III

(Přípravné akty)

EVROPSKÁ CENTRÁLNÍ BANKA

STANOVISKO EVROPSKÉ CENTRÁLNÍ BANKY

ze dne 4. června 2021

k návrhu nařízení Evropského parlamentu a Rady o digitální provozní odolnosti finančního sektoru

(CON/2021/20)

(2021/C 343/01)

Úvod a právní základ

Evropská centrální banka (ECB) obdržela dne 22., 23. a 29 prosince 2020 žádosti Rady Evropské unie a Evropského parlamentu o stanovisko k návrhu nařízení Evropského parlamentu a Rady o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014 a (EU) č. 909/2014 ([1]) (dále jen „navrhované nařízení") a k návrhu směrnice, kterou se mění směrnice 2006/43/ES, 2009/65/ES, 2009/138/ES, 2011/61/EU, 2013/36/EU, 2014/65/EU, (EU) 2015/2366 a (EU) 2016/2341 ([2]) (dále jen „navrhovaná pozměňující směrnice", společně spolu s „navrhovaným nařízením" dále jen „navrhované akty").

Pravomoc ECB zaujmout stanovisko je založena na čl. 127 odst. 4 a čl. 282 odst. 5 Smlouvy o fungování Evropské unie, neboť navrhované akty obsahují ustanovení, která spadají do oblasti působnosti ECB; konkrétně jde o vymezení a provádění měnové politiky, podporu plynulého fungování platebních systémů, příspěvek k řádnému provádění opatření, která příslušné orgány přijímají v oblasti stability systému finančního trhu, a úkoly ECB, které se týkají obezřetnostního dohledu nad úvěrovými institucemi podle čl. 127 odst. 2 první a čtvrté odrážky, čl. 127 odst. 5 a čl. 127 odst. 6 Smlouvy. V souladu s čl. 17.5 první větou jednacího řádu Evropské centrální banky přijala toto stanovisko Rada guvernérů.

1. Obecné připomínky

1.1 ECB vítá navrhované nařízení, jehož cílem je posílit kybernetickou bezpečnost a provozní odolnost finančního sektoru. ECB vítá zejména cíl navrhovaného nařízení, kterým je odstranit překážky a zlepšit vytváření a fungování vnitřního trhu s finančními službami harmonizací pravidel pro řízení rizik v oblasti informačních a komunikačních technologií (IKT) a pro hlášení, testování a rizika v oblasti IKT spojená s třetími stranami. ECB dále vítá cíl navrhovaného nařízení zjednodušit a harmonizovat veškeré překrývající se regulační požadavky nebo očekávání v oblasti dohledu, jimž v současné době podle práva Unie podléhají finanční subjekty.

1.2 ECB vychází z toho, že navrhované nařízení ve vztahu k finančním subjektům určeným jako provozovatelé základních služeb ([3]) představuje odvětvový právní akt (lex specialis) ve smyslu vymezeném v čl. 1 odst. 7 směrnice Evropského paramentu a Rady (EU) 2016/1148 ([4])(dále jen „směrnice o bezpečnosti sítí a informací"); to znamená, že požadavky podle navrhovaného nařízení by zásadně měly mít přednost před směrnicí o bezpečnosti sítí a informací. V praxi by finanční subjekty určené jako provozovatelé základních služeb ([5]) mimo jiné hlásily incidenty podle navrhovaného nařízení, a nikoli podle směrnice o bezpečnosti sítí

([1]) COM(2020) 595 final.
([2]) COM(2020) 596 final.
([3]) Viz čl. 1 odst. 2 navrhovaného nařízení.
([4]) Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Úř. věst. L 194, 19.7.2016, s. 1).
([5]) Viz článek 5 směrnice o bezpečnosti sítí a informací.

a informací. Přestože ECB vítá snížení případných překrývajících se požadavků na finanční subjekty v oblasti hlášení incidentů, je třeba dále zvážit otázku interakce mezi navrhovaným nařízením a směrnicí o bezpečnosti sítí a informací. Podle navrhovaného nařízení by se například na poskytovatele služeb IKT z řad třetích stran ([6]) mohla vztahovat doporučení vydaná hlavním orgánem dohledu ([7]). Zároveň může být tentýž poskytovatel služeb IKT z řad třetích stran klasifikován jako provozovatel základních služeb podle směrnice o bezpečnosti sítí a informací a může podléhat závazným pokynům vydaným příslušným orgánem ([8]). V takovém případě by poskytovatel služeb IKT z řad třetích stran mohl podléhat protichůdným doporučením vydaným podle navrhovaného nařízení a závazným pokynům vydaným podle směrnice o bezpečnosti sítí a informací. ECB navrhuje, aby legislativní orgány Unie dále zvážily možné nesrovnalosti mezi navrhovaným nařízením a směrnicí o bezpečnosti sítí a informací, které by mohly bránit harmonizaci a omezení překrývajících se a protichůdných požadavků na finanční subjekty.

1.3 ECB rovněž vychází z toho, že podle návrhu směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148 ([9]) (dále jen „navrhovaná směrnice o bezpečnosti sítí a informací 2“) budou „případy, kdy téměř došlo k incidentu“ ([10]) podléhat oznamovací povinnosti ([11]). I když se v 39. bodě odůvodnění navrhované směrnice o bezpečnosti sítí a informací 2 uvádí význam pojmu „případy, kdy téměř došlo k incidentu“, není jasné, zda je záměrem požadovat, aby případy, kdy téměř došlo k incidentu, hlásily finanční subjekty uvedené v článku 2 navrhovaného nařízení. V tomto ohledu a také s ohledem na skutečnost, že případy, kdy téměř došlo k incidentu, mohou být jako takové identifikovány až poté, co k nim došlo, by ECB uvítala, aby byla o významných případech, kdy téměř došlo k incidentu, včas vyrozuměna, jak je tomu v současné době v případě kybernetických incidentů. ECB navrhuje zvýšit soulad mezi navrhovaným nařízením a navrhovanou směrnicí o bezpečnosti sítí a informací 2, aby se vyjasnil přesný rozsah vykazování, kterému může kterýkoli finanční subjekt podléhat na základě těchto dvou odlišných, avšak propojených právních předpisů Unie. Zároveň by bylo třeba definovat „případy, kdy téměř došlo k incidentu,“ a vypracovat ustanovení objasňující jejich význam.

1.4 ECB vítá, že jsou finanční subjekty motivovány k tomu, aby mezi sebou dobrovolně sdílely zpravodajské informace o kybernetických hrozbách s cílem zlepšit a posílit jejich postavení v oblasti kybernetické odolnosti. ECB sama napomáhala při vytváření Iniciativy pro sdílení informací o kybernetických hrozbách (CIISI-EU), která vzešla z potřeb trhu, a s cílem vytvořit a podpořit tuto iniciativu zpřístupnila příslušné návrhy ([12]).

1.5 ECB podporuje spolupráci mezi příslušnými orgány pro účely navrhovaného nařízení, evropskými orgány dohledu a skupinami pro reakci na počítačové bezpečnostní incidenty (CSIRTS) ([13]). Výměna informací má zásadní význam pro zajištění provozní odolnosti Unie, neboť sdílení informací a spolupráce mezi orgány mohou přispět k předcházení kybernetickým útokům a pomoci omezit šíření hrozeb v oblasti IKT. Mělo by být podporováno společné chápání rizik souvisejících s IKT a mělo by být zajištěno jednotné posuzování těchto rizik v celé Unii. Je nanejvýš důležité, aby příslušné orgány sdílely informace s jednotným kontaktním místem ([14]) a vnitrostátním CSIRTS ([15]) pouze v případě, že existují jasně stanovené systémy pro klasifikaci a sdílení informací doplněné odpovídajícími zárukami pro zajištění důvěrnosti.

1.6 V neposlední řadě by ECB uvítala, kdyby byla v navrhovaném nařízení zavedena pravidla týkající se osobních údajů a uchovávání údajů. Délka doby uchovávání údajů by měla zohledňovat vyšetřování, kontrolu, žádost o informace, sdělení, zveřejnění, hodnocení, ověřování, posuzování a vypracovávání plánů dozoru nebo dohledu, které mohou příslušné orgány provádět v rámci svých příslušných povinností a úkolů podle navrhovaného nařízení. V tomto ohledu by byla přiměřená doba uchovávání údajů v délce 15 let. Tato doba

([6]) Viz čl. 3 odst. 15 navrhovaného nařízení.
([7]) Viz čl. 31 odst. 1 písm. d) navrhovaného nařízení.
([8]) Viz čl. 15 odst. 3 směrnice o bezpečnosti sítí a informací.
([9]) COM(2020) 823 final.
([10]) Události, které by mohly potenciálně způsobit škodu, ale jejímu plnému projevení bylo úspěšně zabráněno, viz 39. bod odůvodnění směrnice o bezpečnosti sítí a informací 2.
([11]) Viz článek 11 směrnice o bezpečnosti sítí a informací 2.
([12]) Cyber threat Intelligence Information Sharing Initiative (CIISI-EU), která je k dispozici na internetových stránkách ECB www.ecb.europa.eu.
([13]) Viz článek 42 navrhovaného nařízení.
([14]) Viz čl. 8 odst. 3 směrnice o bezpečnosti sítí a informací.
([15]) Viz rovněž články 11, 26 a 27 směrnice o bezpečnosti sítí a informací 2.

uchovávání údajů by mohla být v konkrétních případech zkrácena nebo prodloužena. V tomto ohledu ECB navrhuje, aby legislativní orgány Unie při formulování příslušného ustanovení o osobních údajích a uchovávání údajů rovněž zohlednily zásadu minimalizace údajů, jakož i další zpracování pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely ([16]).

2. **Zvláštní připomínky k dozoru a zúčtování a vypořádání obchodů s cennými papíry**

2.1 *Pravomoci ESCB a Eurosystému v oblasti dozoru*

2.1.1 Smlouva a statut Evropského systému centrálních bank a Evropské centrální banky (dále jen „statut ESCB“) s ohledem na úzké spojení se základními úkoly měnové politiky stanoví, že Eurosystém provádí dozor nad zúčtovacími a platebními systémy. Čtvrtá odrážka čl. 127 odst. 2 Smlouvy a shodně článek 3.1 statutu ESCB stanoví, že jedním ze základních úkolů, jež má plnit Evropský systém centrálních bank (ESCB), je podpora plynulého fungování platebních systémů. Při plnění tohoto základního úkolu ECB a národní centrální banky mohou poskytovat facility a ECB může vydávat nařízení proto, aby byly zajištěny účinné a spolehlivé zúčtovací a platební mechanismy uvnitř Unie a ve styku se třetími zeměmi ([17]). V souladu se svou úlohou v oblasti dozoru přijala ECB nařízení Evropské centrální banky (EU) č. 795/2014 (ECB/2014/28) (dále jen „nařízení o SIPS“) ([18]). Nařízení o SIPS prostřednictvím svých norem provádí zásady pro infrastruktury finančního trhu vydané Výborem pro platební a zúčtovací systémy (CPSS) a Mezinárodní organizací komisí pro cenné papíry (IOSCO) v dubnu 2012 ([19]) (dále jen „zásady CPSS-IOSCO“), které jsou právně závazné a vztahují se na systémově významné platební systémy pro velké i malé platby, provozované buď centrální bankou Eurosystému, nebo soukromým subjektem. Rámec politiky Eurosystému v oblasti dozoru ([20]) označuje platební prostředky za „nedílnou součást platebních systémů“, a proto je zahrnuje do rozsahu svého dozoru. Rámec dozoru nad platebními prostředky je v současné době předmětem přezkumu ([21]). V tomto rámci je platební prostředek (např. karta, úhrada, inkaso, převod elektronických peněz a digitální platební token ([22])) definován jako personalizované zařízení (nebo soubor zařízení) a/nebo soubor postupů dohodnutých mezi uživatelem platebních služeb a poskytovatelem platebních služeb, jež se používají k iniciování převodu hodnoty ([23]).

2.1.2 S ohledem na výše uvedené ECB vítá, že z oblasti působnosti navrhovaného nařízení byli vyňati provozovatelé systémů ve smyslu čl. 2 písm. p) směrnice Evropského parlamentu a Rady 98/26/ES ([24]), platební systémy (včetně těch, které jsou provozovány centrálními bankami), platební schémata a platební mechanismy

([16]) Viz čl. 4 písm. b) a článek 13 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39).

([17]) Viz článek 22 statutu ESCB.

([18]) Nařízení Evropské centrální banky (EU) č. 795/2014 ze dne 3. července 2014 o požadavcích v oblasti dozoru nad systémově významnými platebními systémy (ECB/2014/28) (Úř. věst. L 217, 23.7.2014, s. 16).

([19]) K dispozici na internetových stránkách Banky pro mezinárodní platby www.bis.org.

([20]) Dokument s názvem „Eurosystem oversight policy framework, Revised version (July 2016)“, který je k dispozici na internetových stránkách ECB na adrese www.ecb.europa.eu.

([21]) Viz revidovaný a konsolidovaný rámec „Eurosystem oversight framework for electronic payment instruments, schemes and arrangements“ z října 2020 (rámec PISA), který je k dispozici na internetových stránkách ECB na adrese www.ecb.europa.eu.

([22]) Digitální platební token je digitální vyjádření hodnoty zajištěné pohledávkami nebo aktivy zaznamenanými jinde, které umožňuje převod hodnoty mezi koncovými uživateli. V závislosti na příslušné koncepci mohou digitální platební tokeny předpokládat převod hodnoty, aniž by nutně zahrnovaly ústřední třetí stranu a/nebo používaly platební účty.

([23]) „Převod hodnoty“: „Úkon, iniciovaný plátcem, jménem plátce nebo příjemcem, spočívající v převodu peněžních prostředků nebo digitálních platebních tokenů nebo uložení hotovosti na uživatelský účet nebo výběru hotovosti z uživatelského účtu, bez ohledu na jakékoli související povinnosti mezi plátcem a příjemcem. Převod se může týkat jednoho nebo více poskytovatelů platebních služeb.“ Definice „převodu hodnoty“ v rámci PISA se odchyluje od definice převodu „peněžních prostředků“ podle směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES (Úř. věst. L 337, 23.12.2015, s. 35). „Převod hodnoty“ v souvislosti s „platebním prostředkem“ definovaným v uvedené směrnici se může týkat pouze převodu „peněžních prostředků“. Podle uvedené směrnice „peněžní prostředky“ nezahrnují digitální platební tokeny, pokud tyto tokeny nelze klasifikovat jako elektronické peníze (nebo hypotetičtěji jako bezhotovostní peníze).

([24]) Směrnice Evropského parlamentu a Rady 98/26/ES ze dne 19. května 1998 o neodvolatelnosti zúčtování v platebních systémech a v systémech vypořádání obchodů s cennými papíry (Úř. věst. L 166, 11.6.1998, s. 45).

s ohledem na uplatňování výše uvedených rámců dozoru. Z těchto důvodů by pravomoci ESCB podle Smlouvy a pravomoci Eurosystému podle nařízení o SIPS měly být jednoznačně uvedeny v bodech odůvodnění navrhovaného nařízení.

2.1.3 Stejně tak ECB vítá vynětí poskytovatelů služeb IKT z řad třetích stran, kteří podléhají rámcům dozoru vytvořeným za účelem podpory úkolů uvedených v čl. 127 odst. 2 Smlouvy, z uplatňování rámce dohledu stanoveného v navrhovaném nařízení ([25]). V tomto ohledu by ECB ráda zdůraznila, že centrální banky ESCB, které jednají v rámci svých měnových funkcí ([26]), a Eurosystém při poskytování služeb prostřednictvím TARGET2, TARGET2-Securites (T2S) ([27]) a TARGET Instant Payment Settlement (TIPS) ([28]) nespadají do oblasti působnosti článku navrhovaného nařízení, ani nemohou být považovány za poskytovatele služeb IKT z řad třetích stran, a nemohou tedy být pro účely navrhovaného nařízení považovány za kriticky důležité poskytovatele služeb IKT z řad třetích stran. Eurosystém dohlíží na T2S v souvislosti se svým mandátem zajistit účinné a spolehlivé zúčtovací a platební systémy. Orgán ESMA dále objasnil, že T2S není poskytovatelem kritických služeb ([29]) ve smyslu nařízení Evropského parlamentu a Rady (EU) č. 909/2014 ([30]) (dále jen „nařízení o centrálních depozitářích“). V důsledku toho jsou organizační a provozní bezpečnost, účinnost a odolnost T2S zajištěny platným právním, regulačním a provozním rámcem a dohodnutými systémy správy a řízení T2S, a nikoli prostřednictvím nařízení o centrálních depozitářích.

2.1.4 Rámec politiky Eurosystému v oblasti dozoru ([31]) se kromě toho vztahuje na poskytovatele kritických služeb, kterým je například Společnost pro celosvětovou mezibankovní finanční telekomunikaci (Society for Worldwide Interbank Financial Telecommunication – SWIFT). SWIFT je společnost s ručením omezeným se sídlem v Belgii, která poskytuje služby bezpečného zasílání zpráv na mezinárodní úrovni. Nationale Bank van België/Banque Nationale de Belgique působí jako hlavní orgán dozoru nad SWIFT a ve spolupráci s ostatními centrálními bankami G10, včetně ECB, vykonává dozor nad SWIFT na základě ujednání o spolupráci při dozoru. Orgány dozoru skupiny G10 uznávají, že dozor se zaměřuje především na operační riziko SWIFT, neboť toto riziko se považuje za hlavní kategorii rizika, jejímž prostřednictvím by SWIFT mohl představovat systémové riziko pro finanční systém v Unii. V této souvislosti vypracovala skupina pro kolektivní dozor nad systémem SWIFT konkrétní soubor zásad a očekávání na vysoké úrovni, které se vztahují na systém SWIFT a mezi které se řadí identifikace a řízení rizik, bezpečnost informací, spolehlivost a odolnost, technologické plánování a komunikace s uživateli. Orgány dozoru skupiny G10 očekávají, že SWIFT bude dodržovat pokyny Výboru pro platební styk a tržní infrastrukturu (CPMI) a Mezinárodní organizace komisí pro cenné papíry (IOSCO) týkající se kybernetické odolnosti ([32]), jakož i další mezinárodní normy pro bezpečnost IKT, které společně jdou nad rámec požadavků stanovených v navrhovaném nařízení.

2.1.5 Nelze zaručit, že na SWIFT a možná i na další poskytovatele služeb, na něž se vztahuje rámec politiky Eurosystému v oblasti dozoru, by se jako na poskytovatele služeb IKT z řad třetích stran nemohlo vztahovat navrhované nařízení, pokud by poskytovali služby, na něž se nevztahuje čl. 127 odst. 2 Smlouvy. ECB proto velmi vítá skutečnost, že poskytovatelé služeb, na které se již vztahuje rámec politiky Eurosystému v oblasti dozoru a mezi které se řadí například systém SWIFT, jsou vyňati z oblasti působnosti rámce dohledu stanoveného v navrhovaném nařízení.

([25]) Viz čl. 28 odst. 5 navrhovaného nařízení.

([26]) Viz odstavec 1.3 stanoviska Evropské centrální banky ze dne 19. února 2021 k návrhu nařízení o trzích s kryptoaktivy a o změně směrnice (EU) 2019/1937 (CON/2021/4). Všechna stanoviska ECB jsou zveřejněna na internetových stránkách EUR-Lex.

([27]) Viz příloha IIa obecných zásad Evropské centrální banky ECB/2012/27 ze dne 5. prosince 2012 o transevropském expresním automatizovaném systému zúčtování plateb v reálném čase (TARGET2) (Úř. věst. L 30, 30.1.2013, s. 1). Obecné zásady Evropské centrální banky ECB/2012/13 ze dne 18. července 2012 o TARGET2-Securities (Úř. věst. L 215, 11.8.2012, s. 19); rozhodnutí Evropské centrální banky ECB/2011/20 ze dne 16. listopadu 2011, kterým se stanoví podrobná pravidla a postupy pro uplatňování kritérií pro přístup centrálních depozitářů cenných papírů ke službám TARGET2-Securities (Úř. věst. L 319, 2.12.2011, s. 117). Viz také rámcová smlouva T2S a kolektivní smlouva.

([28]) Viz příloha IIb obecných zásad ECB/2012/27.

([29]) Viz čl. 30 odst. 5 nařízení Evropského parlamentu a Rady (EU) č. 909/2014 ze dne 23. července 2014 o zlepšení vypořádání obchodů s cennými papíry v Evropské unii a centrálních depozitářích cenných papírů a o změně směrnic 98/26/ES a 2014/65/EU a nařízení (EU) č. 236/2012 (Úř. věst. L 257, 28.8.2014, s. 1) a článek 68 nařízení Komise v přenesené pravomoci (EU) 2017/392 ze dne 11. listopadu 2016, kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) č. 909/2014, pokud jde o regulační technické normy v oblasti povolování, dohledu a provozních požadavků kladených na centrální depozitáře cenných papírů (Úř. věst. L 65, 10.3.2017, s. 48).

([30]) Nařízení Evropského parlamentu a Rady (EU) č. 909/2014 ze dne 23. července 2014 o zlepšení vypořádání obchodů s cennými papíry v Evropské unii a centrálních depozitářích cenných papírů a o změně směrnic 98/26/ES a 2014/65/EU a nařízení (EU) č. 236/2012 (Úř. věst. L 257, 28.8.2014, s. 1).

([31]) Dokument s názvem „Eurosystem oversight policy framework, Revised version (July 2016)“, který je k dispozici na internetových stránkách ECB na adrese www.ecb.europa.eu.

([32]) K dispozici na internetových stránkách Banky pro mezinárodní platby www.bis.org.

2.2 *Pravomoci ESCB v oblasti vypořádání obchodů s cennými papíry*

2.2.1 Centrální depozitáře cenných papírů jsou infrastruktury finančního trhu, které jsou přísně regulovány a nad nimiž je vykonáván dohled ze strany různých orgánů v souladu s nařízením o centrálních depozitářích, které stanoví požadavky na vypořádání obchodů s finančními nástroji a pravidla týkající se organizace a chování centrálních depozitářů. Centrální depozitáře by kromě toho měly zohlednit pokyny CPMI-IOSCO týkající se kybernetické odolnosti, které byly uvedeny do praxe na základě Očekávání dozoru v oblasti kybernetické odolnosti pro infrastruktury finančních trhů (prosinec 2018) ([33]) . Kromě pravomocí v oblasti dohledu, které byly příslušným vnitrostátním orgánům svěřeny podle nařízení o centrálních depozitářích, jednají členové ESCB jako „relevantní orgány", přičemž jednají jakožto orgány dohledu nad systémy vypořádání obchodů s cennými papíry provozovanými centrálními depozitáři, jakožto centrální banky vydávající nejdůležitější měny, v nichž se vypořádání uskutečňuje, a jakožto centrální banky, na jejichž účtech dochází k peněžnímu vypořádání obchodů ([34]). V tomto ohledu se v 8. bodě odůvodnění nařízení o centrálních depozitářích uvádí, že toto nařízení by se mělo uplatňovat, aniž by byla dotčena povinnost ECB a národních centrálních bank zajišťovat účinnost a spolehlivost clearingových a platebních systémů v rámci Unie a v jiných zemích. V 8. bodě odůvodnění se rovněž uvádí, že nařízení o centrálních depozitářích by nemělo členům ESCB bránit v přístupu k informacím, které jsou důležité pro plnění jejich úkolů ([35]), včetně dozoru nad centrálními depozitáři a jinými infrastrukturami finančního trhu ([36]).

2.2.2 Kromě toho členové ESCB často vystupují jako zúčtovatelé pro hotovostní část obchodů s cennými papíry a Eurosystém nabízí centrálním depozitářům služby vypořádání prostřednictvím T2S. Dozor Eurosystému nad T2S souvisí s jeho mandátem zajistit účinné a spolehlivé zúčtovací a platební systémy, zatímco příslušné a relevantní orgány centrálních depozitářů usilují o zajištění plynulého fungování těchto subjektů, bezpečnosti a efektivnosti vypořádání a řádného fungování finančních trhů ve svých příslušných jurisdikcích.

2.2.3 Podle navrhovaného nařízení ([37]) se centrální banky ESCB neúčastní vypracovávání technických norem, pokud jde o specifikaci rizik v oblasti IKT. Podobně podle navrhovaného nařízení ([38]) nejsou příslušné orgány informovány o žádných incidentech souvisejících s IKT. Centrální banka ESCB by měla být i nadále zapojena ve stejné míře, jaká je v současnosti stanovena v nařízení o centrálních depozitářích, a příslušné orgány by měly být informovány o incidentech souvisejících s IKT. Eurosystém je příslušným orgánem pro všechny centrální depozitáře v eurozóně a pro několik dalších centrálních depozitářů v EU. Centrální banky ESCB by měly být informovány o incidentech souvisejících s IKT, které jsou důležité pro plnění jejich povinností, včetně dozoru nad centrálními depozitáři a jinými infrastrukturami finančního trhu. Rizika, jimž jsou centrální depozitáře vystaveny, včetně rizik v oblasti IKT, mohou ohrozit řádné fungování centrálních depozitářů. Rizika v oblasti IKT jsou proto důležitá pro příslušné orgány, jimž by měl být poskytnut úplný a podrobný přehled těchto rizik s cílem posoudit je a ovlivnit přístup centrálních depozitářů k řízení rizik. Navrhované nařízení by nemělo stanovit méně přísné požadavky, pokud jde o rizika v oblasti IKT, ve srovnání s požadavky stanovenými v nařízení o centrálních depozitářích a ve stávajících souvisejících regulačních technických normách.

2.2.4 Legislativní orgány Unie by navíc měly vyjasnit vzájemný vztah mezi navrhovaným nařízením ([39]) a regulačními technickými normami, které doplňují nařízení o centrálních depozitářích. Zejména není jasné, zda má být centrální depozitář osvobozen od povinnosti mít své vlastní sekundární místo, pokud poskytovatel služeb IKT z řad třetích stran takové místo provozuje ([40]). Pokud by byl centrální depozitář z této povinnosti provozovat sekundární místo osvobozen, není jasné, jakou právní hodnotu by tento požadavek měl. Obdobně

([33]) K dispozici na internetových stránkách ECB www.ecb.europa.eu.

([34]) Viz článek 12 nařízení (EU) č. 909/2014.

([35]) Viz rovněž článek 13 a čl. 17 odst. 4 a čl. 22 odst. 6 nařízení (EU) č. 909/2014.

([36]) Viz odstavec 7.3 stanoviska Evropské centrální banky ze dne 6. dubna 2017 k určení kritických infrastruktur pro účely bezpečnosti informačních technologií (CON/2017/10); odstavec 7.2 stanoviska Evropské centrální banky ze dne 8. listopadu 2018 k určení klíčových služeb a poskytovatelů klíčových služeb pro účely bezpečnosti sítí a informačních systémů (CON/2018/47); odstavec 3.5.2 stanoviska Evropské centrální banky ze dne 2. května 2019 k bezpečnosti sítí a informačních systémů (CON/2019/17); a odstavec 3.5.2 stanoviska Evropské centrální banky ze dne 11. listopadu 2019 k bezpečnosti sítí a informačních systémů (CON/2019/38).

([37]) Viz čl. 54 odst. 5 navrhovaného nařízení a čl. 45 odst. 7 nařízení (EU) č. 909/2014.

([38]) Viz čl. 54 odst. 4 navrhovaného nařízení a čl. 45 odst. 6 nařízení (EU) č. 909/2014.

([39]) Viz čl. 11 odst. 5 navrhovaného nařízení.

([40]) Viz čl. 78 odst. 3 nařízení Komise v přenesené pravomoci (EU) 2017/392 ze dne 11. listopadu 2016, kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) č. 909/2014, pokud jde o regulační technické normy v oblasti povolování, dohledu a provozních požadavků kladených na centrální depozitáře cenných papírů (Úř. věst. L 65, 10.3.2017, s. 48).

odkazuje navrhované nařízení ([41]) na cílovou dobu a okamžik obnovy provozu jednotlivých funkcí ([42]), zatímco příslušná regulační technická norma rozlišuje mezi kritickými funkcemi ([43]) a nejdůležitějšími operacemi ([44]) ve vztahu k době potřebné k obnovení provozu stanovené pro nejdůležitější operace centrálních depozitářů. S cílem zabránit riziku vzniku protichůdných požadavků by měly legislativní orgány Unie blíže vyjasnit a dále posoudit vzájemný vztah mezi navrhovaným nařízením a regulačními technickými normami, které doplňují nařízení o centrálních depozitářích. V neposlední řadě by mělo být vyjasněno, že výjimky udělené centrálním depozitářům provozovaným některými veřejnými subjekty podle nařízení o centrálních depozitářích ([45]) se uplatňují i podle navrhovaného nařízení.

2.3 *Pravomoci ESCB v oblasti clearingu cenných papírů*

2.3.1 Centrálním bankám ESCB jsou svěřeny pravomoci v oblasti dozoru nad ústředními protistranami. V tomto ohledu národní centrální banky Eurosystému často spolupracují s příslušnými vnitrostátními orgány ve funkcích dozoru a dohledu nad ústředními protistranami a účastní se kolegia ústřední protistrany zřízeného podle nařízení Evropského parlamentu a Rady (EU) č. 648/2012 ([46]) (dále jen „nařízení EMIR"). Příslušní členové Eurosystému ([47]) se účastní kolegií EMIR v rámci své funkce dozoru a zastupují Eurosystém jako emisní centrální banku pro ústřední protistrany, u kterých je euro jednou z nejdůležitějších měn pro finanční nástroje, u nichž se provádí clearing (a pro offshore ústřední protistrany, které provádějí clearing významného podílu finančních nástrojů v eurech). ECB je emisní centrální bankou pro ústřední protistrany mimo eurozónu.

2.3.2 Podle navrhovaného nařízení ([48]) nejsou centrální banky ESCB zapojeny do vypracovávání technických norem, pokud jde o specifikaci rizik v oblasti IKT. Navrhované nařízen ([49]) navíc neobsahuje žádný odkaz na cílovou dobu a okamžik obnovy provozu, které vyžaduje nařízení EMIR ([50]). Navrhovaný regulační rámec by neměl stanovit méně přísné požadavky, pokud jde o rizika v oblasti IKT, než ty, které platí v současné době. S cílem zajistit spolehlivý rámec řízení kontinuity provozu je proto zásadní stanovit jednoznačnou cílovou dobu a okamžik obnovy provozu. Zachování konkrétní cílové doby a okamžiku obnovy provozu je rovněž součástí zásad CPMI-IOSCO pro infrastruktury finančního trhu ([51]). Stávající ustanovení v nařízení EMIR by mělo být zachováno a navrhované nařízení by mělo být odpovídajícím způsobem upraveno. Centrální banky ESCB by měly být zapojeny do přípravy všech sekundárních právních předpisů, jakož i do dalšího vyjasnění a úvah legislativních orgánů Unie ohledně vzájemného působení navrhovaného nařízení a doplňujících regulačních technických norem, aby se zabránilo riziku vzniku protichůdných nebo překrývajících se požadavků.

3. **Zvláštní připomínky k aspektům obezřetnostního dohledu**

3.1 Nařízení (EU) č. 1024/2013 ([52]) (dále jen „nařízení o jednotném mechanismu dohledu") svěřuje ECB zvláštní úkoly týkající se obezřetnostního dohledu nad úvěrovými institucemi v eurozóně a ukládá ECB odpovědnost za účinné a konzistentní fungování jednotného mechanismu dohledu, v jehož rámci jsou mezi ECB a zúčastněné vnitrostátní příslušné orgány rozděleny konkrétní povinnosti v oblasti dohledu. ECB má zejména za úkol vydávat a odebírat povolení všem úvěrovým institucím. ECB má rovněž mimo jiné za úkol zajistit soulad s příslušnými právními předpisy Unie, které úvěrovým institucím ukládají obezřetnostní požadavky, včetně požadavku zavést spolehlivé systémy správy a řízení, jako jsou řádné postupy řízení rizik a mechanismy vnitřní kontroly ([53]). Za tímto účelem má ECB veškeré pravomoci v oblasti dohledu, aby mohla zasahovat do činnosti úvěrových institucí a které jsou

([41]) Viz čl. 11 odst. 6 navrhovaného nařízení.
([42]) Viz čl. 3 odst. 17 navrhovaného nařízení.
([43]) Viz čl. 76 odst. 2 písm. d) a e) nařízení Komise v přenesené pravomoci (EU) 2017/392.
([44]) Viz čl. 78 odst. 2 a 3 nařízení Komise v přenesené pravomoci (EU) 2017/392.
([45]) Viz čl. 1 odst. 4 nařízení (EU) č. 909/2014.
([46]) Nařízení Evropského parlamentu a Rady (EU) č. 648/2012 ze dne 4. července 2012 o OTC derivátech, ústředních protistranách a registrech obchodních údajů (Úř. věst. L 201, 27.7.2012, s. 1).
([47]) Viz čl. 18 odst. 2 písm. g) a h) nařízení EMIR.
([48]) Viz čl. 53 odst. 2 písm. b) a odst. 3 navrhovaného nařízení a čl. 34 odst. 3 nařízení EMIR.
([49]) Viz čl. 53 odst. 2 písm. a) navrhovaného nařízení.
([50]) Viz článek 34 nařízení EMIR.
([51]) Viz Zásady CPMI-IOSCO pro infrastruktury finančního trhu, které jsou k dispozici na internetových stránkách Banky pro mezinárodní platby na adrese www.bis.org.
([52]) Nařízení Rady (EU) č. 1024/2013 ze dne 15. října 2013, kterým se Evropské centrální bance svěřují zvláštní úkoly týkající se politik, které se vztahují k obezřetnostnímu dohledu nad úvěrovými institucemi (Úř. věst. L 287, 29.10.2013, s. 63).
([53]) Viz čl. 4 odst. 1 písm. e) a čl. 6 odst. 4 nařízení (EU) č. 1024/2013.

nezbytné pro výkon jejích funkcí. ECB a příslušné vnitrostátní příslušné orgány jsou tedy příslušnými orgány vykonávajícími konkrétní pravomoci obezřetnostního dohledu podle nařízení Evropského parlamentu a Rady (EU) č. 575/2013 ([54]) (dále jen „nařízení o kapitálových požadavcích“) a směrnice Evropského parlamentu a Rady 2013/36/EU ([55]) (dále jen „směrnice o kapitálových požadavcích“).

3.2 Navrhované nařízení stanoví, že jednotný soubor pravidel a systém dohledu je třeba doplnit tak, aby zahrnovaly digitální provozní odolnost a zabezpečení IKT, pomocí rozšíření mandátů orgánů finančního dohledu pověřených sledováním a ochranou finanční stability a integrity trhu ([56]). Cílem je podpořit komplexní rámec pro riziko v oblasti IKT nebo operační riziko prostřednictvím harmonizace klíčových požadavků na digitální provozní odolnost pro všechny finanční subjekty ([57]). Cílem navrhovaného nařízení je zejména konsolidovat a aktualizovat požadavky na riziko v oblasti IKT, které jsou dosud samostatně upraveny v různých právních předpisech ([58]).

3.3 Požadavky související s rizikem v oblasti IKT pro finanční sektor jsou v současné době rozloženy do řady aktů práva Unie, včetně směrnice o kapitálových požadavcích, a nástrojů tzv. měkkého práva (jako jsou pokyny EBA) a jsou rozmanité a v někdy neúplné. V některých případech bylo riziko v oblasti IKT řešeno pouze implicitně jako součást operačního rizika, zatímco v jiných případech nebylo řešeno vůbec. To by mělo být napraveno sladěním navrhovaného nařízení s těmito akty. Za tímto účelem předkládá navrhovaná pozměňující směrnice soubor změn, které se zdají být nezbytné pro zajištění právní jednoznačnosti a jednotnosti, pokud jde o uplatňování různých požadavků na digitální provozní odolnost. Změny směrnice o kapitálových požadavcích, které jsou v současné době navrhovány v navrhované pozměňující směrnici ([59]), se však týkají pouze ustanovení o pohotovostních plánech a plánech zachování provozu ([60]), neboť údajně implicitně slouží jako základ pro řešení řízení rizika v oblasti IKT.

3.4 Navrhované nařízení ([61]) dále stanoví, že finanční subjekty, včetně úvěrových institucí, musí disponovat interními řídicími a kontrolními rámci, které zajistí účinné a obezřetné řízení všech rizik v oblasti IKT. Navrhované nařízení ([62]) stanoví, že se požadavky, které jsou v něm stanoveny, uplatňují na individuálním a konsolidovaném základě; k tomu však dochází bez dostatečné koordinace s uvedenými odvětvovými právními předpisy. V neposlední řadě navrhované nařízení ([63]) stanoví, že aniž jsou dotčena ustanovení o rámci dohledu pro kritické poskytovatele služeb IKT z řad třetích stran uvedená v navrhovaném nařízení ([64]), dodržování povinností stanovených tímto nařízením zajišťuje v případě úvěrových institucí příslušný orgán stanovený v souladu s článkem 4 směrnice o kapitálových požadavcích, aniž jsou dotčeny zvláštní úkoly svěřené ECB nařízením o jednotném mechanismu dohledu.

3.5 S ohledem na výše uvedené má ECB za to, že ve vztahu k úvěrovým institucím a s výjimkou ustanovení navrhovaného nařízení týkajících se rámce dohledu nad kritickými poskytovateli služeb IKT z řad třetích stran ([65]) je záměrem navrhovaného nařízení stanovit obezřetnostní interní řídící rámec pro řízení rizika v oblasti IKT, který bude začleněn do obecného interního řídícího rámce podle směrnice o kapitálových požadavcích. Navíc vzhledem k obezřetnostní povaze navrhovaného rámce budou příslušnými orgány odpovědnými za dohled nad dodržováním povinností stanovených v navrhovaném rámci, včetně ECB, orgány odpovědné za bankovní dohled v souladu s nařízením o jednotném mechanismu dohledu.

([54]) Nařízení Evropského parlamentu a Rady (EU) č. 575/2013 ze dne 26. června 2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky a o změně nařízení (EU) č. 648/2012 (Úř. věst. L 176, 27.6.2013, s. 1).

([55]) Směrnice Evropského parlamentu a Rady 2013/36/EU ze dne 26. června 2013 o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu nad úvěrovými institucemi a investičními podniky, o změně směrnice 2002/87/ES a zrušení směrnic 2006/48/ES a 2006/49/ES (Úř. věst. L 176, 27.6.2013, s. 338).

([56]) Viz 8. bod odůvodnění navrhovaného nařízení.

([57]) Viz 11. bod odůvodnění navrhovaného nařízení.

([58]) Viz 12. bod odůvodnění navrhovaného nařízení.

([59]) Viz 4. a 5. bod odůvodnění navrhované pozměňující směrnice.

([60]) Viz článek 85 směrnice o kapitálových požadavcích.

([61]) Viz čl. 4 odst. 1 navrhovaného nařízení.

([62]) Viz čl. 25 odst. 3 a 4 navrhovaného nařízení.

([63]) Viz článek 41 navrhovaného nařízení.

([64]) Viz oddíl II kapitoly V navrhovaného nařízení.

([65]) Viz oddíl II kapitoly V navrhovaného nařízení.

3.6 Legislativní orgány Unie by proto mohly zvážit následující návrhy na zvýšení jednoznačnosti a souladu mezi navrhovaným nařízením a směrnicí o kapitálových požadavcích. Za prvé, požadavky podle navrhovaného nařízení mohou být výslovně kvalifikovány jako obezřetnostní, jak tomu bylo mimo jiné v nařízení o centrálních depozitářích ([66]). Za druhé, mohlo by být rozšířeno znění bodů odůvodnění navrhované pozměňující směrnice ([67]) vzhledem k tomu, že požadavky podle navrhovaného nařízení jdou nad rámec pouhé fáze pohotovostních plánů a plánů zachování provozu. Opatření k řízení rizik v oblasti IKT celkově spadají pod obecnější rozsah spolehlivých systémů správy a řízení podle článku 74 směrnice o kapitálových požadavcích ([68]). Za třetí, navrhované nařízení ([69]) by mělo být změněno tak, aby v bodech odůvodnění připomínalo pravomoc ECB v oblasti obezřetnostního dohledu nad úvěrovými institucemi podle Smlouvy a nařízení o jednotném mechanismu dohledu. Za čtvrté, odkaz na uplatňování požadavků, které jsou stanoveny v uvedeném nařízení, na individuálním a konsolidovaném základě ([70]) by měl být revidován, neboť subkonsolidovaný a konsolidovaný základ nejsou v navrhovaném nařízení definovány a některé druhy zprostředkovatelů nepodléhají dohledu na konsolidovaném základě podle příslušných právních předpisů (např. platební instituce). Kromě toho by úroveň uplatňování požadavků podle navrhovaného nařízení měla vycházet výhradně z právních předpisů platných pro jednotlivé druhy finančních subjektů. V případě úvěrových institucí je dána jasná vazba mezi směrnicí o kapitálových požadavcích a navrhovaným nařízením, takže požadavky podle navrhovaného nařízení by se automaticky uplatňovaly na individuální, subkonsolidované nebo případně konsolidované úrovni ([71]). Legislativní orgány Unie by rovněž mohly zvážit zavedení přechodného režimu pro období mezi vstupem navrhovaného nařízení v platnost a vstupem v platnost regulačních technických norem stanovených v navrhovaném nařízení, neboť na některé zprostředkovatele, včetně úvěrových institucí, se již vztahují pravidla týkající se rizik v oblasti IKT, která platí pro konkrétní odvětví a která jsou podrobnější než obecná ustanovení navrhovaného nařízení.

3.7 ECB byla nařízením o jednotném mechanismu dohledu pověřena úkolem zajistit, aby úvěrové instituce dodržovaly požadavky práva Unie, které vyžadují, aby úvěrové instituce zavedly spolehlivé postupy řízení rizik a mechanismy vnitřní kontroly ([72]). To znamená, že ECB musí zajistit, aby úvěrové instituce uplatňovaly zásady a postupy pro hodnocení a řízení své expozice vůči operačnímu riziku, včetně modelového rizika, a pro pokrytí méně četných, ale vysoce rizikových událostí. Pro účely těchto zásad a postupů musí úvěrové instituce jasně zformulovat, co tvoří operační riziko ([73]).

3.8 V červenci 2017 přijala Rada guvernérů Evropské centrální banky (ECB) rámec jednotného mechanismu dohledu pro hlášení kybernetických incidentů (dále jen „rámec“) na základě návrhu Rady dohledu v souladu s čl. 26 odst. 8 a čl. 6 odst. 2 nařízení o jednotném mechanismu dohledu a čl. 21 odst. 1 nařízení Evropské centrální banky (EU) č. 468/2014 (ECB/2014/17) ([74]). Rámec sestává ze závazné žádosti (jednotlivých rozhodnutí určených úvěrovým institucím) o informace a/nebo podávání zpráv na základě článku 10 nařízení o jednotném mechanismu dohledu ([75]). Některé země již zavedly postup hlášení incidentů, který vyžaduje, aby úvěrové instituce hlásily všechny závažné kybernetické incidenty svým vnitrostátním příslušným orgánům. V těchto zemích budou významné úvěrové instituce nadále hlásit incidenty vnitrostátním příslušným orgánům, které je pak bez zbytečného odkladu předají ECB jménem dohlížených subjektů. Výše uvedená rozhodnutí jsou proto rovněž

([66]) Viz název kapitoly II oddílu 4 „Obezřetnostní požadavky“ nařízení o centrálních depozitářích.

([67]) Viz 4. bod odůvodnění navrhované pozměňující směrnice.

([68]) Článek 85 směrnice 2013/36/EU je pouhým upřesněním. V tomto ohledu viz rovněž s. 4, 11 a 37 pokynů Evropského orgánu pro bankovnictví k řízení rizik v oblasti IKT a bezpečnosti ze dne 29. listopadu 2019 (dále jen „pokyny EBA“), kde je jako obecný právní základ výslovně uveden článek 74 směrnice 2013/36/EU.

([69]) Viz čl. 41 odst. 1 navrhovaného nařízení.

([70]) Viz čl. 25 odst. 3 a 4 navrhovaného nařízení.

([71]) Viz článek 109 směrnice o kapitálových požadavcích.

([72]) Viz čl. 4 odst. 1 písm. e) nařízení o jednotném mechanismu dohledu.

([73]) Viz článek 85 směrnice o kapitálových požadavcích.

([74]) Nařízení Evropské centrální banky (EU) č. 468/2014 ze dne 16. dubna 2014, kterým se stanoví rámec spolupráce Evropské centrální banky s vnitrostátními příslušnými orgány a vnitrostátními pověřenými orgány v rámci jednotného mechanismu dohledu (nařízení o rámci jednotného mechanismu dohledu) (ECB/2014/17) (Úř. věst. L 141, 14.5.2014, s. 1).

([75]) Kybernetický bezpečnostní incident (tj. zjištěné možné porušení bezpečnosti informací ať už v důsledku zlého úmyslu, tak náhodné) musí být konkrétně hlášen ECB, pokud je splněna alespoň jedna z těchto podmínek: 1) potenciální finanční dopad činí 5 mil. EUR nebo 0,1% CET1; 2) o incidentu byla informována veřejnost nebo incident poškozuje pověst instituce; 3) incident byl postoupen řediteli informačních technologií nad rámec obvyklého vykazování; 4) banka o incidentu uvědomila CERT/CSIRT, bezpečnostní agenturu či policii; 5) byly spuštěny postupy pro obnovu provozu po havárii či kontinuitu provozu nebo byl vznesen nárok na plnění v rámci pojištění kybernetických rizik; 6) došlo k porušení právních či regulatorních požadavků nebo 7) banka uplatní interní kritéria či odborný úsudek (včetně potenciálního systémového dopadu) a rozhodne se informovat ECB.

určena těmto vnitrostátním příslušným orgánům, které by tyto informace měly na základě rámce předávat ECB. ECB podporuje úsilí legislativních orgánů Unie o prosazování harmonizace a zefektivnění, mimo jiné pokud jde o soubor pravidel a povinností vztahujících se na úvěrové instituce v oblasti hlášení incidentů. V této souvislosti je ECB s ohledem na případné přijetí navrhovaného nařízení připravena rámec v případě potřeby změnit (a případně zrušit).

4. Zvláštní připomínky k řízení rizik v oblasti IKT, hlášení incidentů, testování provozní odolnosti a riziku třetích stran v oblasti IKT

4.1 *Řízení rizik v oblasti IKT*

4.1.1 ECB vítá skutečnost, že navrhovaným nařízením byl zaveden pevný a komplexní rámec řízení rizik v oblasti IKT, který zahrnuje pokyny CPMI-IOSCO ke kybernetické odolnosti a který je úzce sladěn s osvědčenými postupy, včetně Očekávání dozoru v oblasti kybernetické odolnosti infrastruktur finančního trhu v rámci Eurosystému.

4.1.2 ECB podporuje myšlenku, že finanční subjekty by měly mít povinnost provádět posouzení rizik při každé „významné změně“ infrastruktury sítě a informačního systému ([76]). Navrhované nařízení však neobsahuje žádnou definici „významné změny“, což vytváří nevítaný prostor pro rozdílné výklady ze strany finančních subjektů, které by v konečném důsledku mohly ohrozit harmonizační cíle navrhovaného nařízení. V zájmu právní jistoty by legislativní orgány Unie mohly zvážit, zda by do navrhovaného nařízení neměly zavést definici „významné změny“.

4.1.3 ECB obecně podporuje myšlenku, že finanční subjekty jiné než mikropodniky nahlásí příslušným orgánům veškeré náklady a ztráty způsobené výpadky IKT a incidenty souvisejícími s IKT ([77]). S cílem zajistit celkovou účinnost systému a zabránit tomu, aby příslušné orgány a finanční subjekty byly zavaleny nadměrným počtem zpráv, by bylo prospěšné, aby legislativní orgány Unie prozkoumaly zavedení příslušných prahových hodnot, pokud možno kvantitativní povahy.

4.1.4 ECB bere na vědomí, že finanční subjekty mohou po schválení příslušnými orgány delegovat úkoly týkající se ověřování souladu s požadavky na řízení rizik v oblasti IKT na podniky v rámci skupiny nebo na externí podniky ([78]). Zároveň je důležité, aby legislativní orgány Unie objasnily, jak by schválení příslušnými orgány bylo uděleno v případech, kdy by finanční subjekt podléhal více příslušným orgánům. K tomu může dojít v případě, že finanční subjekt je úvěrovou institucí, poskytovatelem služeb souvisejících s kryptoaktivy a/nebo poskytovatelem platebních služeb. Pokud jde o identifikaci a klasifikaci, kterou mají finanční subjekty provádět podle navrhovaného nařízení ([79]), by ECB pro účely klasifikace aktiv považovala za obezřetné, aby finanční subjekty podle navrhovaného nařízení musely zohledňovat význam těchto aktiv (tj. zda podporují zásadní funkce).

4.2 *Hlášení incidentů*

4.2.1 ECB vítá úsilí, které vyplývá z navrhovaného nařízení a jehož cílem je harmonizace hlášení incidentů v oblasti IKT v rámci Unie a centralizované hlášení závažných incidentů souvisejících s IKT ([80]). Zavedení harmonizovaného rámce pro hlášení závažných incidentů souvisejících s IKT ([81]) příslušným orgánům by v zásadě zjednodušilo a harmonizovalo zpravodajskou zátěž finančních subjektů, včetně úvěrových institucí. Širší rozsah pokrývaných incidentů, který by překračoval rámec kybernetických incidentů, na něž se v současnosti vztahují stávající rámce ([82]), by byl pro příslušné orgány prospěšný. Budoucí přijetí navrhovaného nařízení by vyžadovalo přezkum a případné zrušení stávajících rámců, včetně rámce jednotného mechanismu dohledu pro oznamování kybernetických incidentů. V zájmu dosažení skutečného zjednodušení a plného sladění všech rámců je však zásadní zajistit, aby oblast působnosti ustanovení o hlášení incidentů podle navrhovaného nařízení, včetně všech příslušných definic, prahových hodnot a parametrů hlášení, byla plně v souladu s příslušnými rámci. Zejména je

([76]) Viz čl. 7 odst. 3 navrhovaného nařízení.
([77]) Viz čl. 10 odst. 9 navrhovaného nařízení.
([78]) Viz čl. 5 odst. 10 navrhovaného nařízení.
([79]) Viz článek 7 navrhovaného nařízení.
([80]) Viz článek 19 navrhovaného nařízení.
([81]) Viz čl. 3 odst. 7, článek 17 a článek 18 navrhovaného nařízení.
([82]) Viz například Rámec.

nanejvýš důležité zajistit soulad mezi navrhovaným nařízením na jedné straně a směrnicí Evropského parlamentu a Rady (EU) 2015/2366 ([83]) (dále jen „PSD2“) a obecnými pokyny EBA k hlášení závažných incidentů (dále jen „pokyny EBA“) na straně druhé. Navrhovaná pozměňující směrnice ([84]) obsahuje změny směrnice PSD2, pokud jde o vymezení hlášení incidentů mezi navrhovaným nařízením a směrnicí PDS2, což by mělo dopad zejména na poskytovatele platebních služeb, kteří by rovněž mohli mít povolení působit jako úvěrové instituce, jakož i na příslušné orgány. Postup oznamování incidentů není dostatečně jasný a některé incidenty, které je třeba oznamovat podle navrhovaného nařízení i podle obecných pokynů orgánu EBA, se mohou překrývat.

4.2.2 Postupy oznamování závažných incidentů podle navrhovaného nařízení ([85]), směrnice PSD2 a odpovídajících obecných pokynů EBA by od poskytovatelů platebních služeb vyžadovaly, aby po klasifikaci incidentu předkládali zprávu o incidentu svému příslušnému orgánu. Počáteční zprávy ve skutečnosti nezachycují podstatu, příčinu nebo funkční oblast ovlivněnou incidentem a poskytovatelé platebních služeb mohou být schopni takové rozlišení provést až později, kdy budou k dispozici podrobnější informace o incidentu. V důsledku toho by mohly být první hlášení o incidentech předkládány jak podle navrhovaného nařízení, tak podle obecných pokynů orgánu EBA, nebo by poskytovatelé platebních služeb mohli zvolit jeden rámec pro podávání hlášení a svá hlášení opravit později. Stejná nejistota (například pokud jde o hlavní příčinu jakéhokoli incidentu) se může projevit i v průběžných a závěrečných zprávách. To by opět zvýšilo možnost, aby zprávy byly příslušným orgánům předkládány souběžně podle navrhovaného nařízení a podle směrnice PSD2.

4.2.3 Některé incidenty, které mohou být klasifikovány jako incidenty související s IKT, mohou mít dopad i na jiné oblasti, a v důsledku toho by musely být oznámeny podle obecných pokynů orgánu EBA. Může tomu tak být v případě, že incident má dopad z hlediska IKT, ale zároveň přímo ovlivnil poskytování platebních služeb a/nebo ovlivnil jiné funkční oblasti nebo kanály, které se netýkají IKT. Kromě toho by mohly nastat případy, kdy není možné rozlišovat mezi provozními incidenty a incidenty souvisejícími s IKT. Kromě toho v případě, kdy je tatáž finanční instituce zároveň významnou úvěrovou institucí a poskytovatelem platebních služeb, by tentýž subjekt musel podle navrhovaného nařízení hlásit incident související s IKT dvakrát, neboť by podléhal dvěma příslušným orgánům. S ohledem na výše uvedené by navrhované nařízení mělo jasněji formulovat, jak má interakce mezi směrnicí PSD2 a obecnými pokyny orgánu EBA fungovat v praxi. Podstatnější je, že v zájmu harmonizace a zefektivnění oznamovací povinnosti by bylo důležité, aby legislativní orgány Unie zvážily zbývající otázky dvojího oznamování a aby objasnily, zda by navrhované nařízení na jedné straně a PSD2 a pokyny EBA na straně druhé existovaly souběžně, nebo zda by měl existovat jediný soubor požadavků na hlášení incidentů.

4.2.4. Navrhované nařízení zavádí požadavek, aby příslušné orgány ([86]) po obdržení zprávy potvrdily její přijetí a co nejrychleji finančnímu subjektu poskytly nezbytnou zpětnou vazbu nebo pokyny, zejména pojednávající o nápravě na úrovni daného subjektu nebo o způsobech minimalizace nepříznivého dopadu napříč odvětvími. To by znamenalo, že by příslušné orgány měly aktivně přispívat ke zvládání a nápravě incidentů a současně posuzovat reakci dohlíženého subjektu na kritické incidenty. ECB zdůrazňuje, že odpovědnost za nápravu a důsledky incidentu by měly zůstat výhradně a jednoznačně na dotčeném finančním subjektu. ECB proto navrhuje omezit zpětnou vazbu a pokyny pouze na obezřetnostní zpětnou vazbu a pokyny na vysoké úrovni. Pokud by zpětná vazba byla širší, vyžadovalo by to specializované odborníky s velmi značnými technickými znalostmi, kteří nejsou obvykle k dispozici v nabídce talentů, kterou mají k dispozici orgány obezřetnostního dohledu.

4.3 *Testování digitální provozní odolnosti*

4.3.1 ECB vítá požadavky, které navrhované nařízení ([87]) stanoví pro testování digitální provozní odolnosti ve všech finančních subjektech, jakož i požadavek, aby každá instituce měla vlastní program testování. Navrhované nařízení ([88]) uvádí různé typy testů pro finanční subjekty. Typy testů nejsou příliš jasné a u některých testů, jako jsou testy kompatibility, dotazníky nebo testy na základě scénářů, je dán prostor pro výklad ze strany evropských

([83]) Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, o změně směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a o zrušení směrnice 2007/64/ES (Úř. věst. L 337, 23.12.2015, s. 35).
([84]) Viz čl. 7 odst. 9 navrhované pozměňující směrnice.
([85]) Viz čl. 17 odst. 3 navrhovaného nařízení.
([86]) Viz článek 20 navrhovaného nařízení.
([87]) Viz články 21 a 22 navrhovaného nařízení.
([88]) Viz čl. 22 odst. 1 navrhovaného nařízení.

orgánů dohledu, příslušných orgánů nebo finančních subjektů. Kromě toho nejsou k dispozici žádné pokyny, pokud jde o četnost jednotlivých testů. Možným řešením by mohlo být, že navrhované nařízení by stanovilo obecné požadavky na testování a přesnější popis typů testů by byl obsažen v regulačních a prováděcích technických normách.

4.3.2 Penetrační testování na základě hrozeb (threat-led penetration testing – TLPT) je účinným nástrojem pro testování bezpečnostní obrany a připravenosti. ECB proto podporuje provádění TLPT finančními subjekty. Pomocí tohoto nástroje se testují nejen technická opatření, ale také zaměstnanci a procesy. Výsledky těchto testů mohou významně zvýšit povědomí o bezpečnosti, které má vrcholné vedení v testovaných subjektech. Evropský rámec TIBER-EU (European Framework for Threat Intelligence Based Ethical Red-teaming) ([89]) a další nástroje TLPT, které jsou již k dispozici mimo Unii, jsou primárními nástroji, díky kterým mohou subjekty samy posuzovat, testovat, uplatňovat a zlepšovat svou kybernetickou odolnost a obranu.

4.3.3 Ve většině členských států, v nichž byl rámec TIBER-EU proveden, orgány dozoru a orgány dohledu nehrají aktivní úlohu při provádění místního programu TIBER-XX a téměř ve všech případech je TIBER Cyber Team situován nezávisle na těchto funkcích. Z tohoto důvodu by pokročilé testování podle navrhovaného nařízení ([90]) prostřednictvím TLPT mělo být prováděno jako nástroj k posílení finančního ekosystému a zvýšení finanční stability, a nikoli výlučně jako nástroj dohledu. Kromě toho není třeba vyvíjet nový pokročilý rámec pro testování kybernetické odolnosti, neboť mnoho členských států již přijalo rámec TIBER-EU, což je v současné době jediný takový rámec v EU.

4.3.4 Požadavky na subjekty provádějící testování by neměly být obsaženy v hlavní části navrhovaného nařízení, neboť odvětví související s TLPT se stále vyvíjí a uložení konkrétních požadavků by mohlo bránit inovacím. ECB je však toho názoru, že v zájmu zajištění vysokého stupně nezávislosti při provádění testů by finanční subjekty neměly zaměstnávat subjekty provádějící testování ani testování zadávat subjektům, které jsou zaměstnány nebo najímány finančními subjekty v jejich vlastní skupině nebo které jsou jinak vlastněny nebo ovládány finančními subjekty, které mají být testovány.

4.3.5 Aby se snížilo riziko roztříštěnosti a zajistila harmonizace, mělo by navrhované nařízení stanovit jeden rámec TLPT, který se vztahuje na finanční sektor v celé Unii. Roztříštěnost může vést ke zvýšení nákladů a požadavků na technické, provozní a finanční zdroje jak pro příslušné orgány, tak pro finanční instituce. Tyto zvýšené náklady a požadavky mohou mít v konečném důsledku negativní dopad na vzájemné uznávání testů. Tato nedostatečná harmonizace a z toho vyplývající problémy spojené se vzájemným uznáváním mají zásadní význam zejména pro finanční subjekty, které mohou být držiteli více licencí a/nebo působit ve více jurisdikcích v celé Unii. Regulační a prováděcí technické normy, které mají být vypracovány pro TLPT podle navrhovaného nařízení, by měly být v souladu s rámcem TIBER-EU. ECB kromě toho vítá příležitost zapojit se do přípravy těchto regulačních a prováděcích technických norem ve spolupráci s evropskými orgány dohledu.

4.3.6 Aktivní zapojení příslušných orgánů do testování by mohlo vést k možnému střetu zájmů s jinou funkcí, kterou tyto orgány vykonávají, tj. posuzováním testovacího rámce finančního subjektu. V této souvislosti ECB navrhuje, aby byla z navrhovaného nařízení odstraněna jakákoli povinnost příslušných orgánů týkající se potvrzování dokladů a vydávání potvrzení pro účely testování TLPT.

4.4 Riziko třetích stran v oblasti IKT

4.4.1 ECB vítá zavedení komplexního souboru klíčových zásad a pevného rámce dohledu pro identifikaci a řízení rizik v oblasti IKT, která vznikají u poskytovatelů služeb IKT z řad třetích stran bez ohledu na to, zda patří do stejné skupiny finančních subjektů. V zájmu dosažení účinné identifikace a řízení rizik v oblasti IKT je však důležité správně identifikovat a klasifikovat mimo jiné kritické poskytovatele služeb IKT z řad třetích stran. V tomto ohledu lze uvítat zavedení aktů v přenesené pravomoci ([91]), které doplní kritéria pro účely klasifikace ([92]), s tím, že ECB by měla být před přijetím těchto aktů v přenesené pravomoci konzultována.

([89]) K dispozici na internetových stránkách ECB www.ecb.europa.eu.
([90]) Viz články 23 a 24 navrhovaného nařízení.
([91]) Viz čl. 28 odst. 3 navrhovaného nařízení.
([92]) Viz čl. 28 odst. 2 navrhovaného nařízení.

4.4.2 Pokud jde o strukturu rámce dohledu ([93]), je třeba dále vyjasnit úlohu, kterou má plnit společný výbor. ECB zároveň vítá své začlenění do fóra dohledu jako pozorovatel, neboť tato úloha poskytne ECB stejný přístup k dokumentaci a informacím jako hlasujícím členům ([94]). ECB by ráda upozornila legislativní orgány Unie na skutečnost, že ECB by ve své roli pozorovatele přispívala k činnosti fóra dohledu jako emisní centrální banka, která odpovídá za dohled nad tržními infrastrukturami, i jako orgán obezřetnostního dohledu nad úvěrovými institucemi. ECB dále poznamenává, že kromě toho, že by byla pozorovatelem ve fóru dohledu, byla by ECB jako příslušný orgán rovněž součástí společného vyšetřovacího týmu. V tomto ohledu by legislativní orgány Unie mohly dále zvážit složení společných vyšetřovacích týmů ([95]), aby se zajistilo přiměřeně významné zapojení dotčených příslušných orgánů. Ze stejného důvodu se ECB domnívá, že by měl být zvýšen maximální počet účastníků společných vyšetřovacích týmů, a to s ohledem na kritičnost, složitost a rozsah služeb třetích stran v oblasti IKT.

4.4.3 ECB si všímá, že podle navrhovaného nařízení může hlavní orgán dohledu zabránit tomu, aby kritičtí poskytovatelé služeb IKT z řad třetích stran uzavřeli další ujednání o subdodávkách, pokud i) plánovaný subdodavatel je třetí stranou poskytující služby IKT nebo subdodavatelem IKT usazeným ve třetí zemi a ii) subdodávky se týkají zásadní nebo důležité funkce finančního subjektu. ECB by ráda zdůraznila, že tyto pravomoci může hlavní orgán dohledu uplatnit jen v souvislosti s ujednáními o subdodávkách, kdy kritická třetí strana poskytující služby IKT zadá zásadní nebo důležitou funkci samostatnému právnímu subjektu usazenému ve třetí zemi. ECB chápe, že hlavní orgán dohledu by nemohl uplatnit srovnatelné pravomoci s cílem zabránit tomu, aby kritická třetí strana poskytující služby IKT externě zadávala zásadní nebo důležité funkce finančního subjektu do zařízení tohoto poskytovatele služeb, která se nacházejí ve třetí zemi. Mohlo by se například stát, že z provozního hlediska mohou být kritické údaje a/nebo informace uchovávány nebo zpracovávány zařízeními umístěnými mimo Evropský hospodářský prostor (EHP). V takovém případě nemusí pravomoci hlavního orgánu dohledu odpovídajícím způsobem zmocňovat příslušné orgány k přístupu ke všem informacím, prostorám, infrastrukturám a personálu, které jsou relevantní pro výkon všech zásadních nebo důležitých funkcí finančního subjektu. Aby bylo zajištěno, že příslušné orgány jsou schopny bez překážek plnit své úkoly, ECB navrhuje, aby hlavní orgán dohledu měl rovněž pravomoc omezit využívání zařízení umístěných mimo EHP poskytovateli služeb v oblasti IKT z řad třetích stran. Tato pravomoc by mohla být uplatněna v těch konkrétních případech, kdy nejsou uzavřena administrativní ujednání s příslušnými orgány třetích zemí, jak je stanoveno v navrhovaném nařízení ([96]), nebo kdy zástupci kritických poskytovatelů služeb IKT z řad třetích stran neposkytli dostatečné ujištění podle rámce příslušné třetí země, pokud jde o přístup k informacím, prostorám, infrastruktuře a personálu, který je potřebný k plnění úkolů v oblasti dozoru nebo dohledu.

4.4.4 V neposlední řadě je třeba uvést, že existuje riziko, že požadavek, aby se příslušné orgány řídily doporučeními hlavního orgánu dohledu ([97]), by se mohl ukázat jako neúčinný, neboť příslušné orgány nemusí mít komplexní přehled o rizicích, která vytvářejí jednotliví kritičtí poskytovatelé služeb IKT z řad třetích stran. Pokud doporučení kritičtí poskytovatelé služeb z řad třetích stran nedodrží, mohou být příslušné orgány kromě toho povinny přijmout opatření proti finančním subjektům, nad nimiž vykonávají dohled. Podle navrhovaného nařízení ([98]) mohou příslušné orgány požadovat, aby finanční subjekty, nad nimiž vykonávají dohled, dočasně přestaly využívat služby poskytované kritickou třetí stranou nebo ukončily existující smlouvy s kritickými poskytovateli služeb z řad třetích stran. Je obtížné převést předpokládaný proces následných opatření do konkrétních kroků. Konkrétně není jasné, zda bude dohlížený finanční subjekt schopen přerušit nebo ukončit smlouvu s kritickým poskytovatelem služeb z řad třetích osob. Důvodem je skutečnost, že kritická třetí strana poskytující služby IKT by mohla být významným poskytovatelem služeb pro tento finanční subjekt, nebo smluvní či jiné náklady a škody, které finanční subjekt může utrpět v důsledku takového přerušení nebo ukončení. Tento přístup navíc nepodporuje sbližování dohledu, neboť příslušné orgány mohou vykládat stejné doporučení odlišně. To by v konečném důsledku mohlo narušit předpokládanou harmonizaci a jednotný přístup při sledování rizika kritických třetích stran v oblasti IKT na úrovni Unie. S ohledem na výše uvedené by legislativní orgány Unie mohly zvážit, zda zákonným orgánům dohledu neudělí zvláštní donucovací pravomoci ve vztahu ke kritickým poskytovatelům služeb IKT z řad třetích stran, a to s přihlédnutím k omezením uloženým doktrínou *Meroni*, kterou částečně zmírnil Soudní dvůr ve svém rozsudku ve věci ESMA ([99]).

([93]) Viz článek 29 navrhovaného nařízení.
([94]) Viz čl. 29 odst. 3 navrhovaného nařízení.
([95]) Viz článek 35 navrhovaného nařízení.
([96]) Viz čl. 39 odst. 1 navrhovaného nařízení.
([97]) Viz čl. 29 odst. 2 a článek 37 navrhovaného nařízení.
([98]) Viz čl. 37 odst. 3 navrhovaného nařízení.
([99]) Viz rozsudek Soudního dvora (velkého senátu) ze dne 22. ledna 2014 Spojené království Velké Británie a Severního Irska v. Evropský parlament a Rada Evropské unie – nařízení (EU) č. 236/2012–C-270/12.

Konkrétní pozměňovací návrhy k těm ustanovením navrhovaného nařízení, která ECB doporučuje změnit, jsou uvedeny v samostatném technickém pracovním dokumentu včetně příslušného odůvodnění. Technický pracovní dokument je k dispozici v anglickém jazyce na internetových stránkách EUR-Lex.

Ve Frankfurtu nad Mohanem dne 4. června 2021.

Prezidentka ECB
Christine LAGARDE