svarīgā trešā persona, kas sniedz IKT pakalpojumus. Turklāt kompetentajām iestādēm var būt vajadzīgs vērsties pret to uzraudzītajām finanšu vienībām, ja kritiski svarīgās trešās personas, kas sniedz IKT pakalpojumus, nav ņēmušas vērā ieteikumus. Saskaņā ar ierosināto regulu ([98]) kompetentās iestādes var noteikt to uzraudzītajām finanšu vienībām pienākumu īslaicīgi apturēt kritiski svarīgu pakalpojumu, ko sniedz trešā persona, vai izbeigt neizpildītos līgumus, kas ir noslēgti ar kritiski svarīgām trešām personām, kas sniedz pakalpojumus. Paredzēto turpmāko pasākumu procesu ir grūti pārvērst konkrētās darbībās. Konkrētāk, nav skaidrs, vai uzraudzīta finanšu vienība spēs apturēt vai izbeigt līgumu ar kritiski svarīgu trešo personu, kas sniedz pakalpojumus. Tas ir tādēļ, ka kritiski svarīgā trešā persona, kas sniedz IKT pakalpojumus, varētu būt nozīmīgs pakalpojumu sniedzējs šai finanšu vienībai, vai arī tādēļ, ka šāda apturēšana vai izbeigšana finanšu vienībai var radīt līgumiskas vai citādas izmaksas un zaudējumus. Turklāt šī pieeja neveicina pārraudzības konverģenci, jo kompetentās iestādes vienu un to pašu ieteikumu var interpretēt atšķirīgi. Tas galu galā varētu kavēt paredzēto saskaņošanu un vienotas pieejas izmantošanu, uzraugot kritiski svarīgo ar trešo personu saistīto IKT risku Savienības mērogā. Ņemot vērā iepriekš minēto, Savienības likumdevējas iestādes varētu apsvērt iespēju piešķirt juridiskajiem pārraugiem īpašas izpildes nodrošināšanas pilnvaras attiecībā uz kritiski svarīgām trešajām personām, kas sniedz IKT pakalpojumus, ņemot vērā Meroni doktrīnas noteiktos ierobežojumus, ko Tiesa daļēji mīkstināja savā spriedumā EVTI lietā ([99]).

([93]) Sk. ierosinātās regulas 29. pantu.
([94]) Sk. ierosinātās regulas 29. panta 3. punktu.
([95]) Sk. ierosinātās regulas 35. pantu.
([96]) Sk. ierosinātās regulas 39. panta 1. punktu.
([97]) Sk. ierosinātās regulas 29. panta 4. punktu un 37. pantu.
([98]) Sk. ierosinātās regulas 37. panta 3. punktu.
([99]) Sk. Tiesas spriedumu (virspalāta), 2014. gada 22. janvāris, Lielbritānijas un Ziemeļīrijas Apvienotā Karaliste/Eiropas Parlaments un Eiropas Savienības Padome, Regula (ES) Nr. 236/2012, C-270/12.

Gadījumos, kuros ECB iesaka grozīt ierosināto regulu, konkrēti redakcionālie priekšlikumi ir izklāstīti atsevišķā tehniskā darba dokumentā, kuram pievienots attiecīgs paskaidrojuma teksts. Tehniskais darba dokuments angļu valodā ir pieejams *EUR-Lex*.

Frankfurtē pie Mainas, 2021. gada 4. jūnijā

ECB prezidente
Christine LAGARDE