UNIVERZITA KARLOVA

Právnická fakulta

Právní regulace silného ověření uživatele

Rigorózní práce

Mgr. Karel Řehůlka

Pověřený akademický pracovník: JUDr. Tomáš Sejkora, Ph.D.

Katedra finančního práva a finanční vědy

Datum vypracování práce (uzavření rukopisu): 22. 01. 2023

Prohlášení

Prohlašuji, že jsem předkládanou rigorózní práci vypracoval samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této rigorózní práce včetně poznámek pod čarou má 243.456 znaků včetně mezer.

V Praze, dne 22. 01. 2023

Mgr. Karel Řehůlka

Poděkování

Velice rád bych touto cestou poděkoval vedoucímu této rigorózní práce JUDr. Tomáši Sejkorovi, Ph.D. za cenné rady, odborné vedení a čas, jež mi věnoval při zpracování problematiky, která je obsahem této rigorózní práce.

Mgr. Karel Řehůlka

Obsah

1. Úvod

Výměna zboží a služeb je stará jako civilizace sama. Již několik tisíc let před naším letopočtem ve starověké Mezopotámii existoval tzv. barterový obchod spočívající ve směně jednoho zboží na jiné v poměru dle jejich hodnot. To se postupem času ukázalo jako poměrně nepraktické a o několik tisíc let později začaly být jako platidlo za zboží používány ražené mince. Ve středověké Evropě používali obchodníci na trzích poměrně často také směnky jako nástroj reprezentující písemný příslib osoby v budoucnu zaplatit za touto osobou nakoupené zboží. Specifické pak byly směnky bankovní, které byly vydávány institucemi představujícími tehdejší obdobu dnešních bank a které mohli lidé směňovat za vzácné kovy – typicky za zlato či stříbro. S dalším rozvojem národních ekonomik a mezinárodního obchodu vyvstala potřeba pro větší přesuny peněz, a proto byly vynalezeny papírové peníze a také šeky, které se postupně staly dominantním způsobem převodu peněz podniky i jednotlivce.

Rozvoj technologií a nástup internetu v posledních několika desetiletích významnou mírou ovlivnily oblast platebních služeb a platebního styku. Umožnily vznik elektronického platebního styku, který postupem času nabíral na důležitosti, přičemž dnes si bez jeho řádného fungování dovedeme představit fungující finanční systém jen stěží. Pandemie COVID-19, která v posledních letech postihla celý svět, díky souvisejícím vládním restrikcím nepřímo posílila roli elektronického platebního styku a umocnila nastupující trend používání mobilních a jiných elektronických chytrých zařízení pro placení. Během pouhých několika měsíců tak došlo k urychlenému přesunu velkého množství aktivit do online prostředí, ale zároveň také ke změně řady návyků mnohých z nás, a to včetně těch platebních.

Jelikož při placení dnes již na denní bázi využíváme platební karty, chytré telefony nebo hodinky a internetové bankovnictví a přehled o svých financích „nosíme v kapse“, je více než dříve aktuální otázka bezpečnosti našich financí a osobních údajů. Jednou z nejvýznamnějších regulací, která byla v posledních letech v oblasti bezpečnosti elektronického platebního styku zavedena, je právní úprava silného ověření uživatele. Ta se díky stanovení požadavku na dvoufázové ověření totožnosti uživatele snaží dosáhnout snížení míry a objemu podvodů u elektronických plateb a zajištění vyšší bezpečnosti uživatelů v oblasti elektronického platebního styku. K tomuto dvoufázovému ověření jsou vyžadovány vždy dva na sobě nezávislé prvky z kategorií znalost, držení a inherence.

Zavedením této regulace došlo k významnému posunu ve vnímání a kladení požadavků na bezpečnost elektronického platebního styku. Z důvodu aktuálnosti tohoto tématu, které navíc nabylo v posledních letech na důležitosti díky dopadům pandemie, a osobního zájmu o bezpečnost v této oblasti jsem si jako téma této rigorózní práce zvolil právní úpravu silného ověření uživatele, kterou se budu v jednotlivých kapitolách této rigorózní práce podrobněji zabývat.

V úvodní části se budu nejdříve věnovat stručnému přehledu úpravy platebního styku, popisu platebních systémů, platebních služeb a osob oprávněných je poskytovat a závěrem také přehledu účinných právních předpisů v této oblasti. Jelikož je úprava silného ověření uživatele s těmito tématy úzce propojena, považuji zahrnutí úvodní části na toto téma jako vhodné z důvodu snahy o lepší pochopení navazujících částí. V další části se budu věnovat samotnému konceptu silného ověření uživatele a rozboru jeho jednotlivých složek, na který naváži částí o jednotlivých situacích, při kterých musí poskytovatelé platebních služeb silné ověření uživatele vyžadovat, a současně také o situacích, při kterých mohou poskytovatelé naopak využít některé z výjimek. Závěrem se budu věnovat tématu behaviorální biometrie a její roli v rámci silného ověření uživatele, srovnání unijní úpravy se stavem v některých zemích mimo území Evropského hospodářského prostoru a v úplném závěru poté analýze úskalí, dopadů a celkovému zhodnocení právní regulace silného ověření uživatele.

Cílem této práce je vytvoření uceleného přehledu stávající právní úpravy silného ověření uživatele, poukázat na případné nedostatky této regulace a navrhnout související řešení, učinit srovnání této úpravy v mezinárodním měřítku, zhodnotit dopady a účelnost jejího zavedení a zaměřit se na případné trendy, které mohou určovat její budoucí vývoj. Vzhledem k tomuto cíli by převážná část práce měla být z důvodu snahy o vytvoření přehledu aktuálně účinné právní úpravy deskriptivního a pozitivistického charakteru, nicméně v závěrečné části se v rámci normativního zkoumání budu v rámci úvah de lege ferenda zabývat možnostmi napravení jejích případných nedostatků. Pro tento účel budu využívat také metody komparace při srovnání se situací v jiných zemích mimo území Evropského hospodářského prostoru, analýzy a případně také indukce při rozboru behaviorální biometrie, možností jejího použití v rámci silného ověření uživatele a při zhodnocení úskalí regulace silného ověření uživatele a jejích dopadů.

Při psaní této práce budu používat a pracovat především s texty samotných právních předpisů, odbornou literaturou, elektronickými zdroji, doporučeními, stanovisky, sděleními a pokyny příslušných regulátorů a dle potřeby také s judikaturou či odbornými články.

2. Platební styk

V této části rigorózní práce se budu nejdříve věnovat právní úpravě platebního styku. Jelikož je silné ověření uživatele součástí úpravy bezpečnosti platebního styku a z povahy věci je tak na něj přímo navázáno, považuji za relevantní se v úvodních kapitolách a podkapitolách alespoň v obecné rovině zaměřit na některé aspekty a instrumenty platebního styku. Postupně se budu věnovat základnímu vymezení platebního styku, bezhotovostnímu platebnímu styku se zaměřením na popis platebního účtu a platebních systémů, dále úpravě platebních služeb a subjektů, které jsou oprávněny je poskytovat, a závěrem této části se rámcově zaměřím na účinnou právní úpravu bezhotovostního platebního styku na území České republiky a Evropské Unie.

2.1. Vymezení platebního styku

V rámci finančního práva řadíme právní úpravu platebního styku do jeho zvláštní části, kterou dále dělíme na část fiskální a nefiskální. Do odvětví fiskální části řadíme především úpravu veřejných rozpočtů, jejich příjmů a výdajů. Nefiskální část se naopak zabývá samotnou peněžní masou, její tvorbou, rozdělováním a užitím a spadá do ní především regulace peněž a peněžního systému.[1] Právní úpravu platebního styku tak řadíme do nefiskální části finančního práva, konkrétně do pododvětví měnového práva, kam ji lze zařadit společně s právní úpravou měny a peněžního oběhu.[2]

Platební styk hraje důležitou roli ve finančním systému a jeho řádné a efektivní fungování je nezbytné pro fungování ekonomiky jako celku. Se spojením „platební styk“ se můžeme setkat v různém kontextu. V širším slova smyslu jej lze chápat jako jakoukoliv formu placení mezi osobami, která se (zpravidla) děje za účelem splnění peněžitého závazku.

[1] JANOVEC, Michal. Postavení dohledu nad finančním trhem v systému finančního práva. *Bulletin-advokacie.cz* [online]. 2014 [cit. 05. 03. 2022]. Dostupné z: http://www.bulletin-advokacie.cz/postaveni-dohledu-nad-financnim-trhem-v-systemu-financniho-prava

[2] BAKEŠ, Milan, Marie KARFÍKOVÁ, Petr KOTÁB, Hana MARKOVÁ a kol. *Finanční právo*. 6. vydání. Praha: C. H. Beck, 2012, s. 14, ISBN 978-80-7400-440-7.

Naopak v užším slova smyslu jím rozumíme pouze takové případy, kdy mezi plátce a příjemce vstupuje třetí osoba, která pro ně přesun peněžních prostředků zajišťuje.[3]

Platební styk v české legislativě přímo definován není, nicméně v odborné literatuře se s jeho definicí lze v řadě případů setkat. Platební styk je vymezen např. jako „*systém organizovaný bankami a finančními institucemi, který umožňuje hotovostní i bezhotovostní finanční přesuny mezi jednotlivými subjekty hospodářského života – fyzickými i právnickými osobami*“.[4] Další autoři na něj naopak pohlíží jako na „*vztah mezi plátcem a příjemcem platby, při kterém dochází k uskutečnění platby, tedy k převodu peněžních aktiv mezi plátcem a příjmem.*“[5] nebo na „*vztah mezi plátcem a příjemcem, který je uskutečňován v určitých formách buď přímo mezi nimi, nebo prostřednictvím peněžního ústavu*.“[6].

Platební styk může mít různou formu a lze jej dělit podle následujících kritérií:

(i) podle formy použitých platebních prostředků rozlišujeme (a) **hotovostní platební styk**, při němž mezi příjemcem a plátcem dochází k přesunu peněz v hotovosti za pomoci zákonných platidel. Podle § 16 zákona č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů (dále jen „**Zákon o ČNB**“) jsou zákonnými penězi platné bankovky a mince vydané Českou národní bankou ve své nominální hodnotě při všech platbách na území České republiky.[7] Opakem je (b) **bezhotovostní platební styk**, který nemá materiální podobu a při kterém dochází k úhradě bezhotovostním převodem na účtech plátců a příjemců a k použití hotových peněz tak nedochází;[8]

---

[3] BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. *Zákon o platebním styku. Komentář.* Praha: Wolters Kluwer ČR, 2020, s. 3. ISBN 978-80-7598-788-4.

[4] MARVANOVÁ, Marie, Martin HOUDA a kol. *Platební styk (aneb platební a zajišťovací instrumenty ve vnitřním a zahraničním obchodě)*. Brno: E.P.B.K., 1993, s. 14. ISBN: 80-901627-0-3.

[5] POLOUČEK, Stanislav a kol. *Bankovnictví.* 2. vydání. Praha: C. H. Beck, 2013, s. 98. ISBN 978-80-7400-491-9.

[6] SCHLOSSBERGER, Otakar a Marcela SOLDÁNOVÁ. *Platební styk*. 3. vydání. Praha: Bankovní institut, a.s., 2005, s. 24. ISBN 80-7265-072-6.

[7] Tuzemské bankovky a mince a jejich oběh jsou blíže upraveny zákonem č. 136/2011 Sb., o oběhu bankovek a mincí a o změně zákona č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů.

[8] ŠENKÝŘOVÁ, Bohuslava a kol. *Bankovnictví.* 1. vydání. Praha: Vysoká škola finanční a správní, o.p.s., 2010, s. 147-148. ISBN 978-80-7408-029-6.

(ii) podle teritoria transakce rozlišujeme (a) **tuzemský platební styk**, k němuž dochází mezi subjekty uvnitř národní ekonomiky jednoho státu a (většinou) v domácí měně tohoto státu, (b) **zahraniční platební styk**, který se odehrává mezi tuzemskými a zahraničními subjekty a řadíme do něj platby do a ze zahraničí včetně plateb mezi tuzemskými subjekty překračující hranice jednoho státu (v takovém případě bude mít jeden ze subjektů účet vedený u finanční instituce v jiném státě), a (c) **přeshraniční platební styk**, který se týká přeshraničních plateb[9] mezi účty vedenými u finančních institucí na území dvou různých států v rámci Evropského hospodářského prostoru (dále jen „**EHS**“);[10]

(iii) podle náležitostí průvodních dokumentů rozlišujeme (a) **dokumentární platební styk**, při kterém mají platby vazbu na průvodní dokumenty, které je při platbě potřeba předložit (např. dokumentární akreditiv, dokumentární inkaso), a (b) **nedokumentární platební styk**, při němž platba probíhá pouze na základě příkazu jednoho účastníka platebního vztahu (např. příkazy k úhradě v tuzemském platebním styku nebo hladké platy[11] v zahraničním platebním styku);[12]

(iv) podle lhůty k provedení platby dělíme platební styk na (a) **přednostní (expresní)**, u kterého se jedná o urychlené odepsání peněžních prostředků

[9] Pravidla pro přeshraniční platby stanoví Nařízení Evropského Parlamentu a Rady (EU) 2021/1230 ze dne 14 července 2021 o přeshraničních platbách v Unii.

[10] POLOUČEK, Stanislav a kol. *Bankovnictví.* 2. vydání. Praha: C. H. Beck, 2013, s. 99. ISBN 978-80-7400-491-9.

[11] Hladký plat (jinak také jako prostá úhrada či bankovní převod) neobsahuje žádný závazek banky, provádí se volně na základě příkazu plátce a není podmíněn předložením dokumentů nebo jakéhokoliv protiplnění od příjemce. Dělíme je na vyšlé (úhrady do zahraniční) a došlé (úhrady ze zahraničí).
Zdroj: ŠENKÝŘOVÁ, Bohuslava a kol. *Bankovnictví.* 1. vydání. Praha: Vysoká škola finanční a správní, o.p.s., 2010, s. 155-156. ISBN 978-80-7408-029-6; a BAKEŠ, Milan, Marie KARFÍKOVÁ, Petr KOTÁB, Hana MARKOVÁ a kol. *Finanční právo*. 6. vydání. Praha: C. H. Beck, 2012, s. 399, ISBN 978-80-7400-440-7.

[12] POLOUČEK, Stanislav a kol. *Bankovnictví.* 2. vydání. Praha: C. H. Beck, 2013, s. 99. ISBN 978-80-7400-491-9.

z účtu klienta, a (b) **standardní**, při kterém je příkaz proveden dle předem dohodnutých (standardních) podmínek;[13]

(v) podle skutečnosti, jestli do závazku vstupuje banka či nikoli, rozlišujeme (a) **závazkový platební styk**, při němž banka vstupuje vedle klienta nebo namísto něj do závazků při realizaci platebního instrumentu (např. bankovní záruka), a (b) **bezzávazkový platební styk**, při kterém banka vystupuje pouze jako prostředník;[14]

(vi) podle počtu bank v transakci dále rozlišujeme (a) **vnitrobankovní platební styk** probíhající mezi klienty téže banky a (b) **mezibankovní platební styk** s využitím služeb dvou nebo více bank;[15] a

(vii) podle předmětu platebního závazku rozlišujeme platební styk na (a) **obchodní**, při němž platba zajišťuje zaplacení obchodního závazku, a (b) **neobchodní**, při kterém platba není podložena žádným obchodním případem.[16]

2.2. Bezhotovostní platební styk

Jak bylo uvedeno v předchozí kapitole 2.1 (*Vymezení platebního styku*) výše, dle formy použitých platebních prostředků dělíme platební styk na hotovostní, ve kterém dochází k provádění plateb za pomocí mincí a bankovek, a bezhotovostní, který vymezujeme jako převod peněžních prostředků mezi subjekty bez fyzické potřeby hotovostních peněz prostřednictvím jejich platebních účtů. Bezhotovostní platební styk probíhá zpravidla bez současné fyzické přítomnosti plátce a příjemce, a proto vyvstává zvýšená potřeba ověřování totožnosti těchto osob. Aby však vůbec mohlo dojít k převodu peněžních prostředků, je nezbytná existence platebních účtů a také platebních systémů, které slouží

[13] MÁČE, Miroslav. *Platební styk – klasický a elektronický.* 1. vydání. Praha: GRADA Publishing, a.s., 2006, s. 28. ISBN 80-247-1725-5.

[14] SCHLOSSBERGER, Otakar a Marcela SOLDÁNOVÁ. *Platební styk*. 3. vydání. Praha: Bankovní institut, a.s., 2005, s. 25. ISBN 80-7265-072-6.

[15] POLOUČEK, Stanislav a kol. *Bankovnictví.* 2. vydání. Praha: C. H. Beck, 2013, s. 99. ISBN 978-80-7400-491-9.

[16] Tamtéž, s. 100.

k vypořádávání platebních transakcí. V následujících podkapitolách se těmto dvěma pojmům budu blíže věnovat.

2.2.1. Úvod do bezhotovostního platebního styku

S rozvojem technologií a nástupem digitalizace pozorujeme v posledních letech trend upřednostňování bezhotovostních plateb oproti platbám hotovostním. Obecně lze říci, že čím rozvinutější je ekonomika, tím vyšší je míra pravděpodobnosti, že osoby v rámci ní budou při placení preferovat používání bezhotovostních platebních převodů. Tento trend byl v předcházejících letech umocněn pandemií COVID-19, díky níž se potřeba omezení bezprostředního osobního kontaktu mezi lidmi významným způsobem projevila také v platebním styku. Výjimkou v tomto případě nebyla ani Česká republika, jak lze vyčíst z dat v níže uvedených tabulkách.

Statistika držitelů platebních karet v České republice[17]

Kritérium	Rok 2010	Rok 2015	Rok 2019	Rok 2020	Rok 2021
Celkový počet vydaných karet	9.268.914	11.421.038	12.711.604	13.518.528	14.092.533
Celkový počet akceptačních míst	211.884	508.200	692.280	812.512	869.069
Celkový počet bezhotovostních transakcí u obchodníků	224.409.914	539.016.124	1.322.431.628	1.516.755.126	1.851.747.446
Celkový objem transakcí (v Kč)	203.591.130.598	366.300.097.459	844.566.994.214	959.060.169.646	1.235.173.991.731

[17] Vlastní tvorba autora. Zdroj podkladových dat: Sdružení pro bankovní karty (SBK). Souhrnná statistika SBK. *Bankovnikarty.cz* [online]. 2022 [cit. 06. 03. 2022]. Dostupné z: http://www.bankovnikarty.cz/pages/czech/profil_statistiky.html

Statistika výběru z bankomatů (ATM) v České republice[18]

Kritérium	Rok 2010	Rok 2015	Rok 2019	Rok 2020	Rok 2021
Celkový počet instalovaných ATM	3.868	4.545	5.644	5.551	5.572
Celkový počet výběrů hotovosti z ATM	158.676.047	178.611.083	179.715.635	143.220.785	142.111.485
Celkový objem výběrů z ATM (v Kč)	585.279.726.085	686.007.550.688	821.874.915.144	735.114.138.639	796.527.965.282

Česká národní banka (dále jen „**ČNB**“) jako centrální banka České republiky společně s ostatními národními centrálními bankami v rámci Evropské unie (dále jen „**EU**“) stanovuje a zavádí zpravodajské postupy pro poskytování statistických informací a shromažďuje data o platebním styku v souladu s nařízením Evropské centrální banky (dále jen „**ECB**“).[19] Data o statistice platebního styku jsou veřejně k dispozici v systému ARAD, který je veřejnou databází a je součástí informačního servisu ČNB.[20]

V procentuálním počtu držitelů platebních karet u osob ve věku od 15 let se Česká republika nachází v mezinárodním srovnání až za ekonomicky nejvyspělejšími zeměmi, kdy v roce 2017 se s výsledkem 74,99 % umístila na 36. místě. Žebříčku kralují severské státy (Dánsko, Finsko, Norsko, Švédsko), které společně s Nizozemím dosahují hodnot převyšujících 97 % a postupně směřují k bezhotovostní společnosti.[21] Jako příklad lze uvést Švédsko, kde v průzkumech tamní centrální banky Riskbank, zaměřených na platební morálku švédského obyvatelstva, uvedlo pouhých 9 % korespondentů, že k poslední úhradě použili hotovost (oproti 39 % v roce 2010), a pouze polovina ze všech dotazovaných

[18] Vlastní tvorba autora. Zdroj podkladových dat: Tamtéž.

[19] Nařízení Evropské Centrální Banky (EU) č. 1409/2013 ze dne 28. listopadu 2013, o statistice platebního styku.

[20] Česká národní banka. ARAD – Systém časových řad. *Cnb.cz* [online]. 2019 [cit. 06. 03. 2022]. Dostupné z: https://www.cnb.cz/cnb/STAT.ARADY_PKG.STROM_SESTAVY?p_strid=AAAE

[21] TheGlobalEconomy.com. Percent people with debit cards – Country rankings. *TheGlobalEconomy.com* [online]. 2017 [cit. 06. 03. 2022]. Dostupné z: https://www.theglobaleconomy.com/rankings/people_with_debit_cards/

korespondentů uvedla, že v posledním měsíci použila hotovost, přičemž ještě v roce 2018 to bylo 61 %.[22]

2.2.2. Platební účet

V rámci bezhotovostního platebního styku dochází k převodu peněz mezi subjekty, který je realizovaný prostřednictvím jejich běžných nebo jiných účtů vedených u zprostředkovatelských institucí. Z daného vyplývá, že účastníkem tohoto vztahu bude nad rámec plátce a příjemce vždy minimálně také třetí strana zprostředkovávající samotný převod (např. banka) a že bez existence účtu odesílatele i příjemce platby nebude možné bezhotovostní převod realizovat.

Klientský účet může mít několik forem, které se liší dle jeho účelu a způsobu použití:[23]

(i) **běžný účet**, který slouží k uložení finančních prostředků klienta a jejich využití k placení;

(ii) **úvěrový účet**, na kterém je evidován čerpaný úvěr a způsob jeho splácení;

(iii) **kontokorentní účet**, který je kombinací dvou výše uvedených účtů a klient může čerpat finanční prostředky do smluvně určené maximální výše;

(iv) **vkladový (spořící) účet** sloužící k uložení volných finančních prostředků klienta; a

(v) **depotní účet**, na kterém jsou evidovány cenné papíry v úschově či správě banky.

[22] Sveriges Riksbank. The payment market is being digitized – Cash is losing ground. *Riskbank.se* [online]. 2020 [cit. 06. 03. 2022]. Dostupné z: https://www.riksbank.se/en-gb/payments--cash/payments-in-sweden/payments-in-sweden-2020/1.-the-payment-market-is-being-digitalised/cash-is-losing-ground/the-use-of-cash-is-declining/

[23] MÁLEK, Petr, Gabriela OŠKRDALOVÁ a Petr VALOUCH. *Osobní finance*. 1. vydání. Brno: Ekonomicko-správní fakulta Masarykovy Univerzity, 2010, s. 122. ISBN 978-80-210-5157-7; a POLOUČEK, Stanislav a kol. *Bankovnictví.* 2. vydání. Praha: C. H. Beck, 2013, s. 100. ISBN 978-80-7400-491-9.

Zákon č. 370/2017 Sb., o platebním styku, ve znění pozdějších předpisů (dále jen „**ZPS**“) nám definuje platební účet jako „*účet, který slouží k provádění platebních transakcí*“[24]. Platební transakce je v něm poměrně široce definována jako „*vložení peněžních prostředků na platební účet, výběr peněžních prostředků z platebního účtu nebo převod peněžních prostředků, je-li prováděna v rámci platební služby*“.[25]

Samotná definice platebního účtu nám nedává jednoznačnou odpověď na otázku, které druhy účtů lze podřadit pod platební účet ve smyslu ZPS. Touto otázkou se částečně zabýval Soudní dvůr Evropské unie (dále jen „**SDEU**“) v rámci řízení o předběžné otázce, o které SDEU rozhodoval v souladu s článkem 267 Smlouvy o fungování Evropské Unie.[26] V tomto řízení se na SDEU v roce 2017 obrátil rakouský Nejvyšší soud (*Oberster Gerichthof*) s následující předběžnou otázkou:

„*Musí být článek 4 bod 14 směrnice [o platebních službách][27] vykládán v tom smyslu, že i online spořicí účet, s kterým může klient (denně a bez zvláštního spolupůsobení banky) provádět prostřednictvím telebankingu vklady na referenční účet vedený na jeho jméno a výběry z téhož referenčního účtu (běžný účet v Rakousku), je nutno zařadit pod pojem ‚platební účet‘, a že tedy spadá do působnosti této směrnice?*“

K tomu SDEU uvedl, že „*možnost provádět z účtu platební transakce ve prospěch třetí strany nebo být příjemcem takových transakcí od třetí strany je základním znakem pojmu „platební účet.“. Účet, z něhož takové platební transakce nemohou být prováděny přímo, avšak k jejichž uskutečnění je nezbytné využít zprostředkovacího účtu, tedy nelze považovat za „platební účet“.* Z tohoto důvodu bylo SDEU rozhodnuto, že *„pod pojem „platební účet“*

[24] § 2 odst. 1 písm. b) ZPS

[25] § 2 odst. 1 písm. a) ZPS

[26] Rozsudek SDEU ze dne 4. 10. 2018, ING-DiBa Direktbank Austria, C-191/17, ECLI:EU:C:2018:809. Dostupné z: https://curia.europa.eu/juris/liste.jsf?language=cs&num=C-191/17

[27] Směrnice Evropského parlamentu a Rady 2007/64/ES ze dne 13. listopadu 2007 o platebních službách na vnitřním trhu, kterou se mění směrnice 97/7/ES, 2002/65/ES, 2005/60/ES a 2006/48/ES a zrušuje směrnice 97/5/ES (dále jen „**Směrnice PSD**“).

nespadá spořicí účet, který umožňuje disponovat uloženými částkami na požádání a z něhož lze vklady a výběry provádět pouze prostřednictvím běžného účtu.“[28]

Výše uvedený závěr se bude aplikovat také na novou směrnici o platebních službách[29], jelikož v ní oproti Směrnici PSD zůstala definice platebního účtu nezměněna. Důvodová zpráva k ZPS[30] shodně uvádí, že spořicí účet nebude platebním účtem pokud „*možnost majitele účtu disponovat peněžními prostředky na účtu je výrazně omezena předem dohodnutými podmínkami nebo vázána na další součinnost osoby, která účet vede*.“ Pod platební účet z tohoto důvodu nebudou spadat ani terminované vklady a účty stavebního spoření. U úvěrových účtů bude vždy záležet na tom, jestli jsou peněžní prostředky z úvěrového účtu vypláceny přímo příjemci úvěru a jestli na daném účtu dochází k převodům, nebo jen k vkládání a vybírání peněžních prostředků. O platební účet tak nepůjde tehdy, pokud přesun peněžních prostředků od poskytovatele úvěru k třetím osobám nelze považovat za samotný převod založený na libovůli příjemce úvěru, ale pouze za jeho distribuci v souladu s předem dohodnutými podmínkami. Typicky tak pod platební účet nepůjde podřadit úvěrový účet s předem určeným účelovým vymezením.[31]

Platebním účtem nebude ani vkladní knížka[32], protože umožňuje uživateli pouze vklad a výběr peněžních prostředků a neslouží k jejich převodu. Nad rámec tohoto důvodu zde chybí také element třetí strany, která by byla příjemcem nebo plátcem platební transakcí na účet nebo z účtu, ke kterému byla vkladní knížka zřízena. V neposlední řadě ani jednorázový vklad[33] nelze považovat za platební účet, protože příjemce se v rámci něj

[28] Rozsudek SDEU ze dne 4. 10. 2018, ING-DiBa Direktbank Austria, C-191/17, ECLI:EU:C:2018:809, bod 31-33. Dostupné z: https://curia.europa.eu/juris/liste.jsf?language=cs&num=C-191/17

[29] 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 (dále jen „**Směrnice PSD2**“).

[30] Důvodová zpráva k zákonu č. 370/2017 Sb., o platebním styku. Zvláštní část k § 2. 2017. Dostupné z: www.beck-online.cz

[31] Tamtéž.

[32] § 2676 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdější předpisů (dále jen „**OZ**“).

[33] Tamtéž, § 2680.

zavazuje po zániku závazku vklad vrátit a zaplatit za něj úrok. Tato jednorázová povaha neodpovídá požadavkům platebního účtu.[34]

Platební účet se zřizuje na základě smlouvy o účtu, kterou se budou řídit práva a povinnosti majitele účtu a subjektu, který vede účet. Příslušná ustanovení OZ týkající se smlouvy o účtu[35] se budou aplikovat také na platební účet ve smyslu ZPS. Smlouva o účtu má konsenzuální povahu a jejím účastníkům tak stačí ujednat smluvené závazky, aniž by bylo zapotřebí reálného jednání (např. vkladu hotovosti na účet). Závazkem osoby, která vede účet, bude (i) zřídit od určité doby v určité měně účet pro majitele, (ii) umožnit majiteli vložení hotovosti na účet a její výběr, a (iii) umožnit provádění převodů peněžních prostředků z tohoto účtu či na tento účet. V případě vkladu peněz na účet bude mít majitel pohledávku z účtu odpovídající výši vkladu vůči osobě, která tento účet vede.[36]

2.2.3. Platební systémy

Bezhotovostní převody peněžních prostředků z jednoho platebního účtu na druhý jsou zajišťovány prostřednictvím platebních systémů. Jejich existence nám umožňuje a usnadňuje poměrně rychlým a efektivním způsobem přesouvání peněžních prostředků mezi subjekty, které geograficky dělí jakákoliv vzdálenost.

ZPS nám platební systém definuje jako „*systém s jednotnými pravidly, který slouží k provádění, zúčtování nebo vypořádání platebních transakcí*.“.[37] Vymezení platebního systému nalezneme také v odborné literatuře, a to např. jako „*systém, který zajišťuje převody peněz nebo likvidity. Může být provozován buď na principu zúčtování a vypořádání jednotlivých položek při současné kontrole jejich krytí (hrubý platební systém), nebo na principu zúčtování rozdílů (sald) vypočtených ze vzájemných pohledávek a závazků účastníků systému (čistý platební systém), případně jako kombinace těchto principů. Právně se jedná o formální dohodu založenou na soukromém kontraktu nebo zákonem předepsanou konstrukci. Dohoda se vyznačuje vícenásobným členstvím, společnými pravidly*

[34] BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. *Zákon o platebním styku. Komentář.* Praha: Wolters Kluwer ČR, 2020, s. 20-21. ISBN 978-80-7598-788-4.

[35] § 2662 OZ.

[36] HULMÁK, Milan a kol. *Občanský zákoník VI. Závazkové právo. Zvláštní část (§ 2055–3014).* 1. vydání. Praha: C. H. Beck, 2014, s. 1186. ISBN 978-80-7400-287-8.

[37] § 2 odst. 2 písm. k) ZPS

a standardizovaným uspořádáním pro převod a vypořádání pohledávek a dluhů vzniklých mezi členy platebního systému.“[38]

Základním kritériem při dělení platebních systémů je způsob organizace bezhotovostního platebního styku, tedy jestli je daná platba vypořádána v rámci jedné banky, anebo dochází k vypořádání mezi dvěma či více bankami. Platební systémy podle tohoto kritéria dělíme na **vnitrobankovní**, při níž jsou plátce i příjemce klienty stejné banky a peněžní prostředky neopouští danou banku, a **mezibankovní**, při níž plátce i příjemce jsou klienty různých bank a pro úspěšný převod platby je zapotřebí propojení mezi těmito bankami.[39]

Mezibankovní platební systémy lze dále dělit podle toho, jestli zúčtování platby probíhá přímým spojením přes vzájemné korespondentské účty nebo prostřednictvím třetí zúčtovací banky, u které mají jednotlivé banky otevřené účty a která provede zúčtování v rámci těchto účtů. V prvním případě se jedná o **korespondentský platební systém**, ve druhém pak o **zúčtovací (clearingový) platební systém**.[40]

Podle způsobu vypořádání lze platební systémy rozdělit také na hrubé a čisté platební systémy. V **hrubém platebním systému** dochází k převodu peněžních prostředků jednotlivě podle zpracovávaných příkazů s krytím každé jednotlivé transakce. Pokud by platba nebyla v momentě vypořádání dostatečně kryta, může dojít k jejímu neprovedení a vrácení prostředků, nebo k jejich zadržení do doby, než bude mít druhá banka dostatečné krytí na svém účtu. Podle skutečnosti, jestli vypořádání probíhá v dávkách nebo kontinuálně, je dále dělíme na **dávkový (batchový) systém** a **systém zpracování v reálném čase**. Naopak **čistý (clearingový) platební systém** funguje na principu vzájemného započtení pohledávek a závazků jednotlivých účastníků systému a zúčtování jejich sald.[41]

---

[38] JÍLEK, Josef. *Finance v globální ekonomice I. Peníze a platební styk*. 1. vydání. Praha: GRADA Publishing, a.s., 2013, s. 506. ISBN 978-80-247-3893-2.

[39] DVOŘÁK, Petr. *BANKOVNICTVÍ pro bankéře a klienty*. 3. vydání. Praha: Linde Praha, a.s., 2005, s. 289. ISBN 80-7201-515-X.

[40] Tamtéž, s. 290-293.

[41] SCHLOSSBERGER, Otakar. *Platební služby*. 1. vydání. Praha: Management Press, s. r. o., 2012, s. 177. ISBN 978-80-7261-238-3.

Jediným mezibankovním systémem, který na území České republiky zpracovává platby v českých korunách je platební systém **„CERTIS“** (Czech Express Real Time Interbank Gross Settlement System), který již téměř 30 let provozuje ČNB. Jedná se o platební systém s neodvolatelností zúčtování, jehož hlavním znakem je nemožnost jednostranného odvolání či zrušení platby po její akceptaci zúčtovacím centrem a provozování systému CERTIS, stejně jako práva a povinnosti účastníků tohoto systému, se řídí příslušnými ustanovením ZPS[42] a pravidly, které ČNB jako provozovatel systému v souladu se zákonem stanovuje a uveřejňuje na svém webu.[43] Účty mezibankovního platebního styku jsou vedeny u ČNB na základě uzavřených smluv s účastníky.[44]

ČNB provozuje také platební systém „**ABO**“ (autorizovaných platebních operací), který poskytuje platební služby organizačním složkám českého státu, předává Ministerstvu financí denní informace o účtech státní pokladny a pohybech na těchto účtech a v případě potřeby vytváří účetní výkazy pro organizační složky českého státu. Tento platební systém je napojen na systém řízení státního dluhu a slouží také pro vnitřní potřeby ČNB.[45]

Platby v eurech se na území EU vypořádávají v rámci několika platebních systémů, které můžeme rozlišit například podle jejich provozovatele. Hlavní platební systém se nazývá „**TARGET2**“ a je provozován Eurosystémem, který se skládá z ECB a národních centrálních bank států eurozóny.[46] Jedná se o hrubý zúčtovací platební systém pracující v reálném čase, který je zároveň největším eurovým platebním systémem a zpracovává především přeshraniční velkoobjemové mezibankovní platby v eurech. Účast v TARGET2 je povinná

[42] § 110 a násl. ZPS

[43] Česká národní banka. Pravidla platebního systému CERTIS. *Cnb.cz* [online]. 2019 [cit. 06. 03. 2022]. Dostupné z: https://www.cnb.cz/cs/platebni-styk/certis/pravidla-platebniho-systemu-certis/

[44] Česká národní banka. Popis systému CERTIS. *Cnb.cz* [online]. 2019 [cit. 06. 03. 2022]. https://www.cnb.cz/cs/platebni-styk/certis/popis-systemu-certis/

[45] Česká národní banka. ABO – systém pro vedení účtů a provádění plateb. *Cnb.cz* [online]. 2019 [cit. 06. 03. 2022]. https://www.cnb.cz/cs/platebni-styk/sluzby-pro-klienty/abo-system-pro-vedeni-uctu-a-provadeni-plateb/

[46] EUROPEAN CENTRAL BANK. Eurosystem mission. *Ecb.europa.eu* [online]. 2015 [cit. 06. 03. 2022]. Dostupné z: https://www.ecb.europa.eu/ecb/orga/escb/eurosystem-mission/html/index.en.html

pro všechny státy eurozóny, ale mohou se jej na dobrovolné bázi účastnit i banky a jiné finanční instituce ze zemí mimo eurozónu.[47]

Zbývající systémy provozuje společnost EBA Clearing SAS, která je vlastněna 48 významnými bankami působícími v Evropě a je založena na modelu řízení, který si zachovává neutralitu vůči jednotlivým zemím. Platební systémy společnosti EBA Clearing SAS jsou z podstaty věci celoevropské a liší se rychlostí zúčtování a objemem plateb, které zpracovávají. Jmenovitě se jedná o platební systémy **EURO1**, **STEP1**, **STEP2** a **RT1**.[48]

2.3. Platební služby

Jelikož je právní úprava silného ověření uživatele a nutnosti jeho použití navázána na konkrétní platební služby, vnímám jako relevantní se podrobněji věnovat také termínu *platební služba* a alespoň obecným způsobem uvést, co se jím rozumí, jaké druhy platebních služeb v ČR máme, jakým způsobem jsou v českém právním řádu upraveny a které subjekty jsou oprávněny je poskytovat. Tyto otázky postupně zodpovím v následujících podkapitolách.

Platební služby jsou upraveny v ZPS a jedná se o jeden z klíčových termínů tohoto zákona, protože úprava platebních služeb a jejich poskytování je jedním z hlavních cílů jeho regulace. Úprava platebních služeb vychází z unijní úpravy, konkrétně ze Směrnice PSD2, která byla transponována do českého právního řádu. Platební služby jsou v ZPS vymezeny pozitivním a negativním způsobem. Pozitivně vymezená část definice se skládá z taxativního výčtu osmi platebních služeb, přičemž v negativně vymezené části nalezneme výčet jednotlivých činností, které platebními službami ve smyslu ZPS nejsou a jsou tak z působnosti tohoto zákona vyňaty. To platí i v případě, kdy by některá z těchto činností naplnila parametry jiné, pozitivně vymezené platební služby. V neposlední řadě ZPS obsahuje také zpřesnění aplikace ZPS na obchodování s cizími měnami.

[47] EUROPEAN CENTRAL BANK. What is TARGET2? *Ecb.europa.eu* [online]. 2008 [cit. 06. 03 2022]. https://www.ecb.europa.eu/paym/target/target2/html/index.en.html

[48] EBA CLEARING. The Company. *Ebaclearing.eu* [online]. 2017 [cit. 06. 03. 2022]. https://www.ebaclearing.eu/about-eba-clearing/at-a-glance/the-company/

2.3.1. Pozitivní vymezení platebních služeb

V této podkapitole se budu postupně věnovat stručnému popisu jednotlivých činností, které jsou dle ZPS považovány za platební služby. Nejdříve vždy uvádím textaci dané platební služby (popř. obdobných platebních služeb) a následně je blíže rozvedu. Jedná se o následující:[49]

„a) služba umožňující vložení hotovosti na platební účet vedený poskytovatelem,

b) služba umožňující výběr hotovosti z platebního účtu vedeného poskytovatelem,"

Vložení hotovosti na účet a výběr hotovosti z účtu pod písm. a) a b) výše jsou nejběžnějšími platebními službami a patří mezi tzv. polohotovostní platební transakce, protože vždy u nich dochází k přeměně peněžních prostředků z hotovostních na bezhotovostní nebo naopak. Obě tyto služby jsou zároveň vázány na platební účet a proto např. vložení peněz na účet, který není platebním účtem (viz podkapitola 2.2.2 výše), nebude platební službou. Vložení peněž lze provádět jak prostřednictvím pokladních operací v provozovně poskytovatele, tak prostřednictvím k tomu určených speciálních zařízení, jakými jsou typicky bankomaty a vkladomaty.[50]

Při vložení hotovosti na platební účet má banka nebo jiný poskytovatel platební služby povinnost dodržovat určitá pravidla. Mezi tato budou patřit (i) kontrola pravosti a neporušenosti bankovek a mincí, jejich počtu a hodnoty, (ii) vyhotovení pokladního dokladu, (iii) zúčtování přijatých peněžních prostředků ve prospěch platebního účtu ve stanovené lhůtě,[51] nebo (iv) provedení identifikace složitele při vkladu nad stanovenou výši vkládané částky.[52]

Povinnost identifikace stanovuje zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů

[49] § 3 odst. 1 ZPS

[50] BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. *Zákon o platebním styku. Komentář.* Praha: Wolters Kluwer ČR, 2020, s. 56-57. ISBN 978-80-7598-788-4.

[51] Dle § 172 ZPS připíše poskytovatel částku platební transakce na platební účet příjemce neprodleně po přijetí hotovosti.

[52] SCHLOSSBERGER, Otakar. *Platební služby*. 1. vydání. Praha: Management Press, s. r. o., 2012, s. 107. ISBN 978-80-7261-238-3.

(dále jen „**AML zákon**“), podle kterého povinná osoba provede identifikaci klienta vždy, pokud hodnota obchodu překročí částku 1000 EUR a v některých dalších případech (např. pokud by se jednalo o podezřelý obchod nebo o vznik obchodního vztahu).[53]

> „***c) provedení převodu peněžních prostředků z platebního účtu, k němuž dává platební příkaz***
>
> ***1. plátce,***
>
> ***2. příjemce, nebo***
>
> ***3. plátce prostřednictvím příjemce,***
>
> ***jestliže poskytovatel neposkytuje uživateli převáděné peněžní prostředky jako úvěr,***
>
> ***d) provedení převodu peněžních prostředků z platebního účtu, k němuž dává platební příkaz***
>
> ***1. plátce,***
>
> ***2. příjemce, nebo***
>
> ***3. plátce prostřednictvím příjemce,***
>
> ***jestliže poskytovatel poskytuje uživateli převáděné peněžní prostředky jako úvěr,***“

Textace těchto dvou platebních služeb uvedených pod písm. c) a d) výše se mírně liší od úpravy ve Směrnici PSD2[54], která při úpravě těchto platebních služeb používá namísto termínu „*převod peněžních prostředků*“ termín „*provádění platebních transakcí*“. Platební transakce nicméně obsahuje nad rámec převodu také jejich vložení či výběr z platebního účtu, přičemž tyto jsou upraveny jako samostatné platební služby pod písm. a) a b) a zúžení českého zákonodárce bylo logickým krokem. Peněžními prostředky se rozumějí bankovky, mince, bezhotovostní peněžní prostředky a elektronické peníze.[55] Jejich převod probíhá vždy z platebního účtu plátce (oproti platební službě pod písm. f) – viz níže) a rozdíl mezi službami pod písm. c) a d) tak spočívá pouze v tom, jestli má plátce dostatečné množství peněžních

[53] § 7 AML zákona

[54] odst. 3 přílohy č. 1 ke Směrnici PSD2

[55] § 2 odst. 1) písm. c) ZPS

prostředků na účtu a použije je k provedení převodu, anebo jsou prostředky plátci poskytnuty na dluh.

Typickým příkladem převodu peněžních prostředků, ke kterým dává pokyn plátce, jsou úhrady, při nichž dochází k převodu peněžních prostředků z platebního účtu plátce na platební účet příjemce na základě platebního příkazu plátce danému přímo svému poskytovateli.[56] Ve druhém případě, kdy pokyn dává příjemce platby přímo poskytovateli platebního účtu plátce s jeho předchozím souhlasem, se jedná o inkaso.[57] Ve třetím případě se jedná o situaci, kdy platební příkaz dává plátce za účasti příjemce, který následně tento pokyn předá svému poskytovateli. V tomto případě se typicky bude jednat o transakce prováděné prostřednictvím platební karty nebo obdobného platebního prostředku.[58]

> „***e) vydávání a správa platebních prostředků a, je-li uživatel příjemcem, předávání platebního příkazu a zpracování platebních transakcí,***"

Tato platební služba se vztahuje k platebním prostředkům, které ZPS definuje jako „*zařízení nebo soubor postupů dohodnutých mezi poskytovatelem a uživatelem, které jsou vztaženy k osobě uživatele a kterými uživatel dává platební příkaz".* Spadat pod ně budou věci hmotné – zařízení (jakými jsou např. platební karty), tak věci nehmotné – soubory dohodnutých postupů (jakými jsou např. PIN kód, heslo či aplikace jako softwarové vybavení).[59] Oproti znění předchozího zákona č. 284/2009 Sb., o platebním styku, ve znění pozdějších předpisů (dále jen „**ZPS 2009**")[60], byla navíc doplněna služba označující se jako tzv. acquiring. Jde o službu, která spočívá v předávání platebního příkazu a zpracování platebních transakcí pro příjemce a kterou bude zpravidla poskytovat poskytovatel obchodníkovi přijímajícímu platební prostředky při placení za obchodníkovo zboží nebo jeho služby.[61]

---

[56] § 2 odst. 1) písm. f) ZPS

[57] § 2 odst. 1) písm. e) ZPS

[58] BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. *Zákon o platebním styku. Komentář.* Praha: Wolters Kluwer ČR, 2020, s. 58-59. ISBN 978-80-7598-788-4.

[59] Tamtéž, s. 14

[60] Srov. § 3 odst. 1 písm. e) ZPS 2009

[61] Důvodová zpráva k zákonu č. 370/2017 Sb., o platebním styku. Zvláštní část k § 3. 2017. Dostupné z: www.beck-online.cz

„***f) provedení převodu peněžních prostředků, při němž plátce ani příjemce nevyužívají platební účet u poskytovatele plátce (poukazování peněz),***“

Poukazování peněz je službou založenou na tom, že plátce poskytne hotovost poskytovateli platebních služeb, který příslušnou částku poukáže příjemci nebo jinému poskytovateli platebních služeb jednajícím jménem příjemce.[62] Rozdíl oproti platebním službám uvedeným pod písm. c) a d) výše je tedy v tom, že nedochází k odepsání peněžních prostředků z platebního účtu plátce.

„***g) služba nepřímého dání platebního příkazu,***“

Nepřímé dání platebního příkazu je novou platební službou, která nebyla obsažena v ZPS 2009. Začleněním této platební služby dochází k regulaci inovativních způsobů placení prostřednictvím mobilních a internetových aplikací. Tato služba byla zavedena Směrnicí PSD2, kde je nazvána jako tzv. služba iniciování platby[63] a ZPS ji definuje jako službu „*spočívající v dání platebního příkazu k převodu peněžních prostředků z platebního účtu jménem plátce poskytovatelem rozdílným od poskytovatele, který pro plátce vede daný platební účet, je-li platební příkaz dán prostřednictvím internetu“*[64] Obsahem této služby není samotný převod peněžních prostředků plátce, protože jimi poskytovatel této služby nedisponuje, ale pouze specifický způsob zadání příkazu k jejich převodu.

„***h) služba informování o platebním účtu.***“

Služba informování o platebním účtu je obdobně jako služba nepřímého dání platebního příkazu novou platební službou, která v ZPS 2009 nebyla obsažena. ZPS ji definuje jako službu „*spočívající ve sdělování informací o platebním účtu prostřednictvím internetu poskytovatelem rozdílným od poskytovatele, který vede daný platební účet*.“[65] Zákonodárce tak začleněním této platební služby reaguje na rozvoj služeb

[62] Bod 9 odůvodnění Směrnice PSD2

[63] odst. 7 přílohy č. 1 ke Směrnici PSD2

[64] § 2 odst. 1 písm. k) ZPS

[65] § 2. odst. 1 písm. l) ZPS

v oblasti správy osobních financí a umožňuje uživateli získat v rámci jedné aplikace informace o platebních účtech vedených u různých poskytovatelů.[66]

Nad rámec osmi výše uvedených platebních služeb došlo v ZPS také k zpřesnění pojmu bezhotovostní obchod s cizí měnou, který je nyní považován za převod peněžních prostředků v případě, že se jedná o „*nákup nebo prodej peněžních prostředků v české nebo cizí měně za peněžní prostředky v jiné měně, jestliže jsou peněžní prostředky od uživatele přijaty nebo uživateli dány k dispozici bezhotovostně, s výjimkou směny měn podle § 254 odst. 3*[67] *a nákupu, ke kterému dal plátce platební příkaz prostřednictvím příjemce a u něhož jsou peněžní prostředky plátci vyplaceny v hotovosti*.“ a nejde-li o investiční službu podle zákona č. 256/2004 Sb., o podnikání na kapitálovém trhu, ve znění pozdějších předpisů.[68]

2.3.2. Negativní vymezení platebních služeb

Jak již bylo uvedeno výše, negativní část vymezení platebních služeb spočívá ve výčtu výjimek, jejichž činnosti nelze považovat za platební službu ve smyslu ZPS a nedopadají tak na ně příslušná regulatorní pravidla stanovená v ZPS. To bude platit i v případě, že by některá z těchto činností naplnila parametry některé z pozitivně vymezených platebních služeb. Oproti ZPS 2009 došlo k zpřesnění terminologie a nyní se v ZPS v rámci popisu těchto činnosti používá obecný termín „*platba*“ namísto předchozího pojmu „*platební transakce*“, který byl matoucí, protože zákonodárce nazýval výjimky z působnosti zákona terminologií používanou v souvislosti s platebními službami v rámci celého ZPS 2009.

[66] BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. *Zákon o platebním styku. Komentář.* Praha: Wolters Kluwer ČR, 2020, s. 62. ISBN 978-80-7598-788-4.

[67] V tomto případě se jedná o směnu měn nabídnutou příjemcem nebo jinou osobou prostřednictvím bankomatu nebo v místě prodeje zboží nebo poskytování služeb před zahájením platební transakce.

[68] § 3 odst. 2 ZPS

Seznam výjimek je relativně rozsáhlý, a proto jsou níže uvedeny pouze některé z nich. Podle ZPS platební službou nejsou:

„***a) přeprava, sběr, zpracování a doručení bankovek a mincí.***“

O platební službu se nejedná, protože u přepravy, sběru a doručení bankovek a mincí převažuje funkce transportní nad funkcí platební a celý tento proces probíhá v hotovosti. U zpracování se naopak aplikuje speciální úprava obsažená v zákoně č. 136/2011 Sb., o oběhu bankovek a mincí, ve znění pozdějších předpisů.

„***b) směnárenská činnost,***“

Směnárenská činnost je činností, která obdobně jako zpracování bankovek a mincí podléhá speciální úpravě zvláštního zákona, kterým je v tomto případě zákon č. 277/2013 Sb., o směnárenské činnosti, ve znění pozdějších předpisů. Jak bylo uvedeno výše, tak od této činnosti je nezbytné odlišit bezhotovostní obchod s cizí měnou, který při naplnění zákonných podmínek bude považován za převod peněžních prostředků a může tak být za splnění dalších podmínek jednou z platebních služeb.

Z režimu platebních služeb jsou dále vyňaty některé činnosti související se specifickými prostředky, které buď podléhají speciálním zákonným režimům nebo mají omezený rozsah uplatnění.[69] Příkladem činností podléhajícím zvláštním zákonům lze uvést **platby prostřednictvím šeků, směnek nebo cestovních šeků**[70], jejichž praktický význam s postupem času upadá, nebo **platby prostřednictvím poštovních poukázek**, k jejichž poskytování je zapotřebí poštovní licence.[71]

Oproti ZPS 2009 jsou explicitně z režimu platebních služeb vyňaty také **stravenky**, včetně těch elektronických. Doposud bylo možné papírované stravenky podřadit po výjimku pro papírové poukázky nebo pod výjimku omezené sítě. Z režimu platebních služeb jsou vyňaty také **poukazy či jiné nástroje určené k čerpání fondu kulturních a sociálních**

[69] § 3 odst. 3 písm. c) ZPS

[70] Zákon č. 191/1950 Sb., směnečného a šekového, ve znění pozdějších předpisů.

[71] Zákon č. 29/2000 Sb., o poštovních službách, ve znění pozdějších předpisů.

potřeb (tzv. benefit karty). Obě tyto výjimky se však uplatní za předpokladu, že budou splňovat podmínky pro osvobození od daně z příjmu podle zvláštního zákona.[72]

Oproti ZPS 2009 jsou v rámci výjimky týkající se správy majetku přímo vyjmenované zvláštní předpisy, a to konkrétně zákon upravující výkon advokacie, zákon upravující činnost notářů a zákon upravující činnost soudních exekutorů. Z působnosti ZPS jsou tak vyňaty platby v rámci advokátní, notářské nebo exekuční úschovy. Výjimka ze ZPS se však nevztahuje na správu majetku podle OZ.

Dalšími činnostmi, které nebyly obsaženy v seznamu výjimek ZPS 2009 a jsou nyní explicitně vyňaty z regulace platebních služeb, jsou některé druhy plateb za digitální obsah. ZPS je definuje následovně:[73]

> „***e) platba prováděná poskytovatelem služby elektronických komunikací nebo operátorem podle zákona o elektronických komunikacích, jestliže částka platby odpovídá nejvýše 50 eurům, celková částka plateb, ke kterým dal příkaz jeden koncový uživatel, provedených za 1 měsíc odpovídá nejvýše 300 eurům a***
>
> ***1. platba slouží k zaplacení za digitální obsah nebo hlasové služby, nebo***
>
> ***2. platba je prováděna prostřednictvím elektronického komunikačního zařízení za účelem zaplacení za vstupenky nebo jízdenky nebo za charitativním účelem,*“**

Pod tyto služby lze podřadit např. nákup vyzváněcích tónů, aplikací, informačních služeb týkajících se předpovědi počasí, online nákupu jízdenek nebo vstupenek či dárcovské SMS zprávy.[74]

Závěrem uvedu ještě výjimku dopadající na ***„služby poskytovatelů technických služeb, kteří podporují poskytování platebních služeb, aniž by peněžní prostředky, které***

---

[72] § 3 odst. 3 písm. c) bod 5-7 ZPS; a Důvodová zpráva k zákonu č. 370/2017 Sb., o platebním styku. Zvláštní část k § 3. 2017. Dostupné z: www.beck-online.cz; a § 6 odst. 9. písm. b) a d) zákona č. 586/1992 Sb., o daních z příjmů

[73] § 3 odst. 3 písm. e) ZPS

[74] Důvodová zpráva k zákonu č. 370/2017 Sb., o platebním styku. Zvláštní část k § 3. 2017. Dostupné z: www.beck-online.cz

jsou předmětem platební transakce, přecházely do jejich držby.“[75] Příkladem takových služeb jsou činnosti spočívající ve zpracování a uchovávání údajů, služby na ochranu soukromí, ověřování údajů a totožnosti nebo služby komunikačních sítí, nejsou jimi však nepřímé dání platebního příkazu ani služba informování o platebním účtu, které jsou z této výjimky explicitně vyloučeny.[76]

2.3.3. Poskytovatelé platebních služeb

Poskytování platebních služeb je regulovanou činností a k jejímu provozování je zapotřebí získat veřejnoprávní oprávnění. To je však zapotřebí pouze v případě, že je činnost poskytována jako podnikání. Podnikatelem může být osoba fyzická i právnická. Aby však mohla být považována za podnikatele, musí naplnit jednu z níže uvedených zákonných definicí podnikatele obsažených v OZ:

1) „*Kdo samostatně vykonává na vlastní účet a odpovědnost výdělečnou činnost živnostenským nebo obdobným způsobem se záměrem činit tak soustavně za účelem dosažení zisku, je považován se zřetelem k této činnosti za podnikatele.*“[77] Jedná se o základní vymezení podnikatele, a to o jeho materiální definici, jejíž znaky musejí být naplněny kumulativně a za podnikatele bude taková osoba považována pouze v rámci této činnosti, přičemž v případě záležitostí nevztahujících se k podnikání bude taková osoba vystupovat jako nepodnikatel;[78]

2) výše uvedená definice byla pro účely ochrany spotřebitele a ochranu podnikatelů, kteří jsou v daném smluvním vztahu ve slabším postavení (z hlediska sjednání splatnosti plnění) dále rozšířena tak, že „*za podnikatele se považuje také každá osoba, která uzavírá smlouvy související s vlastní obchodní, výrobní nebo*

[75] § 3 odst. 3 písm. g) ZPS

[76] Důvodová zpráva k zákonu č. 370/2017 Sb., o platebním styku. Zvláštní část k § 3. 2017. Dostupné z: www.beck-online.cz

[77] § 420 odst. 1 OZ

[78] LAVICKÝ, Petr a kol. *Občanský zákoník I. Obecná část (§ 1–654). Komentář*. 2. vydání. Praha: C. H. Beck, 2022, s. 1318-1319. ISBN 978-80-7400-852-8.

obdobnou činností či při samostatném výkonu svého povolání, popřípadě osoba, která jedná jménem nebo na účet podnikatele“[79];

3) podnikatel je vymezen také formálně, a to tak, že se za něj považuje každá osoba zapsaná v obchodním rejstříku u příslušného krajského soudu[80]; a

4) v neposlední řadě existuje také vyvratitelná domněnka, podle které „*se má se za to, že podnikatelem je osoba, která má k podnikání živnostenské nebo jiné oprávnění podle jiného zákona*“[81]. Tímto jiným zákonem může být také ZPS.

Počet kategorií osob oprávněných poskytovatel platební služby bylo dle ZPS 2009 celkem deset, nicméně přijetím ZPS se jejich počet navýšil o další tři, a to konkrétně o správce informací o platebním účtu, zahraniční správce informací o platebním účtu a o držitele poštovní licence, jehož poštovní licence výslovně obsahuje službu dodání peněžní částky poštovním poukazem. Taxativní výčet všech osob oprávněných poskytovat platební služby jako podnikání (za splnění podmínek, které se pro každou kategorii liší) je dle ZPS následující:[82]

a) banky,

b) zahraniční banky,

c) spořitelní a úvěrní družstva,

d) instituce elektronických peněz,

e) zahraniční instituce elektronických peněz,

f) vydavatelé elektronických peněz malého rozsahu,

g) platební instituce,

h) zahraniční platební instituce,

i) poskytovatelé platebních služeb malého rozsahu,

[79] § 420 odst. 2 OZ

[80] § 421 odst. 1 OZ

[81] § 420 odst. 2 OZ

[82] § 5 ZPS

j) správci informací o platebním účtu,

k) zahraniční správci informací o platebním účtu,

l) držitel poštovní licence, jehož poštovní licence výslovně obsahuje službu dodání peněžní částky poštovním poukazem, a

m) ČNB.

Osobu oprávněnou poskytovat platební služby ZPS odlišuje od poskytovatele. Osobou oprávněnou je každá osoba, která spadá pod jednu z třinácti výše uvedených kategorií a je současně držitelem příslušného veřejnoprávního oprávnění, bez ohledu na to, jestli platební služby poskytuje či nikoliv. Poskytovatelem platebních služeb však bude každá osoba, která platební služby opravdu poskytuje.[83] Poskytování platebních služeb bez příslušného oprávnění je přestupkem a jako sankci lze za něj uložit pokutu do výše 20 milionů korun.[84] Řízení o takovém přestupku by projednávala ČNB.[85] Pokud budu ve zbývající části této rigorózní práce hovořit o poskytovateli platební služby, je tím na mysli takový poskytovatel, který je současně držitelem příslušného veřejnoprávního oprávnění, pokud není explicitně uvedeno jinak.

2.4. Regulace bezhotovostního platebního styku

Platební styk napomáhá s přesuny finančních prostředků mezi jednotlivými subjekty v ekonomice a jeho plynulost a hospodárnost je důležitá pro její řádné fungování. Jelikož v rámci platebního styku dochází k nakládání s finančními prostředky fyzických i právnických osob, je pro zajištění jeho spolehlivosti, efektivnosti, a především bezpečnosti nutno platební styk regulovat.

V České republice je bezhotovostní platební styk regulován především na úrovni zákonné, na kterou poté navazují sekundární právní předpisy ve formě vyhlášek vydávaných ČNB. Existují také předpisy doporučujícího charakteru, kterými jsou především stanoviska,

[83] BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. *Zákon o platebním styku. Komentář.* Praha: Wolters Kluwer ČR, 2020, s. 86. ISBN 978-80-7598-788-4.

[84] § 234 odst. 1 písm. a) a 234 odst. 4. písm. d) ZPS

[85] § 236 odst. 1 písm. d) ZPS

úřední sdělení či metodiky vydávané ČNB. Tyto doporučující předpisy sice nejsou přímo právně závazné, ale subjekty finančního trhu se jimi standardně řídí.

Na unijní úrovni dochází ke snaze vytvořit efektivní a integrovaný trh platebních služeb v EU. Bezhotovostní platební styk je hojně regulován sekundárním právem, a to především nařízeními a směrnicemi. Tyto dále doplňují právně závazné prováděcí akty Evropské komise a akty v přenesené pravomoci přijímané s cílem definovat prováděcí opatření. Obdobně jako na české úrovni jsou jednotlivými orgány EU vydávána také různá doporučení, stanoviska nebo obecné pokyny, které nemají právní závaznost a jsou pouze doporučujícího charakteru. V oblasti platebního styku se nejčastěji setkáme s obecnými pokyny či stanovisky vydanými Evropským orgánem pro bankovnictví (dále jen „**EBA**“).

Jelikož je právní úprava bezhotovostního platebního styku rozsáhlá a její důkladný rozbor by vystačil na téma samostatné práce, tak níže pouze stručně nastíním vývoj v oblasti regulace a uvedu výčet několika klíčových právních předpisů, které se v oblasti bezhotovostního platebního styku aplikují.

2.4.1. Vývoj regulace bezhotovostního platebního styku

První jednotná regulace platebního styku v České republice byla přijata až v rámci příprav českého právního řádu na vstup do EU. Základní právní normou pro oblast platebního styku se stal zákon č. 124/2002 Sb., o převodech peněžních prostředků, elektronických platebních prostředcích a platebních systémech (zákon o platebním styku), který transponoval do českého právního řádu ustanovení tří v té době účinných unijních směrnic. Jak napovídá jeho název, tak jeho předmětem byla úprava tří oblasti převzatých z těchto směrnic, a to konkrétně (i) provádění převodu peněžních prostředků, (ii) vydávání a užívání elektronických platebních prostředků a (iii) vznik a provozování platebních systémů, přičemž ve všech těchto oblastech byl kladen velký důraz na práva klienta jako spotřebitele.[86]

V roce 2007 byla na unijní úrovni přijata Směrnice PSD, jejímž cílem bylo sjednotit regulaci bezhotovostního platebního styku a přispět k možnosti zavedení jednotné oblasti pro

[86] SCHLOSSBERGER, Otakar a Marcela SOLDÁNOVÁ. *Platební styk*. 3. vydání. Praha: Bankovní institut, a.s., 2005, s. 18-19. ISBN 80-7265-072-6.

platby v eurech. Jelikož došlo k celé řadě změn, které by vyžadovaly velmi rozsáhlou novelizaci českého zákona z roku 2002, byl v České republice přijat nový ZPS 2009, který zákon z roku 2002 v celém rozsahu nahradil. Došlo např. k zavedení termínu platební účet, platební služba nebo platební instituce. ZPS 2009 rozsáhle upravoval soukromoprávní část poskytování platebních služeb.

S rychlým rozvojem technologií, nárůstem počtu bezhotovostních transakci prostřednictvím platebních karet a internetu vznikla tzv. Zelená kniha nazvaná „*Na cestě k integrovanému evropskému trhu plateb prováděných kartou, přes internet a pomocí mobilního telefonu*“, jejímž účelem bylo zahájit veřejnou diskusi za účelem vytvořené nové právní úpravy, která by reagovala na tento technologický vývoj. Výsledkem těchto diskusí a s nimi souvisejících prací bylo přijetí Směrnice PSD2, která rozšiřuje měnovou působnost oproti předchozí Směrnici PSD, navyšuje požadavky na bezpečnost při poskytování platebních služeb, posiluje práva spotřebitelů při platbách mimo EU a je výsledkem snahy zefektivnit trh platebních služeb v rámci EU. Transpozicí Směrnice PSD2 došlo na území ČR k přijetí ZPS.

2.4.2. Právní úprava na území EU

V oblasti platebních služeb je jedním z nejdůležitějších předpisů Směrnice PSD2 vytvářející základní právní rámec pro jejich poskytování, kterou měly členské státy EU transponovat do svých právních řádů do 13. ledna 2018. Na základě Směrnice PSD2 má Evropská komise pravomoc přijímat v přenesené působnosti regulační technické normy. Tyto byly vydány i ve vztahu k silnému ověření uživatele a podrobněji se jim budu věnovat v následujících kapitolách.

Spolu se Směrnicí PSD2 bylo přijato **nařízení Evropského parlamentu a Rady (EU) 2015/751 ze dne 29. dubna 2015 o mezibankovních poplatcích za karetní platební transakce**, které stanoví pravidla v oblasti poplatků obchodníků za platební transakce prostřednictvím platebních karet, zejména jejich maximální výši a omezení zavádění dalších poplatků s nimi souvisejících.

V oblasti poplatků lze ještě zmínit **směrnici Evropského parlamentu a Rady 2014/92/EU ze dne 23. července 2014 o porovnatelnosti poplatků souvisejících s platebními účty, změně platebního účtu a přístupu k platebním účtům se základními**

prvky, která stanoví pravidla týkající se transparentnosti a porovnatelnosti poplatků účtovaných spotřebitelům za jejich platební účty vedené EU a která definuje základní rámec pro pravidla a podmínky, v souladu s nimiž mají členské státy povinnost zaručit spotřebitelům právo otevřít si a používat v EU platební účty. Účelem této směrnice bylo především posílit ochranu a práva spotřebitelů v oblasti platebních účtů, zvýšit transparentnost poskytovaných informací a podpořit jednotný trh v rámci EU.

V oblasti přeshraničních plateb došlo v roce 2021 ke kodifikaci úpravy a bylo přijato nové **nařízení Evropského parlamentu a Rady (EU) č. 2021/1230 ze dne 14. července 2021 o přeshraničních platbách v Unii**, které nahradilo původní nařízení z roku 2009. Toto nařízení stanoví pravidla pro přeshraniční platby denominované v eurech (tzv. SEPA platby), kdy členské státy s jinou národní měnou mají možnost rozšířit uplatňování tohoto nařízení i na svoji měnu. Česká republika tak prozatím neučinila. S platbami v eurech dále souvisí také **nařízení Evropského parlamentu a Rady (EU) č. 260/2012 ze dne 14. března 2012, kterým se stanoví technické a obchodní požadavky pro úhrady a inkasa v eurech a kterým se mění nařízení (ES) č. 924/2009**.

Další oblastí, které se regulace v posledních letech hojně věnuje, je oblast praní špinavých peněz. Rok 2015 byl v tomto ohledu přelomový, protože byly přijaty dva důležité unijní předpisy. Prvním z nich bylo **nařízení Evropského parlamentu a Rady (EU) 2015/847 ze dne 20. května 2015 o informacích doprovázejících převody peněžních prostředků a o zrušení nařízení (ES) č. 1781/2006**, které mělo za cíl přiblížit se mezinárodním standardům pro boj proti praní peněz a financování terorismu a šíření zbraní, které v roce 2012 přijal Finanční akční výbor.[87] Toto nařízení stanoví pravidla pro informace o plátcích a příjemcích doprovázející převody peněžních prostředků v jakékoli měně v případech, kdy je alespoň jeden z poskytovatelů platebních služeb zapojených do daného převodu peněžních prostředků a má sídlo v členském státě EU.

Druhým předpisem byla **směrnice Evropského parlamentu a Rady (EU) 2015/849 ze dne 20. května 2015 o předcházení využívání finančního systému k praní peněz nebo financování terorismu, o změně nařízení Evropského parlamentu a Rady (EU) č. 648/2012 a o zrušení směrnice Evropského parlamentu a Rady 2005/60/ES a směrnice**

[87] Bod 3 odůvodnění tohoto nařízení

Komise 2006/70/ES[88] (dále jen „**AML Směrnice**“). Tato směrnice stanovuje například povinnosti hloubkové kontroly klienta, informování o skutečném vlastnictví a související oznamovací povinnosti. Do českého právního řádu byla transponována novelizací AML zákona.

2.4.3. Právní úprava na území České republiky

Základní právní normou v oblasti platebního styku je v České republice ZPS. Tento zákon přijatý v roce 2017 s účinností od 13. ledna 2018 do českého právního řádu transponoval Směrnici PSD2 a obsahově tak do značné míry vychází z unijní legislativy. ZPS je rozdělen na celkem devět části. V té úvodní nalezneme obecná ustanovení a definice, která se používají napříč ZPS. Druhá část se zaměřuje na podmínky poskytování platebních služeb a vydávání elektronických peněz a stanoví regulaci tzv. nebankovních poskytovatelů platebních služeb. Třetí část je zaměřena na platební systémy a navazuje na ni část zaměřená na regulaci soukromoprávních vztahů při poskytování platebních služeb a vydávání elektronických peněz. Pátá část se zabývá platebním účtem, jeho specifiky a představuje transpozici směrnice o platebních účtech.[89] Šestá část, které se v dalších kapitolách budu věnovat podrobněji, je zaměřena na bezpečnost platebního styku a obsahuje úpravu silného ověření uživatele. Na ni navazuje část stanovující přestupky, kterých se subjekty v oblasti platebního styku mohou dopustit a dále část týkající se dohledu nad povinnostmi stanovenými v ZPS. V poslední části pak nalezneme společná, přechodná a závěrečná ustanovení.

ČNB pravidelně vydává nejen stanoviska, sdělení a další dokumenty doporučujícího charakteru, ale také právně závazné prováděcí předpisy k ZPS ve formě vyhlášek, z nichž lze například zmínit následující:

[88] Těmito jsou Směrnice Evropského parlamentu a rady (EU) 2018/843 ze dne 30. května 2018, kterou se mění směrnice (EU) 2015/849 o předcházení využívání finančního systému k praní peněz nebo financování terorismu a směrnice 2009/138/ES a 2013/36/EU, a směrnice Evropského parlamentu a Rady (EU) 2019/2177 ze dne 18. prosince 2019, kterou se mění směrnice 2009/138/ES o přístupu k pojišťovací a zajišťovací činnosti a jejím výkonu (Solventnost II), směrnice 2014/65/EU o trzích finančních nástrojů a směrnice (EU) 2015/849 o předcházení využívání finančního systému k praní peněz nebo financování terorismu.

[89] Směrnice Evropského parlamentu a Rady 2014/92/EU ze dne 23. července 2014 o porovnatelnosti poplatků souvisejících s platebními účty, změně platebního účtu a přístupu k platebním účtům se základními prvky.

(i) vyhláška č. 401/2021 Sb., o předkládání některých výkazů v oblasti platebního styku České národní bance,

(ii) vyhláška č. 150/2019 Sb., o hlášení bezpečnostních a provozních rizik v oblasti platebního styku,

(iii) vyhláška č. 141/2018 Sb., o hlášení závažných bezpečnostních a provozních incidentů osobami oprávněnými poskytovat platební služby,

(iv) vyhláška č. 74/2018 Sb., o službách spojených s platebním účtem, na které se vztahuje jednotné označení,

(v) vyhláška č. 7/2018 Sb., o některých podmínkách výkonu činnosti platební instituce, správce informací o platebním účtu, poskytovatele platebních služeb malého rozsahu, instituce elektronických peněz a vydavatele elektronických peněz malého rozsahu.

Další specifické oblasti související s bezhotovostním platebním stykem lze nalézt v některých dalších zákonech, které se úpravou zaměřují vždy na konkrétní subjekty či konkrétní oblast regulace. Takových předpisů je mnoho a příkladem lze uvést **zákon č. 21/1992 Sb., o bankách** regulující banky jako jedny z největších poskytovatelů platebních služeb, **zákon č. 229/2002 Sb., o finančním arbitrovi**, který stanoví pravidla pro mimosoudní řešení sporů mimo jiné v oblasti platebních služeb, nebo také **zákon č. 6/1993 Sb., o České národní bance, zákon č. 87/1995 Sb., o spořitelních a úvěrních družstvech** či **AML zákon**.

3. Silné ověření uživatele

3.1. Bezpečnost a vývoj právní úpravy

Základním předpokladem pro řádné fungování finančních trhů je zajištění jejich bezpečnosti. K dosažení tohoto cíle je nezbytné využít řadu nástrojů (jakými jsou např. nastavení pravidel pomocí regulace nebo zajištění dostatečné míry ochrany používaných technologií a systémů), které zároveň také napomáhají k vnímání trhů jako bezpečných z pohledu jejich účastníků. Jelikož je cílem většiny podnikatelských subjektů vytvářet zisk a provozovat svoji činnost efektivně za současné minimalizace nákladů s provozem spojených, je zapotřebí nastavit pravidla regulace v oblasti bezpečnosti vhodným způsobem tak, aby to bylo ekonomicky únosné pro podnikatelské subjekty a zároveň aby bylo v co nejvyšší míře dosaženo požadovaného cíle.

S rozvojem digitalizace a dnes již každodenním používáním internetu na pracovišti i v běžném životě je z hlediska bezpečnosti klíčová především technická stránka fungování finanční trhů. Eliminace rizik lze dosáhnout za vytvoření stabilního a zabezpečeného technického zázemí při celé řadě činností, které jsou v rámci finančních trhů a oblasti platebních služeb provozovány na denní bázi (např. provoz platebních systémů a vypořádání platebních transakcí, fungování internetového bankovnictví pro korporátní i retailové klienty nebo třeba činnost regulátorů a finančních subjektů a technické zabezpečení chodu jejich interních systémů). Nedostatečného technického zabezpečení se opakovaně snaží zneužít subjekty, jejichž cílem je často tato zabezpečení prolomit prostřednictvím hackerských útoků, počítačových virů nebo jiných podvodných praktik zpravidla s cílem nelegálně získat peníze nebo citlivé informace o uživatelích.

Neméně důležitým nástrojem je právní regulace, kdy se zákonodárce snaží nastavit pravidla pro fungování finančních trhů prostřednictvím vydávání právních předpisů, které jsou závazné pro jejich jednotlivé účastníky a které jsou opakovaně novelizovány a nahrazovány předpisy novými tak, aby co nejlépe odpovídaly technologickému vývoji a ekonomickým požadavkům efektivity.

V oblasti platebního styku je jedním z nejdůležitějších aspektů bezpečnosti dostatečné zabezpečení plateb, a to především těch bezhotovostních. V zájmu snížení rizik a důsledků neautorizovaných nebo nesprávně provedených platebních transakcí byla

ve Směrnici PSD poprvé zavedena úprava odpovědnosti za neautorizované nebo nesprávně provedené platební transakce, která byla následně transponována do ZPS 2009 (dosavadní zákon o platebním styku z roku 2002 obdobnou úpravu neobsahoval). Za neautorizované platební transakce jsou považovány takové platební transakce, ke kterým nedal plátce souhlas (v případě opakovaných transakcí, kdy plátce udělil souhlas jen jedné či několika z nich), dal souhlas neplatně nebo jej platně odvolal a zároveň takové platební transakce, ke kterým dala souhlas osoba odlišná od plátce a současně k tomu nebyla oprávněna.[90] Nesprávně provedené platební transakce jsou pak takové, které nebyly provedeny řádně a včas. Příkladem lze uvést transakce s nižší/vyšší hodnotou nebo transakce připsané na jiný než požadovaný účet.[91]

U neautorizovaných platebních transakcí spočívala odpovědnost poskytovatele plátce primárně v restituční povinnosti, tedy navrácení účtu plátce do původního stavu. Jestliže tento postup nepřipadal v úvahu, tak ve vrácení částky plátci. V oblasti bezpečnosti ZPS 2009 ukládal povinnosti také uživatelům (plátcům) spočívající v povinnostech (a) používat platební prostředek v souladu s rámcovou smlouvou, zejména byl povinen okamžitě poté, co obdržel platební prostředek, přijmout veškerá přiměřená opatření na ochranu jeho personalizovaných bezpečnostních prvků, a (b) bez zbytečného odkladu po zjištění oznámit poskytovateli nebo osobě jím určené ztrátu, odcizení, zneužití nebo neautorizované použití platebního prostředku.[92] Plátce byl odpovědným za neautorizovanou platební transakci v plném rozsahu, pokud ztrátu platebního prostředku způsobil svým podvodným jednáním nebo tím, že úmyslně nebo z hrubé nedbalosti porušil některou z povinností uvedených výše pod písmeny (a) a (b). Odpovědnost plátce byla omezena částkou 150 euro v případech, kdy byla neautorizovaná platební transakce způsobená ztrátou nebo odcizením platebního prostředku nebo jeho zneužitím v situacích, kdy plátce nezajistil ochranu svých personalizovaných bezpečnostních prvků.[93] Plátce však byl zbaven odpovědnosti

[90] BERAN, Jiří, Daniela DOLEŽALOVÁ, Dalibor STRNADEL a Alice ŠTĚPÁNOVÁ. *Zákon o platebním styku. Komentář*. 1. vydání. Praha: C. H. Beck, 2011, s. 548. ISBN 978-80-7400-369-1; a
PROCTOR, Charles. *The Law and Practise of International Banking*. Londýn: Oxford University Press, 2010, s. 97-98. ISBN 978-0-19-929186-1.

[91] Tamtéž, s. 574.

[92] § 101 ZPS 2009

[93] § 116 odst. 1 ZPS 2009

v případech, kdy ztráta vznikla až po jeho oznámení nebo kdy poskytovatel nezajistil, aby měl plátce k dispozici prostředky k oznámení takové ztrátu, odcizení nebo zneužití.[94]

V případě nesprávně provedené platební transakce nesl odpovědnost poskytovatel plátce, ledaže plátci (popř. poskytovateli příjemce) prokázal, že částka nesprávně provedené platební transakce byla připsána na účet poskytovatele příjemce. Pokud došlo k nesprávně provedené platební transakci, tak měl poskytovatel plátce (a v případě, že částka byla připsána na účet poskytovatele příjemce, tak poskytovatel příjemce) povinnost tuto transakci napravit. Jednotlivé způsoby nápravy byly v ZPS 2009 blíže specifikovány s ohledem na to, jestli plátce trval/netrval na provedení transakce a kdo byl za nesprávně provedenou transakci odpovědný.[95]

Aby bylo možné určovat budoucí směr regulace a vytvářet jednotná preventivní opatření a mezinárodní standardy, je nezbytné sbírat a vyhodnocovat data o trestné činnosti v oblasti platebního styku týkající se podvodných aktivit s platebními kartami a platebními transakcemi. Od roku 2012 začala ECB zveřejňovat souhrnné zprávy o podvodech s platebními kartami. Tyto se zaměřují na platby v jednotné oblasti pro platby v eurech (tzv. SEPA platby). První report analyzoval data za léta 2007 až 2010 a poukázal na celkově klesající tendenci objemu podvodů, a to především v oblastech podvodů s bankomaty a s platebními terminály v místě plateb. Zlepšení zabezpečení platebních karet a základní platební infrastruktury ECB uvedla jako hlavní důvod, proč byly podvody s bankomaty a platebními terminály v roce 2010 nižší než v roce 2007. Jako nejvýznamnější zlepšení bylo uvedeno širší přijetí standardu EMV, který je založen na čipu nabízejícím silnější bezpečnostní prvky oproti klasickým magnetickým proužkům, a to jak pro fyzickou kartu (protože na rozdíl od magnetických proužků nelze čip snadno duplikovat), tak pro technologickou infrastrukturu, která stojí za každou platební transakcí. Rostoucí tendenci naopak bylo možné pozorovat u podvodů s platbami bez přítomnosti karty, tj. platbami prostřednictvím pošty, telefonu nebo internetu (tzv. CNP platby), protože nová bezpečnostní opatření se při nich neuplatnila. Podíl CNP plateb na celkovém objemu podvodů se během období 2007-2010 zvýšil ze 47 % na 50 % a jejich hodnota za stejné období vzrostla

[94] § 116 odst. 2 ZPS 2009

[95] § 117 a 118 ZPS 2009

z 571 milionů EUR (v roce 2007) na 648 milionů EUR (v roce 2010). Celková hodnota podvodů za rok 2010 čítala 1,26 miliardy EUR.[96]

Ze třetí zprávy ECB o podvodech s platebními kartami, která analyzovala data za rok 2012, je zřejmý trend spočívající v nárůstu podílu CNP plateb na celkovém objemu podvodů (60 % za rok 2012) společně s jejich rostoucí hodnotou, která činila 794 milionů EUR za rok 2012, což byl 21,2% nárůst oproti roku 2011 (největší pozorovaný mezi sledovanými kategoriemi). Příčinou tohoto nárůstu byly dle ECB především podvodné aktivity spojené s platbami prostřednictvím internetu. Nárůst podvodů s CNP platbami tak opakovaně ukázal, že existoval silný důvod pro urychlené přijetí účinnějších bezpečnostních opatření na ochranu CNP plateb. CNP platby byly tradičně chráněny pomocí třímístného bezpečnostního kódu uvedeného na zadní straně platební karty. Jelikož však tyto kódy byly vytištěny přímo na kartě, umožňovaly pouze omezenou míru zabezpečení a někteří vydavatelé proto zavedli dodatečná statická hesla podobná PIN kódům. Na získání a zneužití těchto statických hesel se proto často zaměřovali podvodníci.[97]

V rámci výše uvedené třetí zprávy ECB o podvodech s platebními kartami ECB zároveň upozorňovala na některá nová rizika spojená s bezpečností plateb vznikající díky používání mobilních telefonů a technologií pro provádění plateb. Za tato rizika považovala především (a) tehdejší generaci mobilních telefonů a jejich operačních systémů, které nebyly obecně navrženy s ohledem na bezpečnost plateb, (b) používání rádiové technologie pro přenos citlivých platebních údajů a osobních údajů, které vystavovalo mobilní platby rizikům, kterým jiné platby nečelily, (c) nástup nových aktérů, kteří se podíleli na platbách prováděných prostřednictvím mobilních telefonů (např. provozovatelé telekomunikačních sítí), a (d) nižší míru povědomí široké veřejnosti o rizicích spojených s prováděním plateb

[96] EUROPEAN CENTRAL BANK. First ECB report on card fraud shows chips have increased the security of physical transactions. *Ecb.europa.eu* [online]. 2012 [cit. 30. 07. 2022]. https://www.ecb.europa.eu/press/pr/date/2012/html/pr120725_1.en.html; a
EUROPEAN CENTRAL BANK. Report on Card Fraud. *Ecb.europa.eu* [online]. 2012 [cit. 30. 07. 2022]. https://www.ecb.europa.eu/pub/pdf/cardfraud/cardfraudreport201207en.pdf

[97] EUROPEAN CENTRAL BANK. Third Report on Card Fraud. *Ecb.europa.eu* [online]. 2014 [cit. 30. 07. 2022]. https://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201402en.pdf

při používání mobilních telefonů oproti rizikům spojeným s platbami za použití notebooků nebo stolních počítačů.[98]

V zájmu dalšího zvýšení bezpečnosti CNP plateb zmínila ECB ve třetí zprávě také doporučení Evropského fóra pro bezpečnost maloobchodních plateb (dále jen „**SecuRe Pay**“). SecuRe Pay bylo založeno v roce 2011 jako dobrovolná iniciativa mezi orgány dohledu nad poskytovateli platebních služeb, nad platebními systémy a platebními nástroji na území EU a Evropského hospodářského prostoru (mezi které se řadila i ČNB) s cílem usnadnit vývoj tzv. harmonizovaného evropského přístupu k řešením v oblasti bezpečnosti elektronických platebních služeb a nástrojů a v této souvislosti vydávat doporučení.[99]

V lednu 2013 byla zveřejněna první sada doporučení o bezpečnosti internetových plateb. Mezi hlavní doporučení SecuRe Pay patřila:[100]

a) chránit iniciaci internetových plateb a přístup k citlivým platebním údajům silnou autentizací zákazníka;

b) omezit počet pokusů o přihlášení nebo autentizaci, definovat pravidla pro automatické odhlášení internetových platebních služeb a stanovit časové limity pro platnost autentizace;

c) zavést mechanismy sledování platebních transakcí, které mají předcházet těm podvodným, odhalit je a včas zablokovat;

d) zavést více úrovní bezpečnostní ochrany s cílem zmírnit zjištěná rizika; a

[98] Tamtéž.

[99] EUROPEAN CENTRAL BANK. ECB releases final Recommendations for the security of internet payments and starts public consultation on payment account access services. *Ecb.europa.eu* [online]. 2013 [cit. 30. 07. 2022]. https://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html;
a EUROPEAN CENTRAL BANK. Recommendations for the security of internet payments. *Ecb.europa.eu* [online]. 2013 [cit. 30. 07. 2022]. https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf

[100] Tamtéž.

e) poskytovat zákazníkům asistenci a poradenství ohledně osvědčených postupů v oblasti online bezpečnosti, nastavit upozornění a poskytnout zákazníkům nástroje, které jim budou napomáhat ve sledování transakcí.

Na doporučení SecuRe Pay navázala EBA, která jako člen SecuRe Pay souhlasila s tím, že tato doporučení přepracuje do podoby obecných pokynů s úmyslem vytvořit právní základ pro budoucí implementaci těchto doporučení na území všech členských států EU. V návaznosti na veřejnou konzultaci EBA vydala v prosinci roku 2014 obecné pokyny k bezpečnosti internetových plateb, které vycházely z již platných pravidel Směrnice PSD a stanovily minimální soubor požadavků v oblasti bezpečnosti internetových plateb, který byl následně dále rozpracován ve Směrnici PSD2. V těchto obecných pokynech se poprvé objevila úprava silné autentizace klienta, které se podrobněji budu věnovat v následující kapitole.[101]

3.2. Úvod a vymezení silného ověření uživatele

Potřeba aktualizace právní úpravy na evropské úrovni vyústila v přijetí Směrnice PSD2, jejímž cílem bylo především přispět k rozvoji větší integrace, transparentnosti a efektivitě evropského harmonizovaného trhu plateb, zlepšit a zaručit rovné podmínky pro stávající i nové poskytovatele platebních služeb, zaručit vysokou úroveň ochrany spotřebitelů a v neposlední řadě zvýšit bezpečnost a zabezpečení plateb.

Jednou z nejvýznamnějších změn oproti Směrnici PSD je zvýšený akcent na bezpečnost a zabezpečení elektronických plateb a související zajištění ochrany uživatelů z důvodu nárůstu bezpečnostních rizik souvisejících s elektronickými platbami. Tato rizika byla způsobena větší technickou složitostí elektronických plateb, kontinuálním nárůstem plateb přes internet, pomocí mobilních telefonů nebo přes jiné kanály komunikace na dálku (u nichž není relevantní, kde se platební prostředek nebo zařízení použité pro iniciaci platební transakce nachází) a v neposlední řadě také vznikem nových platebních služeb. Směrnice PSD2 tak stanovila povinnost zavést některá bezpečnostní opatření, která by měla odpovídat

[101] European Banking Authority. Final guidelines on the security of the internet payments. *Eba.europa.eu* [online]. 2014 [cit. 30. 07. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/934179/f27bf266-580a-4ad0-aaec-59ce52286af0/EBA-GL-2014-12%20%28Guidelines%20on%20the%20security%20of%20internet%20payments%29_Rev1.pdf

míře rizika spojené s konkrétní platební službou. Zřejmá byla potřeba zajistit důvěrnost, integritu a bezpečné používání osobních bezpečnostních údajů, nastavit pravidla pro používání technologií, které budou schopny zaručit bezpečné ověření totožnosti uživatele, a v maximální možné míře omezit rizika vzniku podvodů.[102]

Směrnice PSD2 navázala na obecné pokyny EBA z roku 2014 k bezpečnosti internetových plateb a zavedla pro elektronické platební transakce jako obecné pravidlo povinnost vyžadovat v některých případech silné ověření uživatele (anglicky: *strong customer authentication,* dále jen „**SCA**"). Podle Směrnice PSD2 je SCA definováno jako:

„*ověření založené na použití dvou nebo více navzájem nezávislých prvků z kategorie znalost (to, co ví pouze uživatel), držení (to, co drží pouze uživatel) a inherence (to, čím uživatel je), kdy nesplněním jednoho z nich není ovlivněna spolehlivost ostatních; postup je navržen tak, aby byla chráněna důvěrnost ověřovacích údajů*"[103]

Český zákonodárce při transpozici Směrnice PSD2 do českého právního řádu definici SCA ve větší míře převzal a v ZPS pojem definoval jako:

„*ověření, které je založeno na použití alespoň 2 z těchto prvků:*

a) údaje, který je znám pouze uživateli,
b) věci, kterou má uživatel ve své moci,
c) biometrických údajů uživatele.

Prvky podle odstavce 3 musí být vzájemně nezávislé a prolomení jednoho prvku nesmí ovlivnit spolehlivost prvků ostatních. Postup ověření musí zabránit zneužití prvků, které jsou k ověření používány."[104]

Zavedení SCA je relevantní ve vztahu k odpovědnosti za ztrátu z neautorizovaných transakcí, jejímuž legislativnímu vývoji jsem se věnoval výše. Jak vyplývá z definice SCA, tak povinnost požadovat SCA má osoba oprávněná poskytovat platební služby,

[102] Body 5, 6, 7, 95 a 96 odůvodnění Směrnice PSD2; a
European Commission. Payment services directive – frequently asked questions. *Ec.europa.eu* [online]. 2018 [cit. 06. 08. 2022]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/memo_15_5793

[103] Článek 4 odst. 30 Směrnice PSD2

[104] § 223 odst. 3 a 4 ZPS

která v případě, že nepožaduje silné ověření uživatele dle § 223 odst. 1 nebo 6 (těmto situacím se budu podrobněji věnovat ve čtvrté části této práce) nese odpovědnost za neautorizovanou platební transakci v plné výši, pokud současně plátce nejednal podvodně.[105] Před nabytím účinnosti novely ZPS č. 129/2022 Sb. původní text tohoto ustanovení vázal odpovědnost na porušení povinnosti uplatnit silné ověření uživatele. Novelizací došlo k zpřesnění tohoto ustanovení, aby řádně reflektovalo možnost aplikace některé z výjimek.

Úpravu vymezení SCA považuji v některých částech za příliš obecnou, což bylo z důvodu snahy o docílení technické neutrality cílem zákonodárce, avšak v praxi vyvstává řada výkladových nejasností, které mohou způsobovat nejistotu pro subjekty poskytující platební služby, na které úprava SCA dopadá a které musí provoz svojí činnosti přizpůsobovat nové právní úpravě. Tomu odpovídá skutečnost, že od doby přijetí Směrnice PSD2 bylo k aplikaci SCA a jeho jednotlivým prvkům položeno (a z převážné části zodpovězeno) již přes 100 dotazů.[106] Z tohoto důvodu se v následujících kapitolách budu podrobněji věnovat nejdříve jednotlivým prvkům SCA a v další části práce následně případům použití SCA a výjimek z povinnosti jeho použití.

3.3. Jednotlivé prvky silného ověření uživatele

3.3.1. Znalost

Prvním prvkem SCA je údaj, který je znám pouze uživateli. Konkrétní vymezení toho, co je považováno za takový údaj, v ZPS ani ve Směrnice PSD2 nenalezneme. Typicky se bude jednat například o přihlašovací heslo do internetového bankovnictví nebo PIN používaný pro platební karty.[107] Abychom dospěli k závěru, jestli lze údaj použít v rámci SCA, bude nezbytné v každém případě individuálně posuzovat, jestli se opravdu jedná o údaj, který je znám pouze uživateli a z povahy věci také příslušné osobě oprávněné poskytovat platební služby.

---

[105] § 182 odst. 3 písm. c) ZPS

[106] European Banking Authority. Single Rulebook Q&A. *Eba.europa.eu* [online]. 2018 [cit. 06. 08. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa

[107] Důvodová zpráva k zákonu č. 370/2017 Sb., o platebním styku. Zvláštní část k § 223. 2017. Dostupné z: www.beck-online.cz

Před zavedením povinnosti SCA ve Směrnici PSD2 byly v době, kdy bylo SCA používáno pouze na základě doporučujících obecných pokynů EBA, při ověřování platebních transakcí běžně používány jako znalostní prvek údaje o platební kartě, jakými jsou datum expirace a CVV kód vytištěný obvykle na zadní straně platební karty. Podle názorů EBA nicméně tyto údaje již samy o sobě nenaplňují požadavky SCA, protože jako prvek dvojí kategorie (znalost a držení) nejsou vzájemně nezávislé a z tohoto důvodu by pro účel SCA musely být doplněny o jiný, na nich nezávislý prvek. Obdobně se EBA staví k uživatelskému jménu (user ID)[108]. Je však otázkou, jestli uživatelské jméno, které nebude generické (například e-mailová adresa uživatele nebo jeho příjmení), může naplnit prvek znalosti? Autoři komentáře k ZPS se v takovém případě domnívají, že ano.[109] K jejich názoru bych se přiklonil, avšak pouze za situace, kdy dané uživatelské jméno bude vždy náhodně vygenerováno pro každého uživatele, nebude žádným způsobem navázáno na osobní údaje uživatele a uživatel pod ním bude vystupovat pouze ve vztahu k dané osobě oprávněné poskytovat platební služby (a nikoliv např. ve vztahu ke třetím stranám).

Nařízení Evropské komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace (dále jen „**Nařízení RTS**“) stanoví povinnost poskytovatelům platebních služeb přijmout opatření ke zmírnění rizika získání prvků SCA z kategorie znalost neoprávněnými stranami nebo jejich sdělení těmto stranám. Nad rámec této povinnosti platí, že použití prvků z kategorie znalost plátcem je podmíněno opatřeními k zmírnění rizika, která mají zabránit jejich sdělení neoprávněným stranám.[110]

---

[108] European Banking Authority. Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC. *Eba.europa.eu* [online]. 2018 [cit. 07. 08. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2137845/0f525dc7-0f97-4be7-9ad7-800723365b8e/Opinion%20on%20the%20implementation%20of%20the%20RTS%20on%20SCA%20and%20CSC%20%28EBA-2018-Op-04%29.pdf

[109] BERAN, Jiří, Daniela DOLEŽALOVÁ, Dalibor STRNADEL a Alice ŠTĚPÁNOVÁ. *Zákon o platebním styku. Komentář*. 1. vydání. Praha: C. H. Beck, 2011, s. 778. ISBN 978-80-7400-369-1.

[110] Článek 6 Nařízení RTS

Nařízení RTS dále stanoví, že je nutné vyžadovat odpovídající bezpečnostní charakteristiky samotného prvku znalosti, jakými jsou jeho délka nebo jeho složitost. Nastavení vhodné délky a složitosti tohoto prvku tak může být jedním z opatření (nikoliv však výlučným), které sníží riziko jeho odhalení.[111] Typicky se bude jednat o požadavek na použití kombinace několika prvků z kategorie velkých/malých písmen, číslic nebo speciálních znaků. Co se samotné délky týče, tak určité vodítko lze nalézt v odpovědi EBA k dotazu vznesenému v rámci Q&A 4053[112] ke Směrnici PSD2 týkajícího se délky ověřovacího kódu generovaného při procesu SCA (konkrétně dotaz směřoval na možnost použití třímístného číselného kódu). EBA v tomto případě uvedla, že při použití třímístného číselného kódu existuje pouze 1000 možných kombinací a existuje tak vyšší riziko jeho odhalení.[113] Z této odpovědi lze usuzovat, že poskytovatelé by měli stanovit vyšší nároky na délku a složitost prvku znalosti, než tomu bylo v rámci položeného dotazu, jinak by se mohli dopustit nedodržení povinnosti nastavit dostatečná bezpečnostní opatření.

Klíčovou otázkou ve vztahu k prvku znalosti je však vyřešení situace, kdy je údaj s jinými subjekty sdílen přímo uživatelem. Může v takovém případě být tento údaj použit v rámci SCA? Na první pohled se může zdát jako zřejmé, že takový údaj nenaplní požadavek zákona a není možné jej pro SCA použít, protože předáním údaje třetí osobě je automaticky nemožné splnit podmínku, že údaj je znám pouze uživateli (a z povahy věci poskytovateli platební služby). Domnívám se však, že takto zjednodušený závěr by poskytovatele platebních služeb stavěl vždy do situace, kdy by za jakýchkoliv okolností automaticky nesl odpovědnost za neautorizovanou platební transakci, což mi vzhledem k povaze dané úpravy nepřijde jako přiměřené vůči poskytovatelům a mám současně pochybnosti o tom, že by takový byl ve skutečnosti záměr zákonodárce (důvodová zpráva k ZPS k danému mlčí). Kloním se v tomto případě k názoru autorů komentáře k ZPS, kteří považují

[111] Bod 6 odůvodnění Nařízení RTS

[112] Z anglického „*questions and answers*“ (otázky a odpovědi)

[113] European Banking Authority. Single Rulebook Q&A. Length of authentication codes. *Eba.europa.eu* [online]. 2019 [cit. 07. 08. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4053

za správný výklad, aby se požadavek na to, jestli je údaj známý pouze uživateli, kladl na poskytovatele, který údaj uživateli poskytnul.[114]

V jednotlivých případech bychom tak měli zkoumat, jestli poskytovatel dostatečným způsobem splnil svoji povinnost zavést dostatečná bezpečnostní opatření, kterou mu stanoví Nařízení RTS, a jestli jeho jednáním, opomenutím nebo nedostatečným zabezpečením nedošlo ke sdílení/vyzrazení údaje třetí osobě. Níže analyzuji několik možných scénářů, které mohou nastat:

1) **údaj je sdílen uživatelem s třetí osobou a poskytovatel platební služby o této skutečnosti neví (a objektivně by tuto informaci nemohl získat ani při zavedení dostatečných bezpečnostních opatření**) – v takovém případě se domnívám, že poskytovatel se na daný údaj stále může v rámci SCA spolehnout a pokud by došlo k neautorizované platební transakci způsobené díky sdílení tohoto údaje, tak by se mohlo jednat (s ohledem na okolnosti) o hrubou nedbalost uživatele, který by svým jednáním porušil svojí povinnost na ochranu jeho osobních bezpečnostních prvků[115] a za neautorizovanou transakci by v takovém případě byl odpovědný v plném rozsahu;[116]

2) **údaj je sdílen uživatelem s třetí osobou a poskytovatel platební služby se tuto skutečnost dozví nebo má důvodné podezření, že se tak stalo** – poskytovatel se nesmí pouze spoléhat, že plátce automaticky splní svoji povinnost chránit své osobní bezpečnostní prvky, ale má povinnost zavést mechanismy sledování transakcí, které mu pomohou odhalit podvodné nebo neautorizované platební transakce.[117] V tomto případě by tento údaj poskytovatel neměl akceptovat pro účel použití SCA. Pokud by se tak stalo, porušil by svoji povinnost požadovat SCA a nesl by plnou odpovědnost za neautorizovanou platební transakci;[118]

[114] BERAN, Jiří, Daniela DOLEŽALOVÁ, Dalibor STRNADEL a Alice ŠTĚPÁNOVÁ. *Zákon o platebním styku. Komentář*. 1. vydání. Praha: C. H. Beck, 2011, s. 777. ISBN 978-80-7400-369-1.

[115] § 165 ZPS

[116] § 182 odst. 1 písm. b) ZPS

[117] Článek 2 odst. 1 Nařízení RTS

[118] § 183 odst. 3. písm. c) ZPS

3) **údaj byl získán třetí osobou a uživatel (plátce) tuto skutečnost poskytovateli platebních služeb neoznámil** – za této situace by se mělo individuálně posuzovat, jestli uživatel i poskytovatel dostatečným způsobem splnili své povinnosti, které jim právní úprava stanovuje. Pokud by si ztráty, odcizení nebo zneužití byl uživatel vědom a neoznámil je, nesl by za neautorizovanou platební transakci odpovědnost v plném rozsahu za předpokladu, že by současně poskytovatel splnil své povinnosti (v takovém případě by se dle mého názoru poskytovatel na údaj jako prvek znalosti mohl při použití SCA spolehnout). Pokud by však poskytovatel nezajistil vhodné prostředky umožňující ohlášení ztráty, odcizení nebo zneužití nebo by porušil jinou svoji povinnost, nesl by odpovědnost poskytovatel;

4) **údaj byl získán třetí osobou a uživatel tuto skutečnost poskytovateli platebních služeb včas oznámil** – pokud uživatel řádně splnil své ostatní povinnosti, tak by byl odpovědný maximálně do částky odpovídající 50 eurům a od chvíle oznámení by poskytovatel neměl údaj jako prvek znalosti akceptovat při použití SCA;

5) **údaj je sdílen uživatelem s jiným poskytovatelem platební služby** – ZPS předpokládá situaci, kdy se jiný poskytovatel služby nepřímého dání platebního příkazu nebo služby informování o platebním účtu může spolehnout na postupy SCA poskytovatele, který vede uživateli platební účet. V takové situaci by mohl být poskytovatel předem obeznámen s tím, že k předání přihlašovacích údajů uživatele došlo. Kloním se však v tomto případě opět k názoru autorů komentáře k ZPS, že je zde zřejmý záměr zákonodárce sdílení údaje povolit, a jsem tak názoru, že poskytovatel by takový údaj předaný v tomto specifickém případě měl mít stále možnost akceptovat pro účel SCA.

Rozbor prvku znalosti lze uzavřít demonstrativním výčtem příkladů prvků znalosti, které EBA uvedla ve svém stanovisku k jednotlivým prvkům SCA.[119] Podotýkám, že toto

[119] European Banking Authority. Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2. *Eba.europa.eu* [online]. 2019 [cit. 07. 08. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf

stanovisko není pro poskytovatele platebních služeb právně závazné, ale má spíše doporučující a informativní povahu. EBA v tomto stanovisku zmiňuje, že prvkem znalosti mohou být:

- heslo;
- PIN;
- odpovědi na otázky založené na znalostech uživatele (angl. *knowledge based challenge questions*);
- heslové fráze (angl. *passphrase*);
- dráha pro přejetí prstem jako zabezpečovací prvek (angl. *memorized swiping path*);
- CVV kód k platební kartě, ovšem pouze za předpokladu, že není vytištěn na dané kartě a že byl s uživatelem sdílen separátním způsobem (jako např. PIN kód); a
- údaje k jednorázové virtuální platební kartě, kdy uživatel obdrží jednorázové číslo karty a CVV kódu.

Prvek znalosti podle názoru EBA naopak nenaplňují:

- e-mailová adresa,
- uživatelské jméno,
- údaje vytištěné na platební kartě, a
- jednorázově vygenerovaná hesla sloužící jako důkaz pro doložení prvku držení (a to z důvodu, že prvek znalosti by měl existovat již předtím, než je použit pro účely SCA).

3.3.2. Držení

Druhý prvek SCA je podle Směrnice PSD2 z kategorie držení (to, co drží pouze uživatel).[120] ZPS jej poté vymezuje jako věc, kterou má uživatel ve své moci.[121] Bližší popis ani jeden z předpisů neposkytuje. Pro účely ZPS bychom tak měli vycházet z definice věci v OZ, který věc v právním slova smyslu vymezuje jako vše, co je rozdílné od osoby a slouží potřebě lidí.[122] Definičními znaky věci jsou rozdílnost od osob (fyzických i právnických) a také její užitečnost a ovladatelnost. Vymezení věci v OZ je poměrně široké a za věc považuje hmotné předměty i nehmotné entity, včetně majetkových práv. S rozvojem lidského poznání a technických možností společnosti se mohou věcmi stát i entity, které dříve věcí nebyly (jako např. nově vynalezená technická zařízení), nebo je lidé doposud nebyli schopni ovládat či pro ně neměly užitek.[123] Z pohledu ZPS vnímám široký výklad věci v OZ jako spíše příznivý, protože dává prostor budoucím inovacím bez nutnosti novelizace tohoto ustanovení. Široký výklad by měl obstát i z pohledu Směrnice PSD2, protože i nehmotné věci může mít uživatel ve své moci.[124]

Nařízení RTS ve vztahu k prvku z kategorie držení stanoví pro poskytovatele platebních služeb opět povinnosti, které spočívají v přijetí opatření ke zmírnění rizika toho, že prvky držení jsou použity neoprávněnými stranami. Použití těchto prvků ze strany plátce je podmíněno zavedením opatření, která mají zabránit jejich replikaci.[125] Opět jako v případě prvku znalosti je dle Nařízení RTS nutné vyžadovat bezpečnostní charakteristiky i u prvku držení, jakými jsou specifikace algoritmu, délka klíče a informační entropie.[126] Byť je tento výčet poměrně obecný, tak se domnívám, že u tohoto prvku je regulátorem kladen důraz především na technickou úroveň zabezpečení zařízení (např. proti virům či malware), které je pro účel SCA používáno. Poskytovatelé by tak měli být schopni zjistit, jestli

[120] Článek 4 odst. 30 Směrnice PSD2

[121] § 223 odst. 3 písm. b) ZPS

[122] § 489 OZ

[123] PETROV, Jan, Michal VÝTISK, Vladimír BERAN a kol. Občanský zákoník. Komentář. 2. vydání. Praha: C. H. Beck, 2022, s. 540-541. ISBN: 978-80-7400-747-7.

[124] BERAN, Jiří, Daniela DOLEŽALOVÁ, Dalibor STRNADEL a Alice ŠTĚPÁNOVÁ. *Zákon o platebním styku. Komentář*. 1. vydání. Praha: C. H. Beck, 2011, s. 779. ISBN 978-80-7400-369-1.

[125] Článek 7 Nařízení RTS

[126] Bod 6 odůvodnění Nařízení RTS

je konkrétní zařízení dostatečně bezpečné pro SCA, přičemž by jeho použití pro účel SCA neměli umožnit v případě, kdy tomu tak nebude.

Termín „*mít ve své moci*“ by se měl vykládat tak, že by s věcí měl mít možnost nakládat pouze uživatel. Při analýze tohoto prvku tak vyvstává obdobná otázka jako u prvku znalosti, a to co se bude dít v případě, že s věcí bude nakládat osoba odlišná od uživatele? Hlavním rozdílem oproti prvku znalosti je skutečnost, že nakládáním s touto věcí jinou osobou automaticky nezaniká možnost tento prvek použít v rámci SCA a bude možné jej stále použít ve chvíli, kdy bude daná věc navrácena uživateli. Relevantní tak vždy bude, jestli s věcí uživatel nakládal ve chvíli použití SCA. Autoři komentáře z ZPS v tomto smyslu uvádí, že termín „*mít ve své moci*“ by se měl vykládat jako požadavek, jež se aplikuje na poskytovatele platební služby, který věc uživateli k ověření poskytnul.[127] V případě určení odpovědnosti za neautorizovanou transakci bude nezbytné v individuálních případech zkoumat, obdobně jako bylo uvedeno v předchozí kapitole, jestli každá ze stran dostatečným způsobem splnila povinnosti, které jsou jí právními předpisy uloženy, a podle toho aplikovat jednotlivá ustanovení v ZPS.

EBA se opakovaně vyjadřovala k tomu, co lze považovat za prvek držení. V obecných pokynech k bezpečnosti internetových plateb byl jako příklad uveden mobilní telefon, token či čipová karta.[128] Ještě před přijetím Nařízení RTS ve svém stanovisku z roku 2018 uvedla, že zařízení lze považovat za prvek držení, pokud existuje spolehlivý způsob ověření jeho držení uživatelem spočívající ve vygenerování nebo přijetí dynamického ověřování prvku na tomto zařízení.[129] Jako důkaz pro ověření prvku držení může sloužit

---

[127] BERAN, Jiří, Daniela DOLEŽALOVÁ, Dalibor STRNADEL a Alice ŠTĚPÁNOVÁ. *Zákon o platebním styku. Komentář*. 1. vydání. Praha: C. H. Beck, 2011, s. 780. ISBN 978-80-7400-369-1.

[128] European Banking Authority. Final guidelines on the security of the internet payments. *Eba.europa.eu* [online]. 2014 [cit. 07. 08. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/934179/f27bf266-580a-4ad0-aaec-59ce52286af0/EBA-GL-2014-12%20%28Guidelines%20on%20the%20security%20of%20internet%20payments%29_Rev1.pdf

[129] European Banking Authority. Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC. *Eba.europa.eu* [online]. 2018 [cit. 07. 08. 2022]. Dostupné z:

jednorázově vygenerované heslo prostřednictvím softwaru nebo hardwaru, jakým může být token, autorizační SMS zpráva nebo tzv. push notifikace.[130]

Ve vztahu k prvkům držení byla položena v rámci procesu Q&A řada otázek. V případě Q&A 4039 byl vznesen dotaz, jestli jednorázové heslo zaslané prostřednictvím autorizační SMS zprávy na mobilní telefon může naplnit prvek držení, což EBA potvrdila s upozorněním, že prvkem držení nebude samotná autorizační SMS zpráva, ale typicky SIM karta spojená s příslušným telefonním číslem.[131] V případě Q&A 4827 se EBA zabývala otázkou, jestli tokenizovaná řešení pro platby kartou mohou představovat prvek držení. EBA dospěla k závěru, že tokenizace údajů o platební kartě může prvek držení naplnit, pokud je plátcův poskytovatel platebních služeb (jako vydavatel) zapojen do procesu vydávání tokenu přímo nebo nepřímo (např. prostřednictvím smlouvy o outsourcingu s třetí stranou, tj. žadatelem o token). Podle EBA tokenizace (i) poskytuje důkaz, že uživatel platebních služeb má v držení digitalizovanou verzi platební karty (proces tokenizace může držitele karty a token vázat na důvěryhodné zařízení), a (ii) zmírňuje riziko, že token bude použit neoprávněnou osobou nebo dojde k jeho replikaci, čímž dochází k naplnění požadavků na zavedení bezpečnostních opatření.[132] V neposlední řadě se EBA v rámci Q&A 4984 taktéž

https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2137845/0f525dc7-0f97-4be7-9ad7-800723365b8e/Opinion%20on%20the%20implementation%20of%20the%20RTS%20on%20SCA%20and%20CSC%20%28EBA-2018-Op-04%29.pdf

[130] European Banking Authority. Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2. *Eba.europa.eu* [online]. 2019 [cit. 07. 08. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf

[131] European Banking Authority. Single Rulebook Q&A. Qualification of SMS OTP as an authentication factor. *Eba.europa.eu* [online]. 2018 [cit. 07. 08. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4039

[132] European Banking Authority. Single Rulebook Q&A. Tokenised card details as a SCA possession element. *Eba.europa.eu* [online]. 2019 [cit. 07. 08. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4827

opakovaně vyjádřila k použití tzv. push notifikace, která za splnění podmínek Nařízení RTS může sloužit způsob ověření přítomnosti prvku držení.[133]

EBA ve svém stanovisku k prvkům SCA dále uvádí, že prvkem držení mohou být i přístupy založené na mobilních aplikacích, webových prohlížečích nebo výměně (veřejných a soukromých) klíčů, pokud ovšem zahrnují proces vazby na zařízení, který zajišťuje jedinečné spojení mezi takovou aplikací, prohlížečem nebo klíčem uživatele a samotným zařízením. EBA jako příklad zmiňuje hardwarové kryptografické zabezpečení, registraci webového prohlížeče a mobilního zařízení nebo uložení klíče v zabezpečeném prvku zařízení.[134]

Důkaz o držení by mohl být zajištěn také prostřednictvím digitálního podpisu, který by byl vygenerován např. pomocí soukromého klíče. Držení karty nebo zařízení by mohlo být ověřeno také prostřednictvím naskenování QR kódu zobrazeného na této kartě (popřípadě dynamickým CVV kódem, který není zobrazen na kartě a je pravidelně obměňován) nebo naskenováním specifického QR kódu na tomto zařízení (který však musí být jedinečný pro dané zařízení).[135]

Pro přehlednost níže shrnuji demonstrativní výčet prvků držení, které dle stanoviska EBA splňují požadavky pro jejich použití v rámci SCA:

- zařízení, jehož držení je ověřeno prostřednictvím vygenerování nebo přijetí jednorázově vygenerovaného hesla (např. tokenem, autorizační SMS zprávou);
- zařízení, jehož držení je ověřeno digitálním podpisem, který byl vygenerován např. pomocí soukromého klíče;

[133] European Banking Authority. Single Rulebook Q&A. "Push based" authentication and SCA requirements. *Eba.europa.eu* [online]. 2019 [cit. 07. 08. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2019_4984

[134] European Banking Authority. Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2. *Eba.europa.eu* [online]. 2019 [cit. 07. 08. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf

[135] Tamtéž.

- karta nebo zařízení, jejichž držení je ověřeno naskenováním jejich unikátního QR kódu;
- aplikace, webový prohlížeč nebo klíč za předpokladu, že jsou jedinečným způsobem propojeny se zařízením (např. prostřednictvím čipu v zařízení nebo soukromého klíče); nebo
- platební karta ověřená čtečkou karet nebo platební karta, u níž je držba doložena dynamickým CVV kódem.

Závěrem EBA dodává, že samostatná aplikace nainstalovaná na zařízení nebo platební karta, u níž je držení ověřeno pouze opsáním údajů vytištěných na kartě, bezpečnostní požadavky stanovené pro prvek držení nesplňují.

3.3.3. Inherence

Třetím a zároveň posledním prvkem, který lze použít k SCA, je podle Směrnice PSD2 „*inherence (to, čím uživatel je)*". S pojmem inherence pracuje i Nařízení RTS, avšak ani jeden z předpisů bohužel neobsahuje jeho bližší definici. Vodítkem může být výklad EBA, podle níž se inherence, která zahrnuje biologickou a behaviorální biometrii, týká fyzických vlastností částí těla, fyziologických charakteristik a behaviorálních procesů vytvářených tělem a jakékoli jejich kombinace.[136] Český zákonodárce třetí prvek pojmenoval jako „*biometrické údaje uživatele*", nicméně jeho definici bychom v ZPS taktéž hledali neúspěšně. Důvodová zpráva k ZPS v tomto směru odkazuje na definici biometrického údaje obsaženou v rámci Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (dále jen „**Nařízení GDPR**").[137] Nařízení GDPR v článku 4 odst. 14 definuje biometrické údaje jako:

[136] European Banking Authority. Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2. *Eba.europa.eu* [online]. 2019 [cit. 11. 08. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf

[137] Důvodová zpráva k zákonu č. 370/2017 Sb., o platebním styku. Zvláštní část k § 223. 2017. Dostupné z: www.beck-online.cz

„*osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje*“.

V obecné rovině biometrickým údajem rozumíme měřitelný fyzický či fyziologický a po dobu života člověka prakticky neměnný znak, který umožňuje zjištění nebo ověření identity dané osoby. Biometrika tedy slouží k jednoznačné identifikaci osob na základě jedinečných a měřitelných znaků člověka.[138] Tyto znaky lze označit také jako biometrické prvky, které jsou do určité míry univerzální (existují u všech osob), jedinečné (odlišují osoby od sebe) a stálé (v průběhu času si jej osoby uchovávají).[139]

Zpracování biometrických prvků probíhá v současnosti tak, že jsou snímány za použití specializovaných senzorů, které následně převedou tyto „hrubé“ údaje do digitální podoby a umožní tak jejich další zpracování. Software, který tyto údaje zpracovává, vybere z naměřených biometrických prvků rysy, které jsou specifické pro daného jednotlivce a vytvoří z nich tzv. „šablonu“, která je redukovaným biometrickým obrazem zkoumaného jednotlivce.[140] Jako příklady biometrických údajů lze uvést např. otisky prstů, dlaně či chodidla, obraz oční sítnice nebo duhovky, záznam dynamického projevu chůze, ale i rozbor tváře či hlasového projevu.[141]

Biometriku a biometrické údaje lze v teorii rozlišovat dle různých kritérií. Podle použití konkrétního biometrického prvku ji můžeme dělit na daktyloskopickou biometrii

---

[138] KUČEROVÁ, Alena; Ludmila NOVÁKOVÁ, Vanda FOLDOVÁ, František NONNEMANN a Daniel POSPÍŠIL. *Zákon o ochraně osobních údajů*. *Komentář.* 1. vydání. Praha: C. H. Beck, 2012, s. 60-61. ISBN 978-80-7179-226-0.

[139] Ministerstvo vnitra České republiky. Cestovní doklady s biometrickými prvky (CDBP). *Mvcr.cz* [online]. 2022 [cit. 12. 08. 2022]. Dostupné z: https://www.mvcr.cz/clanek/cestovni-doklady-s-biometrickymi-prvky-cdbp.aspx?q=Y2hudW09MQ%3D%3D

[140] Tamtéž, a MATEJKA, Ján, Alžběta Krausová a Güttler Vojen. Biometrické údaje a jejich právní režim. *Revue pro právo a technologie* [online]. 2018, č. 17, s. 91. [cit. 12. 08. 2022]. Dostupné z: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=nrptembrhbpxe4dul4ytox3tl44tc&groupIndex=5&rowIndex=0#

[141] KUČEROVÁ, Alena; Ludmila NOVÁKOVÁ, Vanda FOLDOVÁ, František NONNEMANN a Daniel POSPÍŠIL. *Zákon o ochraně osobních údajů*. *Komentář.* 1. vydání. Praha: C. H. Beck, 2012, s. 61. ISBN 978-80-7179-226-0.

(zkoumající papilární linie vytvořené na vnitřní straně článků prstů, na dlaních, prstech nohou nebo chodidlech)[142], biometrii obličeje, biometrii hlasu, biometrii sítnice nebo biometrii krevního řečiště.[143] Jako další příklad lze uvést dělení na základě podkladových dat:[144]

a) **stabilní data** – zde se jedná o postupy založené na fyzických a fyziologických aspektech, které měří fyziologické vlastnosti osoby a zahrnují:
   i. verifikaci otisku prstu,
   ii. rozpoznávání duhovky,
   iii. analýzu sítnice,
   iv. rozpoznávání obličeje,
   v. analýzu markantů (charakteristických znaků) hlavy,
   vi. rozpoznávání tvaru ucha,
   vii. detekci pachu těla,
   viii. rozpoznávání hlasu, a
   ix. analýzu vzorku DNA;

b) **dynamická data nebo charakteristiky chování** – zde se jedná o postupy založené na rysech chování, které měří chování osob a zahrnují:
   i. verifikaci vlastnoručního podpisu, a
   ii. analýzu stisku tlačítek.

Kategorii b) výše lze rovněž označit pojmem behaviorální biometrika. Jde o oblast, která v posledních letech prošla významným technologickým vývojem, a jejím předmětem je kvantifikace chování jednotlivců s cílem vytvořit individuální profily za účelem identifikace těchto jednotlivců. V rámci analýzy chování lze zkoumat mimo jiné např. psaný

[142] Policie České republiky. Kriminalistická daktyloskopie. *Policie.cz* [online]. 2022 [cit. 12. 08. 2022]. Dostupné z: https://www.policie.cz/clanek/kriminalisticka-daktyloskopie-266095.aspx

[143] BERAN, Jiří, Daniela DOLEŽALOVÁ, Dalibor STRNADEL a Alice ŠTĚPÁNOVÁ. *Zákon o platebním styku. Komentář*. 1. vydání. Praha: C. H. Beck, 2011, s. 781. ISBN 978-80-7400-369-1.

[144] Ministerstvo vnitra České republiky. Cestovní doklady s biometrickými prvky (CDBP). *Mvcr.cz* [online]. 2022 [cit. 12. 08. 2022]. Dostupné z: https://www.mvcr.cz/clanek/cestovni-doklady-s-biometrickymi-prvky-cdbp.aspx?q=Y2hudW09MQ%3D%3D

text, specifické vzorce pro používání počítače/mobilního telefonu nebo kognitivní schopnosti osoby, které vykazuje při plnění specifických úloh.[145]

Biometrické údaje jsou standardně využívány ke dvěma účelům – k identifikaci a autentizaci. V rámci identifikace dochází k určení totožnosti neznámé osoby, a to např. v kriminalistice na základě přiřazení vzorků biometrických prvků konkrétní osobě. Naopak při autentizaci dochází k prokázání totožnosti konkrétní osoby, která své biometrické údaje zpravidla již poskytla předem (např. registrací do zařízení/databáze) a nyní dochází pouze k porovnání nového vzorku biometrických údajů s vzorkem již dříve poskytnutým.[146] Při používání biometrických údajů je však na místě podotknout, že se jedná o zvláštní kategorii osobních údajů ve smyslu článek 9 Nařízení GDPR, která podléhá speciální režimu zpracování a ochrany a nad rámec regulatorních povinností ve vztahu k SCA musí poskytovatelé platební služby nastavit interní procesy tak, aby nedocházelo k porušení předpisů vztahujícím se ke zpracování a ochraně osobních údajů.

Nařízení RTS klade speciální požadavky na poskytovatele platebních služeb ve vztahu k zařízením a softwaru používaným pro prvky z kategorie inherence. Povinností poskytovatelů je přijmout opatření na zmírnění rizika spočívajícím v odhalení údajů z kategorie inherence neoprávněnými entitami. Jako příklad takových bezpečnostních opatření uvádí Nařízení RTS u zařízení a softwaru, které jsou používány pro zpracování prvků z kategorie inherence, specifikaci algoritmu, biometrické čidlo a ochranné prvky vzoru.[147] Nařízení RTS dále stanoví jako nezbytné minimum povinnost zajistit, aby u zařízení a softwaru pro přístup existovala velmi nízká pravděpodobnost ověření neoprávněné strany jako plátce. Z Nařízení RTS bohužel nevyplývá, jaká míra pravděpodobnosti znamená míru velmi nízkou. Použití prvků inherence je v neposlední řadě podmíněno opatřeními, která mají zajistit, aby zařízení a software, které používá plátce k ověření prvku inherence, zaručovaly

[145] MATEJKA, Ján, Alžběta Krausová a Güttler Vojen. Biometrické údaje a jejich právní režim. *Revue pro právo a technologie* [online]. 2018, č. 17, s. 91. [cit. 12. 08. 2022]. Dostupné z: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=nrptembrhbpxe4dul4ytox3tl44tc&groupIndex=5&rowIndex=0#

[146] TOMÍŠEK, Jan. Právní jednání biometrickými prostředky v elektronickém bankovnictví. *Právní rozhledy* [online]. 2018, č. 5, s. 160. [cit. 12. 08. 2022]. Dostupné z: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=nrptembrhbpxa4s7gvpxgxzrgyya&groupIndex=2&rowIndex=0

[147] Bod 6 odůvodnění Nařízení RTS.

odolnost vůči neautorizovanému použití prvků prostřednictvím přístupu k zařízením a softwaru.[148]

Závěrem uvádím příklady jednotlivých řešení, které dle stanoviska EBA za splnění technických požadavků Nařízení RTS mohou naplňovat prvek z kategorie inherence. Jedná se o následující:[149]

- sken otisku prstu,
- rozpoznávání hlasu,
- rozpoznávání žil,
- geometrie rukou a obličeje,
- rozpoznávání duhovky a sítnice,
- dynamika stisku kláves,
- analýza srdeční frekvence nebo jiného pohybového vzorce těla,
- úhel, pod kterým drží uživatel zařízení.

V rámci Q&A 4237[150] dále EBA zmínila, že srovnání podpisu uživatele obchodníkem a jeho srovnání s podpisem např. na jeho platební kartě nemůže být považováno za biometrický údaj, ani za kterýkoliv z předchozích dvou prvků. Oproti tomu v rámci Q&A 4238[151] EBA uvedla, že podpis uživatele na digitální obrazovce může být považován za prvek behaviorální biometrie, a tedy vhodný jako prvek z kategorie inherence za předpokladu,

[148] Článek 8 Nařízení RTS

[149] European Banking Authority. Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2. *Eba.europa.eu* [online]. 2019 [cit. 12. 08. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf

[150] European Banking Authority. Single Rulebook Q&A. Signature on a paper slip from a payment terminal, as a factor in a two-factor SCA. *Eba.europa.eu* [online]. 2018 [cit. 29. 10. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4237

[151] European Banking Authority. Single Rulebook Q&A. Signature performed on the screen of a digital device as a factor in a two-factor SCA. *Eba.europa.eu* [online]. 2018 [cit. 29. 10. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4238

že by zařízení i rozpoznávací software byly schopny zajistit velmi malé riziko zneužití neoprávněnou stranou.

Prvky z kategorie inherence (biometrických údajů) jsou a bezpochyby budou vzhledem ke svojí povaze předmětem budoucích inovací a můžeme očekávat, že společnosti přijdou s různými technologickými řešeními, které bude možné díky velmi obecné definici prvku inherence (biometrických údajů) pro účel SCA používat. Vždy bude potřeba analyzovat jaké zařízení nebo software bude pro účel SCA používán, a především jakým způsobem budou poskytovatelé platebních služeb schopni zajistit jejich zabezpečení. Vzhledem k citlivosti biometrických údajů nesmí poskytovatelé platebních služeb opomenout požadavky Nařízení GDPR a musí se ujistit o vhodnosti použití biometrických údajů. Užší vymezení třetího prvku v rámci ZPS oproti Směrnici PSD2 by mohlo hypoteticky v budoucnu znamenat, že některá inovativní řešení nemusí naplnit zamýšlenou definici biometrických údajů, na kterou odkazuje důvodová zpráva k ZPS, a nebude tudíž zcela zřejmé, jestli je bude možné na území České republiky aplikovat. Inovativnost poskytovatelů platebních služeb společně s technologickým pokrokem a postojem regulátorů nám v budoucnu ukáží, do jaké míry se tato na první pohled nepatrná odlišnost v pojmosloví projeví v praxi.

3.4. Nezávislost jednotlivých prvků

ZPS stanoví, že při použití SCA musí být jednotlivé prvky uvedené v předchozích podkapitolách vzájemně nezávislé a prolomení jednoho nesmí ovlivnit spolehlivost prvků ostatních.[152] Nařízení RTS tuto povinnost dále specifikuje a zavádí povinnost poskytovatelů platebních služeb zajistit, aby nezávislost a obrana proti prolomení byla podmíněna opatřeními, která z hlediska technologie, algoritmů a parametrů zajistí tuto nezávislost.

Použití minimálně dvou prvků ze třech možných kategorií zároveň znamená, že by se mělo jednat o prvky z různých kategorií, jak uvedla EBA v Q&A 5619[153]. Takový závěr by se měl uplatnit i v případě, kdy některý z těchto prvků nedosahuje takové úrovně

[152] § 223 odst. 4 ZPS

[153] European Banking Authority. Single Rulebook Q&A. Independence of the elements for SCA. *Eba.europa.eu* [online]. 2020 [cit. 29. 10. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5619

ochrany, jako by mohly dosahovat dva prvky ze stejné kategorie. Tomuto požadavku nicméně nebrání, aby k použití více prvků bylo použito jedno víceúčelové zařízení (v dnešní době je takovým zpravidla chytrý mobilní telefon). Jelikož použití jednoho zařízení může snižovat bezpečnost samotného ověřovacího procesu, došlo (poměrně očekávaně) k zavedení požadavků na dodatečná bezpečnostní opatření, která je při každém použití víceúčelového zařízení k SCA splnit. Takovými opatřeními jsou (taxativně):[154]

a) „*použití odděleného bezpečného prostředí pro provedení prostřednictvím softwaru nainstalováno ve víceúčelovém zařízení;*

b) *mechanismy k zajištění toho, aby software nebo zařízení nebyly pozměněny plátcem nebo třetí stranou; a*

c) *došlo-li ke změnám, mechanismy k zmírnění jejich důsledků.*“

V této části jsem detailně popsal jednotlivé prvky SCA, uvedl jejich konkrétní příklady a povinnosti, které poskytovatelům platebních služeb při jejich použití ukládá regulace. Právní úprava výčtu jednotlivých autentizačních prvků a povinností pro poskytovatele platebních služeb je z důvodu snahy o technologickou neutralitu velmi obecná, což vnímám převážně pozitivně, protože dává velký prostor k inovacím a nenutí subjekty omezit se na konkrétní technologické standardy, které za deset let mohou být zastaralé. Na přístup zákonodárce lze nahlížet i opačným prizmatem, kdy v řadě případů není zcela jasné, jestli konkrétní technologické řešení dostatečně reflektuje požadavky stanovené právními předpisy a jestli je možné jej použít v rámci SCA. Z tohoto důvodu EBA čelí relativně často dotazům zaměřeným na různé aspekty SCA a jeho použití. Jelikož odpovědi EBA nejsou právě závazné, ale mají pouze doporučující charakter a napomáhají subjektům s výkladem právních předpisů, tak se může v blízké budoucnosti ukázat jako vhodné některé části těchto předpisů legislativně zpřesnit. V případě jednotlivých autentizačních prvků by například mohlo pomoci stanovení bližších charakteristik či vlastností bezpečnostních opatření, která se od poskytovatelů ve vztahu k SCA očekávají.

[154] Článek 9 odst. 3 Nařízení RTS

4. Použití silného ověření uživatele

V této části práce navazuji na úvod do SCA a rozbor jeho jednotlivých prvků, kterým jsem se věnoval v předchozí části, a zaměřím se na problematiku povinnosti jeho použití. Uvedu jednotlivé okruhy situací, kdy je zákonem daná povinnost uplatnit SCA a současně srovnám úpravu českého a evropského zákonodárce, a následně se budu věnovat jednotlivým výjimkám z povinnosti uplatnit SCA, které byly stanoveny Nařízením RTS.

4.1. Případy použití SCA

Jednotlivé případy povinnosti provádět SCA jsou upraveny v článku 97 Směrnice PSD2, který ve svém prvním odstavci stanoví:

„*Členské státy zajistí, aby poskytovatelé platebních služeb používali silné ověření klienta, pokud plátce:*

a) využívá on-line přístupu ke svému platebnímu účtu;

b) iniciuje elektronickou platební transakci;

c) prostřednictvím prostředků komunikace na dálku provede jakýkoli úkon, který by mohl vést k riziku platebního podvodu nebo jiných zneužití.“

Tento okruh situací, při nichž musí být vyžadováno SCA, byl transponován českým zákonodárcem do ZPS, který v § 223 odst. 1 stanoví:

„Osoba oprávněná poskytovat platební služby použije silné ověření uživatele, jestliže plátce:

a) přistupuje ke svému platebnímu účtu prostřednictvím internetu,

b) dává platební příkaz k elektronické platební transakci,

c) provádí jiný úkon, který je spojen s rizikem podvodného jednání v oblasti platebního styku, zneužitím platebního prostředku nebo informací o platebním účtu, nebo

d) požaduje informace o platebním účtu prostřednictvím poskytovatele služby informování o platebním účtu.“

Textace českého zákonodárce se od původního textu Směrnice PSD2 mírně liší, proto se výše uvedenému výčtu v ZPS budu věnovat podrobněji. Předně je nezbytné uvést, že tento výčet je taxativní a vztahuje se na všechny osoby oprávněné poskytovat platební služby. Oproti Směrnici PSD2 tak došlo k zpřesnění a omezení aplikace tohoto ustanovení na osoby, které mají oprávnění poskytovat platební služby, nikoliv na osoby, které poskytují platební služby v rozporu se zákonem (k poskytovatelům platebních služeb blíže viz kapitola 2.3.3 (*Poskytovatelé platebních služeb*) výše).

Výčet jednotlivých situací je dále omezen toliko na plátce (bez ohledu na to, jestli se jedná o fyzickou nebo právnickou osobu)[155]. Povinnost aplikovat SCA se tak nebude aplikovat na transakce, ke kterým dává platební příkaz výlučně příjemce peněžních prostředků bez jakékoli účasti nebo interakce plátce. Tato situace je relevantní především při zadávání platebního příkazu k elektronickým platebním transakcím, jak je uvedeno pod písm. b) výše. Příkladem lze uvést inkasní platby, při kterých dochází k převodu peněžních prostředků z platebního účtu plátce, ke kterým nicméně dává platební příkaz příjemce na základě předchozího souhlasu plátce. Zadávání platebních příkazů k jednotlivým inkasním platbám příjemcem tak v praxi nebude podléhat povinnosti SCA. EBA se v rámci Q&A 4031[156] zabývala také otázkou, jestli platí povinnost uplatit SCA v případech, kdy příjemce je osobou zadávající pokyn k platebním transakcím na základě (i) předchozího mandátu k zadávání takových transakcí plátcem, nebo (ii) již existující dohody iniciovat takové transakce v rámci poskytovaných služeb mezi příjemcem a plátcem. EBA v tomto případě uvedla, že pokud byl příjemci udělen mandát, který jej opravňuje k iniciaci transakcí prostřednictvím určitého platebního prostředku vydanému pro tento účel a pokud byl tento mandát založen na dohodě obou stran, mohou být takové transakce považovány na iniciované příjemcem (a tedy vyňaty z povinnosti uplatnit SCA), za předpokladu, že iniciaci takové transakce nepředchází konkrétní úkon plátce. Povinnost aplikovat SCA by se nicméně aplikovala na zřízení takového mandátu, pokud by probíhalo na dálku. Důvodem pro tuto aplikaci je zvýšené riziko podvodného jednání při takovém úkonu.

[155] Bod 7 odůvodnění Nařízení RTS

[156] European Banking Authority. Single Rulebook Q&A. Applicability of SCA to 'card payments initiated by the payee only'. *Eba.europa.eu* [online]. 2018 [cit. 29. 10. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4031

Zbývající kategorií jsou situace, kdy příkaz k platební transakci dal plátce prostřednictvím příjemce. V některých případech ZPS specificky rozlišuje případy, kdy byl platební příkaz zadán plátcem prostřednictvím příjemce.[157] Jedná se o případy, kdy platební příkaz dává plátce, avšak nikoli přímo svému poskytovateli, ale za současné účasti příjemce, kdy tento předá daný platební příkaz svému poskytovateli a jeho prostřednictvím poskytovateli plátce. Tento způsob zadávání platebních příkazů je typický u karetních plateb. Výkladem lze dle mého názoru dospět k závěru, že záměrem zákonodárce nebylo specificky vyjmout tyto situace z povinnosti SCA, které se tak bude aplikovat i na situace, kdy platební příkaz zadal plátce prostřednictvím příjemce. Tento závěr při výkladu uplatnila mimo jiné i EBA ve svém stanovisku k finálnímu znění Nařízení RTS před jeho přijetím.[158]

4.1.1. Přístup k platebnímu účtu

První případ povinnosti uplatnit SCA nastane při přístupu plátce k platebnímu účtu prostřednictvím internetu. Definice přístupu k platebnímu účtu není v ZPS ani v PSD2 uvedena, lze jej však chápat jako zpřístupnění poskytovatelem vytvořeného uživatelského prostředí, v němž jsou uživateli k dispozici informace a služby spojené s platebním účtem jako např. výše zůstatku, historie provedených plateb, možnost zadávat platební příkazy nebo informace o platebních prostředcích vydaných k danému účtu a jejich finančních limitů.

Jako poměrně nelogický se jeví požadavek uplatnit SCA při přístupu k platebnímu účtu pouze na plátce, kdy ve chvíli přístupu nemůže být poskytovateli známo, zdali se v dané situace uživatel bude chovat jako plátce či nikoliv. V praxi by tak SCA měli poskytovatelé vyžadovat ve všech případech přístupu k platebnímu účtu uživatelem (s výjimkou situací,

[157] Příkladem lze uvést odvolání platebního příkazu dle § 160 odst. 3, lhůta pro předání platebního příkazu dle § 173 nebo vrácení částky platební transakce § 176 odst. 1 písm. a) ZPS.

[158] European Banking Authority. Final Report. Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2). *Eba.europa.eu* [online]. 2017 [cit. 25. 10. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1761863/314bd4d5-ccad-47f8-bb11-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%28EBA-RTS-2017-02%29.pdf

kdy poskytovatel řádně uplatní některou z výjimek) bez ohledu na to, jestli následně dojde k zadání platebního příkazu k provedení platební transakce či nikoliv.

4.1.2. Elektronické platební transakce

Druhý případ uplatnění SCA nastane při dání platebního příkazu k elektronické platební transakci. Platebním příkazem rozumíme „*pokyn poskytovateli, jímž plátce nebo příjemce žádá o provedení platební transakce*“[159]. Ve vztahu k pokynům zadaným příjemcem a plátcem prostřednictvím příjemce a související povinnosti aplikovat SCA jsem se již vyjádřil výše.

Termín elektronická platební transakce bohužel v ZPS, PSD2 ani v Nařízení RTS definován není. V rámci Q&A 4788[160] EBA uvedla, že transakce, ke kterým je dán platební příkaz prostřednictvím poštovní příkazu nebo příkazu přes telefon, nelze považovat za elektronické platební transakce a nespadají tak do působnosti SCA, a naopak veškeré karetní platební transakce se za elektronické platební transakce považují.

Vzhledem k použití adjektiva elektronický se pro jeho výklad jeví jako relevantní především dva momenty – zadání platebního příkazu a samotné zúčtování platební transakce. Pokud byl záměrem zákonodárce myšlen pouze způsob zadání platebního příkazu k platební transakci elektronickým prostředky (jako např. prostřednictvím internetového či mobilního bankovnictví nebo platby platebními kartami), pak se nejeví vhodné terminologické použití platební transakce, které v sobě (jde-li o převod platebních prostředků) automaticky zahrnuje i samotné zúčtování platební transakce. Větší smysl by v takovém případě dávalo například znění „při dání elektronického platebního příkazu“. Na druhou stranu požadavek na zahrnutí elektronického zúčtování platební transakce se nejeví jako logický z pohledu SCA, u nějž jde především o ověření totožnosti uživatele v daný moment.

Nelze pominout také skutečnost, že mimo hotovostních plateb, obsahující prakticky všechny platební transakce alespoň nějaký elektronický prvek. Jelikož si však lze obtížně představit platební transakci, ke které je zadán platební příkaz elektronickými prostředky

[159] § 2 odst. 3 písm. c) ZPS

[160] European Banking Authority. Single Rulebook Q&A. Treatment of electronic bookings similar to Mail Order and Telephone Orders (MO-TO) transactions. *Eba.europa.eu* [online]. 2019 [cit. 29. 10. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4788

a její zúčtování by elektronicky neproběhlo, domnívám se, že termín elektronická platební transakce by tak měl být vykládán jako případ zahrnující oba výše uvedené momenty, elektronický způsob zadání příkazu i jeho elektronické zúčtování, byť požadavek na samotné zúčtování není ve vztahu k SCA relevantní. V každém případě považuji za velmi problematické nemít jasně stanovenou definici pojmu, který je fundamentálně významný z pohledu výkladu povinnosti vyžadovat či nevyžadovat SCA.

4.1.3. Riziko podvodných jednání

Jako třetí případ je uvedena situace aplikující se při úkonech plátce spojených s rizikem podvodného jednání v oblasti platebního styku. Oproti Směrnici PSD2 se český zákonodárce rozhodl udělat dvě změny – vypustit část „*prostřednictvím prostředků komunikace na dálku*“ a přeformulovat a blíže specifikovat termín „*platebnímu podvodu nebo jiných zneužití*“. Důvodová zpráva se k vypuštění první části bohužel nevyjadřuje a není tak zřejmé co vedlo zákonodárce k této změně, v každém případě tak došlo k rozšíření povinnosti uplatnit SCA i na jiné situace, kdy nedochází k použití prostředků komunikace na dálku.

Zpřesnění pojmu „*jiných zneužití*“ českým zákonodárcem by nemělo být problematické, jelikož přeformulování platebního podvodu na podvod v oblasti platebního styku považuji za dostatečné obecné a široké na to, aby nevytvořilo neúmyslnou mezeru v právu. Vzhledem k povaze tohoto případu povinnost uplatnit SCA se domnívám, že v praxi bude toto ustanovení vykládáno spíše extenzivně. Takovým potenciálně rizikovým jednáním by mohlo být např. vložení platební karty do digitální peněženky jako je Peněženka Google, nastavení možnosti přečerpání sjednaného finančního limitu k platebnímu prostředku nebo změna nastavení inkasních plateb či trvalých platebních příkazů. Textace třetího ustanovení byla na základě zákona č. 129/2022 Sb. novelizována a došlo k záměně termínu „podvod“ za „podvodné jednání“ a jako rizikové tak bude možné vnímat větší množství úkonů uživatele, na které se tak bude vztahovat povinnost uplatnit SCA.

4.1.4. Informování o platebním účtu

V posledním případě český zákonodárce oddělil požadování informací o platebním účtu prostřednictvím poskytovatele služby informování o platebním účtu od přístupu k platebnímu účtu a zavedl jej jako specifickou situaci pro aplikaci SCA. Ve Směrnici PSD2

se tento požadavek vyskytuje ve druhé větě článku 97 odst. 4. Je tak postaveno na jisto, že se SCA vyžaduje i v případě, kdy přístup k platebnímu účtu plátce je vyžádán prostřednictvím poskytovatele odlišného od toho, který vede platební účet.

4.2. Dynamické propojení, ověřovací kód

ZPS dále stanovuje pro vybrané typy platebních transakcí povinnost provést SCA, které zahrnuje jednorázové prvky propojující platební transakci s přesnou částkou a určitým příjemcem (tzv. dynamické propojení). Povinnost dynamického propojení je stanovena pro případy, kdy dá uživatel platební příkaz prostřednictvím internetu nebo prostřednictvím elektronického zařízení, které lze použít k dálkové komunikaci, nebo dá-li platební příkaz nepřímo.[161] Směrnice PSD2 povinnost dynamického propojení stanovuje pro platební transakci na dálku, která je definována jako „*platební transakce iniciovaná po internetu nebo prostřednictvím zařízení, které lze použít k dálkové komunikaci*“[162]. Dalším vodítkem pro výklad pojmu platební transakce na dálku může být odůvodnění ke Směrnici PSD2, ve kterém je uvedeno, že požadavek dynamických kódů by měl být zahrnut u platebních služeb nabízených prostřednictvím internetu nebo přes jiné kanály komunikace, jejichž fungování nezávisí na tom, kde se zařízení použité k iniciování platební transakce a použitý platební prostředek fyzicky nacházejí.[163] Za platební transakci na dálku tak lze považovat takovou transakci, k níž může uživatel dát platební příkaz bez ohledu na fyzické umístění jeho platebního prostředku (např. platební karta) a zařízení poskytovatele k jeho přijetí (např. platební brána). Tento závěr lze uplatnit taktéž na popis okruhu situací, při nichž je povinnost dynamického propojení stanovena v ZPS.

Povinnost dynamického propojení se dle Směrnice PSD2 obdobně uplatní na platby iniciované prostřednictvím poskytovatele služeb iniciování platby, kterou se rozumí „*služba k iniciování platebního příkazu na žádost uživatele platebních služeb ve vztahu k platebnímu účtu vedenému u jiného poskytovatele platebních služeb*“[164]. ZPS použití dynamického propojení při SCA ve vztahu ke všem platebním příkazům daným nepřímo explicitně nenavazuje na způsob jeho zadání, z čehož lze dovozovat, že český zákonodárce nepřímé

[161] § 223 odst. 2 ZPS

[162] Článek 6 odst. 4 Směrnice PSD2

[163] Bod 95 odůvodnění Směrnice PSD2

[164] Články 6 odst. 15 a 97 odst. 4, věta první Směrnice PSD2

dání platebního příkazu vykládá jako elektronické, což lze vyčíst ze samotné definice služby nepřímého dání platebního příkazu, která obsahuje dodatek „*je-li platební příkaz dán prostřednictvím internetu*“[165].

Požadavek dynamického propojení je dále zpřesněn Nařízením RTS. V něm je uvedeno, že dynamické propojení je umožněno vytvářením ověřovacích kódů, které podléhá souboru přísných bezpečnostních požadavků.[166] Pro lepší pochopení dodatečných požadavků kladených na Dynamické propojení je třeba nejprve vysvětlit pojem ověřovací kód, který se v nich opakovaně objevuje. Ověřovací kód je kód, který je vytvořen při uplatnění SCA poskytovatelem platební služby. Má jednorázový charakter a poskytovatel jej může akceptovat výlučně v situaci, kdy jej plátce použije pro jeden z úkonů, pro které je stanovena povinnost SCA.[167] Lze tak dovodit, že povinnost ověřovací kódu byla stanovena pro zvýšení bezpečnosti platebních služeb. Na ověřovací kód jsou tak kladeny poměrně přísné požadavky, které spočívají v povinnosti poskytovatelů platebních služeb přijmout ve vztahu k ověřovacímu kódu kumulativně následující bezpečnostní opatření:

a) ze sděleného ověřovacího kódu nelze odvodit informace o žádném z prvků SCA;

b) na základě znalosti dřívějšího ověřovacího kódu nelze vytvořit ověřovací kód nový; a

c) ověřovací kód nelze zfalšovat.[168]

Vedle výše uvedených opatření musí poskytovatelé přijmout některá další. Příkladem lze zmínit (i) povinnost znemožnění určit, který z prvků SCA nebyl správný, pokud nedojde k vytvoření ověřovacího kódu při SCA, (ii) počet neúspěšných, po sobě následujících pokusů o ověření, po jehož překročení dojde k dočasnému či trvalému zablokování úkonů, na něž je aplikováno SCA, nepřekročí pro dané časové období pět; nebo (iii) maximální doba nečinnosti po ověření za účelem přístupu k platebnímu účtu prostřednictvím internetu

[165] § 2 odst. 1 písm. k) ZPS; a
BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. *Zákon o platebním styku. Komentář*. 1. vydání. Praha: Wolters Kluwer ČR, 2020. s. 775-776. ISBN 978-80-7598-788-4

[166] Bod 4 odůvodnění Nařízení RTS

[167] Článek 4 odst. 1 Nařízení RTS

[168] Článek 4 odst. 2 Nařízení RTS.

nepřesáhne pět minut.[169] V důsledku výše uvedeného dále Nařízení RTS stanoví demonstrativní výčet příkladů řešení, na nichž má být vytvoření ověřovacího kódu založeno, jako jsou jednorázová hesla, digitální podpis, kryptograficky podložená potvrzení platnosti pomocí klíčů či materiálů uložených v ověřovacích prvcích.[170]

K ověřovacímu kódu se opakovaně vyjadřovala EBA v rámci Q&A ke Směrnici PSD2 a Nařízení RTS. Jak již bylo uvedeno v kapitole 3.3.1 (*Znalost*) výše, EBA v rámci procesu Q&A 4053 uvedla, že třímístný číselný ověřovací kód nemusí naplnit požadavky bezpečnostních opatření z důvodu vyššího rizika „odhadnutí" tohoto kódu. V jiném případě EBA v Q&A 4041 uvedla, že poskytovatelé nesmí informovat uživatele o tom, který z prvků při ověření neproběhl správně, ani v případě, kdy jeden z prvků je neměnný a pokud nedojde k technické chybě, tak z povahy věci nemůže být chybným (např. token, který je zabudován v zařízení nebo uložen na cloudovém úložišti) a je tak zřejmé, že chyba nastala při ověření druhého použitého prvku SCA.[171] V neposlední řadě se EBA v Q&A 4141 zabývala dotazem, jestli je možné prvek použitý v rámci SCA (např. při přihlášení do internetového bankovnictví) možné opakovaně použít jako jeden z autentizačních prvků SCA v rámci téže relace pro účel aplikace SCA na iniciaci platební transakce po uplynutí časového limitu pěti minut stanoveného jako požadavek pro ověřovací kód. K danému EBA uvedla, že jeden z prvků použitých v době, kdy uživatel přistupoval ke svému platebnímu účtu online (včetně mobilní aplikace), lze opakovaně použít za předpokladu splnění povinností kladených na ověřovací kód, a současně je zapotřebí, aby dynamické propojení bylo vázáno na druhý prvek SCA, který uživatel použil při iniciaci platební transakce.[172]

Nad rámec požadavků k ověřovacímu kódu byla stanovena povinnost přijmout řadu opatření také v případě situací, kdy je při SCA vyžadováno Dynamické propojení. Jedná se především o následující povinnosti:

---

[169] Článek 4 odst. 3 Nařízení RTS.

[170] Bod 4 odůvodnění Nařízení RTS.

[171] European Banking Authority. Single Rulebook Q&A. Display of incorrect authentication factors in case of failed authentication attempts. *Eba.europa.eu* [online]. 2018 [cit. 26. 10. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4041

[172] European Banking Authority. Single Rulebook Q&A. Authentication code. *Eba.europa.eu* [online]. 2018 [cit. 26. 10. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4141

a) povinnost informovat plátce o výši částky platební transakce a o jejím příjemci;

b) vytvořený ověřovací kód je specifický pouze pro výši částky platební transakce a příjemce schváleného při iniciaci transakce (tento požadavek platí obdobně také pro blokaci peněžních prostředků ve vztahu ke karetní platební transakci a ve vztahu k dávce platebních transakcí pro jednoho či více příjemců)

c) poskytovatelem akceptovaný ověřovací kód odpovídá původní částce a příjemci;

d) jakákoliv změna částky či příjemce vede ke zneplatnění vytvořeného ověřovacího kódu;

e) povinnost zajistit důvěrnost, pravost a integritu údajů ve všech fázích týkajících se ověřovacího kódu.[173]

EBA se opakovaně vyjadřovala v rámci Q&A ke Směrnici PSD2 a Nařízení RTS také v souvislosti s dynamickým propojením. Jako příklad lze uvést Q&A 4556, v němž EBA uvedla, že Nařízení RTS nestanovuje konkrétní požadavky na způsob identifikace příjemce, přičemž je na poskytovateli, jaký způsob jeho identifikace si zvolí. Příjemce tak může být identifikován např. pomocí IBAN kódu, jeho části nebo jakýmkoliv jiným jedinečným způsobem za předpokladu splnění povinností kladených Dynamické propojení popsaných výše.[174] Dále bylo zapotřebí ze strany EBA vyjasnit, jak je to s dynamickým propojením a ověřovacím kódem v situaci, kdy výše transakční částky není dopředu známa. V rámci Q&A 5133[175] tak bylo upřesněno, že se v takové situaci posuzuje finální výše platby ve vztahu k částce, s níž byl plátce předem seznámen a k níž udělil souhlas. Pokud bude vyšší, ověřovací kód se neuplatní a je zapotřebí znova vyžadovat SCA nebo transakci zamítnout. V případě stejné či nižší částky tomu bude naopak a SCA není pro takovou platební transakci opakovaně vyžadovat.

[173] Článek 5 Nařízení RTS

[174] European Banking Authority. Single Rulebook Q&A. Definition of payee for dynamic linking. *Eba.europa.eu* [online]. 2019 [cit. 26. 10. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4556

[175] European Banking Authority. Single Rulebook Q&A. Dynamic linking: transactions for which the final amount is unknown and may be lower or higher than authenticated amoun. *Eba.europa.eu* [online]. 2020 [cit. 29. 10. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5133

Závěrem této kapitoly je třeba zmínit, že pro dva typy platebních služeb, kterými jsou nepřímé dání platebního příkazu a služba informování o platebním účtu, má poskytovatel platební služby, který vede uživateli platební účet povinnost umožnit jiným poskytovatelům některé (či obou) z těchto platebních služeb spoléhat se na postupy ve vztahu k SCA, který poskytovatel vedoucí platební účet v souvislosti se SCA zavedl.[176] Nařízení RTS blíže stanoví pravidla týkající se parametrů rozhraní, které umožní splnění této povinnosti, a požadavku na standardy komunikace. Lze tak shrnout, že pro tyto dvě platební služby, o které byl v rámci ZPS rozšířen okruh původních platebních služeb, bylo záměrem zákonodárce nastavit volnější regulatorní režim a usnadnit poskytování těchto platebních služeb.

4.3. Výjimky z použití SCA

V této kapitole se budu věnovat jednotlivým výjimkám z uplatňování bezpečnostních požadavků na SCA poskytovateli platebních služeb v případech, kdy je tak vyžadováno právními předpisy (v případě České republiky dle § 223 ZPS). Právní úpravu jednotlivých výjimek nalezneme v Nařízení RTS, které v jednotlivých článcích kapitoly III stanoví pravidla pro celkem devět výjimek a kterým se budu postupně věnovat v následujících podkapitolách. Téma výjimek bylo jedním z nejvíce diskutovaných při přípravě Nařízení RTS. EBA při přípravě textu Nařízení RTS zvažovala ve vztahu k výjimkám možný přístup k nastavení regulace především ze dvou pohledů: 1) jestli stanovit povinnost poskytovatelů výjimky uplatňovat v konkrétních případech, anebo stanovit seznam výjimek, které za splnění podmínek mohou poskytovatelé dobrovolně uplatnit, a 2) jestli by množství výjimek mělo být menšího či většího rozsahu. V obou případech EBA nakonec zvolila druhou z možnosti.[177]

[176] § 224 ZPS

[177] European Banking Authority. Final Report. Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2). *Eba.europa.eu* [online]. 2017 [cit. 26. 10. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1761863/314bd4d5-ccad-47f8-bb11-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%28EBA-RTS-2017-02%29.pdf

Před popisem jednotlivých výjimek bych rád zdůraznil, že Nařízení RTS stanoví k výjimkám několik obecných povinností. Předně je třeba říci, že splněním podmínky pro uplatňování výjimky se poskytovatel automaticky nezbavuje všech svých povinností v souvislosti se SCA. Podpůrně se uplatní požadavek, který ve zjednodušené formě patřil mezi jedny z prvních doporučení SecuRe Pay vydaných v roce 2013 (pro bližší informace viz kapitola 3.1 (*Bezpečnost a vývoj právní úpravy*) výše) a který ukládá poskytovatelům platebních služeb povinnost zavést mechanismy sledování transakcí, na základě kterých poskytovatel odhaluje neautorizované a podvodné platební transakce. Tyto mechanismy měly analyzovat platební transakce a jako minimální standard by měly sledovat a zpracovávat následující:

a) „*seznamy vyhrazených nebo odcizených ověřovacích prvků;*

b) *částku každé platební transakce;*

c) *známé scénáře podvodů při poskytování platebních služeb;*

d) *známky napadení malwarem při spojení v rámci postupu ověření; a*

e) *v případě, že poskytovatel platebních služeb poskytuje zařízení nebo software pro přístup, záznam a použití zařízení nebo softwaru pro přístup poskytnutého uživateli platebních služeb a neobvyklé použití zařízení nebo softwaru pro přístup.*“[178]

Výše uvedenou povinnost by měl každý poskytovatel plnit průběžně, měl by pravidelně vyhodnocovat stávající i nová rizika a testovat a kontrolovat, zdali jsou jím nastavené mechanismy dostatečné. Data zpracovávaná v souvislosti s plněním této povinnosti jsou relevantní z důvodu výpočtu celkové míry podvodů vztahující se na platební transakce ověřené na základě SCA a na transakce neověřené z důvodu uplatnění některé z výjimek dle článků 13 až 18 (včetně) Nařízení RTS, a především kvůli možnosti uplatnění výjimky založené na analýze transakčních rizik (blíže viz podkapitola 4.3.9 (*Analýza transakčních rizik*) níže). Celková míra podvodů se počítá na čtvrtletní bázi odděleně

[178] Článek 2 Nařízení RTS

pro (i) elektronické karetní platby na dálku a pro (ii) elektronické úhrady na dálku, a to následujícím způsobem:[179]

$$MP = \frac{A}{B}$$

Přičemž platí, že:

MP = celková míra podvodů u daného typu platební transakce.

A = celková hodnota všech neautorizovaných nebo podvodných transakcí na dálku daného typu za poslední čtvrtletí bez ohledu na případné vrácení peněžních prostředků.

B = celková hodnota všech transakcí na dálku u stejného druhu transakcí za poslední čtvrtletí bez ohledu na to, jestli bylo použito SCA nebo uplatněna některá z výjimek uvedených v 13 až 18 (včetně) Nařízení RTS.

Takto vypočtená míra podvodů je následně porovnána s referenční mírou stanovenou pro jednotlivé typy plateb, přičemž aby mohla být výjimka analýzy transakčních rizik uplatněna, musí být míra podvodů pro jednotlivé výše plateb rovna nebo nižší, než je referenční míra uvedená v tabulce níže:[180]

	Referenční míra podvodů (v %)	
Prahová hodnota pro výjimku	**Elektronické karetní platby na dálku**	**Elektronické úhrady na dálku**
500 EUR	0,01	0,005
250 EUR	0,06	0,01
100 EUR	0,13	0,015

Poskytovatelé uplatňující jakoukoliv z výjimek dle Nařízení RTS mají povinnost zpracovávat výše uvedená data o celkových hodnotách transakcí pro výpočet celkové míry podvodů a současně také informace o průměrné hodnotě transakce, o celkovém počtu transakcí, o jejich procentuálním podílu na celkové hodnotě všech transakcí a zároveň mají

[179] Článek 19 Nařízení RTS

[180] Příloha Nařízení RTS

povinnost tato data zpracovávat odděleně pro transakce, u nichž bylo uplatněno SCA, a pro transakce, u nichž byla uplatněna některá z výjimek.[181]

4.3.1. Informování o platebním účtu

V případě první výjimky má poskytovatel platební služby možnost neuplatnit SCA v případě, kdy je on-line přístup uživatele omezen na (i) zůstatek na jednom či více platebních účtech, nebo (ii) platební transakce za posledních 90 dnů provedené z jednoho či více platebních účtů. Současně při tomto přístupu nesmí být uživateli sděleny citlivé údaje o konkrétních platbách. Povinnost uplatnit SCA nicméně platí v případech, kdy je přístup uživatele k jednomu z uvedených případů učiněn poprvé a kdy od doby posledního použití SCA v souvislosti s výše uvedenými případy uplynulo 90 dnů.[182]

4.3.2. Bezkontaktní platby v místě prodeje

Druhá výjimka se vztahuje na bezkontaktní elektronické platby (čili platby provedené uživatelem například prostřednictvím fyzické platební karty či její virtuální podoby na základě zařízení jakým je chytrý mobilní telefon či hodinky). Zde jsou omezení nastavena na výši jednorázové platby nepřesahující 50 EUR nebo její ekvivalent v jiné měně a současně (i) nesmí být překročena částka 150 EUR nebo její ekvivalent v jiné měně za všechny takto učiněné platby od doby poslední uplatnění SCA, nebo (ii) počet takových transakcí bez uplatnění SCA nesmí přesáhnout pět.[183] Bude tak záležet na rozhodnutí poskytovatele platební služby, který ze dvou možných způsobů si při uplatnění této výjimky zvolí.

4.3.3. Terminály bez obsluhy pro jízdné a poplatky za parkování

Třetí výjimka se vztahuje na případy, kdy plátce iniciuje elektronickou platební transakci u terminálu bez obsluhy za účelem uhrazení jízdného nebo poplatku za parkování.[184] Byla jednou z velmi diskutovaných v rámci příprav Nařízení RTS a jedná se o jednu z výjimek, která nebyla obsažena v prvotních návrzích Nařízení RTS a která byla do jeho textu zahrnuta až po veřejné konzultaci k připravovanému návrhu Nařízení RTS.

[181] Článek 21 Nařízení RTS

[182] Článek 10 Nařízení RTS

[183] Článek 11 Nařízení RTS

[184] Článek 12 Nařízení RTS

EBA se rozhodla tuto výjimku po veřejné konzultaci a podnětů ze strany řady subjektů zahrnout, protože povinnost uplatnění SCA v tomto případě nebyla řadou subjektů považována za proporcionální vzhledem k její nízké rizikovosti a nebyla dle jejich názoru ani ve veřejném zájmu, a to především z důvodu zbytečného vytváření front při placení a z důvodu zamezení tzv. „shoulder surfingu" (získávání citlivých osobních údajů tzv. „pohledem přes rameno").[185]

4.3.4. Důvěryhodní příjemci

Další výjimka lze uplatnit na případy, kdy si uživatel v rámci svého platebního účtu vytvořil seznam důvěryhodných příjemců (jako příjemců platebních transakcí) a provádí platební transakci na účet některého z příjemců zařazených na tento seznam. Povinnost uplatnit SCA se nicméně uplatní v případě nastavení nového příjemce jako důvěryhodného a při jiných změnách stávajícího seznamu.[186] Cílem této výjimky je usnadnit uživatelům pravidelné platby, kdy uživatel např. přeposílá peníze na účet některého z přátel či členů rodiny nebo kdy platí pravidelně za určité služby, u nichž si z jakéhokoliv důvodu nenastavil trvalý příkaz či nedal souhlas k inkasu. Pro takové případy tak má uživatel možnost příjemce nastavit jako důvěryhodného a při všech budoucích platbách nemusí být poskytovatelem vyžadováno SCA.

4.3.5. Opakující se transakce

Nařízení RTS stanoví, že poskytovatel platební služby musí vyžadovat ve všech případech, kdy uživatel poprvé vytváří, mění nebo poprvé iniciuje řadu opakujících se transakcí se stejnou částkou a stejným příjemcem.[187] Na všechny navazující a opakující se transakce, u nichž se nebude měnit příjemce ani stanovená výše částky, lze však uplatnit

[185] European Banking Authority. Final Report. Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2). *Eba.europa.eu* [online]. 2017 [cit. 26. 10. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1761863/314bd4d5-ccad-47f8-bb11-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%28EBA-RTS-2017-02%29.pdf

[186] Článek 13 Nařízení RTS

[187] Článek 14 Nařízení RTS

výjimku z požadavku požadovat SCA. Tato výjimka tak míří především na situace, kdy si uživatel sjedná nějakou službu, za níž platí pravidelné (nejčastěji asi měsíční) předplatné. Typicky se bude jednat o streamovací služby typu Netflix, Disney+, HBO Max, dále pak služby zaměřené na hlasové služby jako jsou Apple Music či Spotify, anebo o předplatná periodik, kdy z českého trhu lze zmínit například předplatné Hospodářských novin. Výjimka by se zároveň měla uplatnit i na tzv. trvalé platební příkazy, u nichž uživatel dopředu nastaví parametry budoucích platebních transakcí (jako výši částky, příjemce, frekvenci zasílání těchto plateb a dobu, po kterou k nim bude docházet) a při každé budoucí platbě na základě tohoto trvalého příkazu platba automaticky proběhne a SCA nebude vyžadováno.

4.3.6. Úhrady mezi účty téže fyzické nebo právnické osoby

Další výjimka se týká iniciace úhrady, kdy plátcem i příjemce je ta stejná fyzická či právnická osoba a oba platební účty jsou vedeny u jednoho poskytovatele platebních služeb.[188] Jinými slovy při uplatnění této výjimky se u všech úhrad uživatele v rámci jednoho poskytovatele platebních služeb (např. banky) nebude při iniciaci platby vyžadovat SCA. Pokud by si však uživatel peněžní prostředky zasílal na svůj účet, který je ale veden u jiného poskytovatele, tak se požadavek na SCA standardně uplatní a výjimku nelze aplikovat.

4.3.7. Transakce týkající se malých částek

Tato výjimka je velmi podobná výjimce zaměřené na bezkontaktní platby v místě prodeje. Pro možnost jejího uplatnění je zapotřebí nepřesáhnout výši elektronické platební transakce stanovené na 30 EUR (a jejího ekvivalentu v cizí měně) a současně (i) nepřekročit kumulativní částku za předchozí obdobné platby ve výši 100 EUR (a jejího ekvivalentu v cizí měně), nebo (ii) nepřesáhnout počet pěti obdobných předchozích transakcí bez použití SCA. Rozdílem je tak pouze výše stanovených částek a okruh situací, kdy se tato výjimka uplatní. Oproti výjimce pro bezkontaktní platby v místě prodeje lze tuto výjimku uplatnit v situaci, kdy plátce iniciuje elektronickou platební transakci na dálku, nikoliv však bezkontaktně.[189] Platební prostředek tak v tomto případě nemusí být fyzicky přítomen na stejném místě jako zařízení poskytovatele k jeho přijetí. Pro vyloučení pochybností je třeba uvést, že výše limitů

[188] Článek 15 Nařízení RTS

[189] Článek 16 Nařízení RTS

či počtu transakcí se počítají pro obě výjimky odděleně a výjimky jsou na sobě vzájemně nezávislé.

Při přípravě Nařízení RTS se řada účastníků vyjadřovala k výši částek, do jejichž výše může poskytovatel za splnění zbývajících podmínek výjimku uplatnit. Prvotním návrhem EBA bylo omezit jednorázovou výši platby na 10 EUR, což řada účastníku považovala za velmi nízké a neproporcionální. Protinávrhem účastníků bylo sjednocení výše částek s těmi, které jsou stanoveny pro výjimku pro bezkontaktní platby v místě prodeje. EBA s těmito názory neztotožnila a uvedla, že v případě elektronických platebních transakcí na dálku existuje vyšší riziko neautorizované nebo podvodné transakce, a to právě z důvodu, že platební prostředek nemusí být na stejném místě jako zařízení poskytovatele k jeho přijetí. Jako kompromis se EBA rozhodla ve finálním návrhu Nařízení RTS, který byl přijat, částku navýšit z původních 10 na 30 EUR.[190]

4.3.8. Zabezpečené platební procesy a protokoly společnosti

Další výjimkou, která byla při přípravě Nařízení RTS častým předmětem diskuzí, je výjimka vztahující se na podnikové platby. Lze ji uplatnit v případech právnických osob, které iniciují elektronické platební transakce za použití zvláštních platebních procesů nebo protokolů, které jsou zpřístupněny pouze plátci, který současně nesmí být spotřebitelem. Uplatnění této podmínky je podmíněno souhlasem příslušného dohledového orgánu, který musí úroveň zabezpečení považovat jako dostatečnou.[191] ČNB v této souvislosti vydala dohledové sdělení, v němž informuje dohlížené subjekty o povinnost předkládat potřebné

[190] European Banking Authority. Final Report. Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2). *Eba.europa.eu* [online]. 2017 [cit. 26. 10. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1761863/314bd4d5-ccad-47f8-bb11-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%28EBA-RTS-2017-02%29.pdf

[191] Článek 17 Nařízení RTS

doklady ČNB k posouzení uplatnění této výjimky, jež zároveň obsahuje odkaz na vzorový formulář obsahující potřebné údaje ke splnění této notifikační povinnosti.[192]

Požadavek na doplnění výjimky vztahující se k podnikovým platbám byl vznesen již při veřejné konzultaci se zainteresovanými stranami v roce 2016. EBA tento návrh zamítla s odůvodněním, že neexistuje důvěryhodný důkaz o tom, že by veškeré podnikové platby byly nízkorizikové a že na podnikové platby lze uplatnit řadu výjimek z návrhu nařízení a ze stávající Směrnice PSD2. Opakovaně se požadavek na doplnění výjimky týkající se podnikových plateb objevil v dopise Evropské komise[193] reagujícím na návrh znění Nařízení RTS, jež jí předložila na počátku roku 2017 EBA a který neobsahoval samostatnou výjimku vztahující se na korporátní platby. Evropská komise ve svém dopise navrhla znění, které neobsahovalo část omezující uplatnění výjimky pouze na plátce, kteří nejsou spotřebiteli. V reakci na tento dopis se EBA k zavedení takové výjimky opět vyjádřila nesouhlasně, nicméně jako kompromis navrhla rozšíření stávající výjimku analýzy transakčních rizik, nikoliv však konkrétně ve vztahu k podnikovým platbám či právnickým osobám, ale ve vztahu k plátcům, kteří nejsou spotřebiteli.[194] Výsledkem těchto diskuzí tak bylo přijetí stávajícího znění, které výjimku omezuje jak na právnické osoby, tak na plátce, kteří nejsou spotřebiteli.

---

[192] ČESKÁ NÁRODNÍ BANKA. Dohledové sdělení č. 2/2021 K možnosti používat výjimku ze silného ověření klienta v případech zabezpečených platebních procesů a protokolů společnosti. *Cnb.cz* [online]. 2021 [cit. 27. 10. 2022]. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/dohled-financni-trh/.galleries/vykon_dohledu/dohledove_benchmarky/download/dohledove_sdeleni_2021_02.pdf

[193] European Banking Authority. Letter from Olivier Guersent, on the Commission intention to amend the draft RTS on SCA and CSC. *Eba.europa.eu* [online]. 2017 [cit. 26. 10. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1863077/efbf06e1-b0e9-4481-88e5-b70daa663cb9/%28EBA-2017-E-1315%29%20Letter%20from%20O%20Guersent%2C%20FISMA%20re%20Commission%20intention%20to%20amend%20the%20draft%20RTS%20on%20SCA%20and%20CSC%20-Ares%282017%292639906.pdf

[194] European Banking Authority. Final Report. Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2). *Eba.europa.eu* [online]. 2017 [cit. 26. 10. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1761863/314bd4d5-ccad-47f8-bb11-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%28EBA-RTS-2017-02%29.pdf

4.3.9. Analýza transakčních rizik

Poslední, nikoliv však nejméně významnou, je výjimka založená na analýze transakčních rizik. Tuto výjimku mohou poskytovatelé platebních služeb použít v případě, kdy plátce iniciuje elektronickou platební transakci na dálku, která byla poskytovatelem identifikována jako transakce s nízkou mírou rizika na základě mechanismů sledování transakcí. Nad rámec výše uvedené obecné povinnosti sledování transakcí, uplatňující se pro všechny poskytovatele platebních služeb, musí být pro uplatnění této výjimky kumulativně splněny následující podmínky:

a) míra podvodů nahlášená poskytovatelem nesmí překročit hodnotu pro daný typ transakce, která se nachází v příloze k Nařízení RTS a která byla blíže popsána v kapitole 4.3 (*Výjimky z použití SCA*) výše;

b) hodnota částky transakce je nižší než příslušná prahová hodnota uvedena ve stejné tabulce, na kterou je odkazováno v bodě a) výše;

c) poskytovatel při analýze rizik nezjistí:

   i. „*neobvyklé výdaje nebo vzorec chování plátce;*

   ii. *neobvyklé informace o zařízení/softwaru plátce pro přístup;*

   iii. *napadení malwarem při spojení v rámci postupu ověření;*

   iv. *známé scénáře podvodů při poskytování platebních služeb;*

   v. *neobvyklé místo plátce;*

   vi. *vysoce rizikové místo příjemce.*“[195]

Pro výpočet míry podvodů se uplatní vzorec popsaný v kapitole 4.3 (*Výjimky z použití SCA*) výše. Na poskytovatele, kteří hodlají či již uplatňují tuto výjimku, jsou kladeny zvýšené notifikační požadavky týkající se prahových hodnot a referenční míry podvodů.

[195] Článek 18 odst. 1 a 2 Nařízení RTS

V případě, že dojde k překročení referenční míry podvodů dvě čtvrtletí po sobě, ztrácí poskytovatel právo výjimku na základě analýzy transakčních rizik poskytovat.[196]

Důvodem zahrnutí této výjimky bylo velké množství připomínek zainteresovaných stran v rámci veřejné konzultace k přípravě Nařízení RTS, které opakovaně požadovaly, aby byla zavedena výjimka, která bude nějakou formou přímo navázána na interní analýzu rizik poskytovatele platební služby. EBA akceptovala tento často se opakující požadavek a snažila se nastavit parametry tak, aby tato výjimka nepokrývala plošně většinu úkonů a nešla tak proti smyslu zavedení SCA. Z tohoto důvodu došlo ke stanovení poměrně přísných požadavků jak na parametry samotné analýzy, tak na prahové hodnoty, kterých je zapotřebí dosáhnout, a na specifické notifikační povinnosti. Pro konkrétnější představu je zapotřebí, aby se pro možnost uplatnění výjimky ve vztahu k elektronickým úhradám na dálku do prahové hodnoty 500 EUR nevyskytlo víc než pět neautorizovaných či podvodných plateb na každých 100 tisíc plateb. V případě elektronických karet se musí jednat o maximálně jednu podvodnou platbu z každých 10 tisíc.[197]

[196] Článek 20 Nařízení RTS

[197] European Banking Authority. Final Report. Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2). Eba.europa.eu [online]. 2017 [cit. 25. 10. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1761863/314bd4d5-ccad-47f8-bb11-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%28EBA-RTS-2017-02%29.pdf

5. Úskalí, dopady a zhodnocení regulace, SCA ve světě

V poslední z hlavních částí této práce se zaměřím na problematiku behaviorální biometrie, na povinnost vyžadovat SCA v některých zemích mimo území EHP, na úskalí stávající regulace a na její celkové zhodnocení. Postupně se tak nejdříve se vrátím k tématu inherence, jako jednoho z prvků SCA, a to konkrétně na oblast behaviorální biometrie a její stávající i budoucí možnosti uplatnění v rámci SCA. Z důvodu posouzení účelnosti úpravy se budu následně věnovat rozboru situace v několika zemích mimo území EHP a závěrem se zaměřím na některá úskalí stávající právní úpravy, analýzu dopadů jejího zavedení a její celkové zhodnocení.

5.1. Behaviorální biometrie

V kapitole 3.3.3 (*Inherence*) jsem se zabýval tématem inherence jako třetího z prvků SCA dle terminologie Směrnice PSD2 (v textu ZPS se jedná o biometrické údaje uživatele) a uvedl jsem několik teoretických klasifikací biometrie. Jedním z dalších pohledů na biometrii je její rozdělení na biometrii tělesnou (fyziologickou), která se zaměřuje na analýzu tělesných aspektů člověka, mezi které patří např. sken otisku prstu, rozpoznání duhovky a sítnice nebo rozpoznávání obličej, a na biometrii chování (behaviorální), které se budu podrobněji věnovat níže.[198]

Biometrie chování se zaměřuje na vlastnosti, které se v životě naučíme díky interakci se svým okolním prostředím a přírodou a které utváří různé vzorce chování, které společně charakterizují jedinečný profil každého jedince. Zaměřuje na zkoumání měřitelného lidského chování, které je následně použito k identifikaci nebo ověření totožnosti tohoto jedince. Vzorce lidského chování ovlivňuje také psychika jedince, jeho sociální vazby a společnost. Jako takové se mění v čase a mohou se vyvíjet s ohledem na různé okolnosti a situace, ve kterých se daný jedinec v konkrétním momentě nachází.[199]

[198] WANG Liang, Xin GENG. *Behavioral biometrics for human identification*. Hershey: IGI Global, 2010, s. 1-44. ISBN 978-1-60566-726-3.

[199] SAEED, Khalid, Marcin ADAMSKI, Tapalina BHATTASALI, Mohammad K. NAMMOUS, Piotr PANASIUK, Mariusz RYBNIK a Soharab H. SHAIKH. *New directions in behavioral biometrics.* Boca Raton: CRC Press, Taylor & Francis Group, LLC, 2017, s. 2-3. ISBN 978-14987-8462-7.

V posledních letech nabrala behaviorální biometrie na popularitě a našla si místo v oblasti informační bezpečnosti v kontextu analýzy jedinců podle jejich jedinečných vlastností a vzorců chování, které lidé vědomě či nevědomě provádí. Předmětem této analýzy je mimo jiné také interakce osob s technologickými zařízeními, jakými jsou například myš nebo klávesnice od počítače, chytré telefony, chytré hodinky nebo tablety s chytrými pery (tzv. stylusy), které bývají součástí jejich příslušenství.[200]

V rámci ověřování uživatele na základě tělesné biometrie dochází k nejdříve k registraci vzorku biometrických dat uživatele, který typicky proběhne jeho nasnímáním za pomoci specializovaného senzoru a následným uložením pro budoucí účely ve formě tzv. digitální šablony. Jakékoliv budoucí ověření pak v praxi probíhá tak, že dojde k nasnímání stejného druhu biometrického údaje, který je poté srovnán s touto digitální šablonou. Ověření tak vždy probíhá výlučně k určitému referenčnímu bodu, kterým je okamžik ověření tohoto opětovně nasnímaného biometrického údaje. Oproti tomu při použití behaviorální biometrie je chování uživatele analyzováno průběžně na pozadí bez vědomí uživatele, aniž by jej rušilo při jeho činnosti či od něj vyžadovalo specifický úkon. Z tohoto důvodu je behaviorální biometrie někdy označována také jako pasivní.[201]

[200] SHARMA, Mridula a Haytham ELMILIGI. *Recent Advances in Biometrics. Behavioral Biometrics: Past, Present and Future* [online]. Londýn: IntechOpen. 2022 [online]. ISBN: 978-1-80355-458-7 Dostupné z: https://www.intechopen.com/chapters/80748

BLAKSTAD, Sofie a Robert ALLEN. *Fintech Revolution. Universal inclusion in the new financial ecosystem*. Londýn: Palgrave Macmillan, 2018, s. 34. ISBN: 978-3-319-76013-1.

[201] The Payments Association. Physical biometrics vs. Behavioral biometrics. Thepaymentsassociation.org [online]. 2021 [cit. 30. 10. 2022]. Dostupné z: https://thepaymentsassociation.org/article/physical-biometrics-vs-behavioral-biometrics/; a

OneSpan Inc. Behavioral Biometrics. *Onespan.com* [online]. 2022 [cit. 30. 10. 2022]. Dostupné z: https://www.onespan.com/topics/behavioral-biometrics; a

REVETT, Kenneth. *Behavioral Biometrics. A Remote Access Approach*. Chichester, UK: John Wiley & Sons ltd, 2008, s. 12-15. ISBN: 978-0-470-51883-0.

Během výše uvedené průběžné analýzy chování dochází za pomoci senzorů a jiných technologií ke kontinuálnímu sběru rozsáhlého množství různých typů dat o uživateli, jeho chování a jeho zařízení. Za příklady takových dat lze označit:

a) **znaky chování související se zařízením** – jedná se o data získaná ve vztahu k fyzické interakci uživatele se zařízením, např. používání myši, psaní na klávesnici, způsob manipulace s počítačem, telefonem nebo jiným podobným zařízením;

b) **znaky chování související se službou** – veškeré interakce s webem či aplikací, které mohou sloužit jako základ pro analýzu, např. denní doba, kdy uživatel službu využívá, jaké funkce používá nebo jakým způsobem, v jaké posloupnosti a jak dlouho službu využívá; nebo

c) **kontextové informace** – jedná se o doplňující údaje k výše uvedeným kategoriím, např. zeměpisná poloha, označení a identifikace WiFi či jiné sítě, prostřednictvím které je uživatel připojen k internetu, nebo jeho IP adresa .[202]

V rámci analýzy výše uvedených dat dochází za pomocí technologií, algoritmů umělé inteligence a metody strojového učení k vytváření jedinečných vzorců chování, jež dohromady utváří jedinečný digitální obraz uživatele. Tento digitální obraz se však může měnit v čase a za pomoci strojového učení dochází k jeho aktualizaci či rozšíření. V budoucích případech tak dochází k neustálému porovnávání nové činnosti s minulým chováním, analýze a ověřování vzorců chování daného uživatele. Díky kombinaci umělé inteligence a strojového učení je současně možné analyzovat rozsáhlé množství dat a v reálném čase odhalovat případné anomálie. Software je na základě těchto anomálií schopen přiřadit nové činnosti skóre podobnosti s předchozím chováním uživatele, kdy vyšší zpravidla znamená vyšší míru pravděpodobnosti, že se jedná o stejnou osobu. S každým dalším úkonem se toto skóre může měnit a ověření tak neprobíhá pouze ve vztahu k jednomu referenčnímu bodu, ale k celé relaci, což je jednou z jeho hlavních výhod této technologie. Naopak nedostatečná míra podobnosti může například vyvolat spuštění dodatečného ověřovacího mechanismu, který napomůže určit, jestli se jedná o stejného uživatele

[202] RecFaces LLC. Behavioral Biometrics: Explaining in Detail. *RecFaces.com* [online]. 2021 [cit. 30. 10. 2022]. Dostupné z: https://recfaces.com/articles/what-are-behavioral-biometrics

či nikoliv. Behaviorální biometrie tak ve zkratce napomáhá určit, zda je konkrétní osoba skutečně tím uživatelem, za kterého se vydává, nebo jestli se jedná o nějakou formu podvodného jednání.[203]

5.1.1. Druhy behaviorální biometrie, její výhody a nevýhody

V rámci biometrie chování dochází k analýze různých typů činnosti uživatelů. Takové činnosti mohou souviset nebo být výsledkem motorických schopností, stylu, preferencí, znalostí, strategie nebo jiných lidských dovedností. Podle znaků a vlastností, které jsou používány pro sběr dat a analýzu chování uživatele, můžeme behaviorální biometrii klasifikovat jako založenou:

a) **na dovednostech uživatele**, kdy je chování založeno na jeho instinktivních a jedinečných svalových pohybech, např. dynamika psaní na klávesnici, styl řízení automobilu, způsob hraní počítačových her nebo schopnost a způsob programování;

b) **na znalostech uživatele**, kdy konkrétní znalosti uživatele jsou předpokladem pro jeho obvyklé chování, např. způsob zadávání hesla nebo tvorba autorského textu;

c) **na stylu uživatele**, který je pro něj jedinečný a lze jej díky němu identifikovat, např. síla stisku, psaní e-mailů, způsob kreslení, používání gest nebo zacházení s myší;

d) **na strategii uživatele**, kterou uživatel používá a je pro něj jedinečná, např. způsob hraní her nebo vyřizování e-mailů;

e) **na preferencích uživatele**, které mohou spočívat v upřednostnění některých zařízení, slov, písmen nebo funkcionalit, např. používání platební karty, používání funkcí a nástrojů u služeb nebo používání jazyka; nebo

[203] Tamtéž a REES Megan. The Future of User Authentication: A Guide to Behavioral Biometrics. *Expertinsights.com* [online]. 2022 [cit. 30. 10. 2022]. Dostupné z: https://expertinsights.com/insights/a-guide-to-behavioral-biometrics/

f) **na motorických dovednostech uživatele,** kdy jednotlivé svalové pohyby jsou pro daného uživatele vrozené nebo přirozené, jedinečné a neměnné, např. styl chůze, mrkání, pohyb rtů, stisk tlačítek na obrazovce, styl podepisování, síla stisku, hlas nebo mluva.[204]

Způsobů klasifikace existuje samozřejmě více, lze se setkat například s tříděním na pohyby těla, hlasové vstupy nebo gesta související se zařízením, popř. lze na biometrii chování nahlížet specificky dle jednotlivých činností, které byly uvedeny jako příklady výše.

Než se dostaneme k analýze možností použití behaviorální biometrie v rámci SCA, považuji za vhodné zmínit hlavní přednosti a úskalí této technologie.

Mezi hlavní výhody lze řadit následující:[205]

(i) **flexibilita** – teoreticky nekonečné množství vlastností a prvků, které jsou k dispozici pro analýzu vzorců chování uživatele a které mohou být přizpůsobeny konkrétním potřebám analýzy;

---

[204] SHARMA, Mridula a Haytham ELMILIGI. *Biometrics: Past, Present and Future.* In: SARFRAZ, Muhammad, editor. *Recent Advances in Biometrics. Behavioral* [online]. Londýn: IntechOpen. 2022 [online]. [cit. 30. 10. 2022]. ISBN: 978-1-80355-458-7. Dostupné z: https://www.intechopen.com/chapters/80748; a PALMA, David a MONTESSORO, Pier Luca. *Biometric-Based Human Recognition Systems: An Overview*. In: SARFRAZ, Muhammad, editor. *Recent Advances in Biometrics. Behavioral* [online]. Londýn: IntechOpen. 2021 [online]. [cit. 30. 10. 2022]. ISBN: 978-1-80355-458-7. Dostupné z: https://www.intechopen.com/chapters/80748

[205] International Biometrics + Identity Association. Behavioral Biometrics. *Ibia.org* [online]. 2017 [cit. 30. 10. 2022]. Dostupné z: https://www.ibia.org/download/datasets/3839/Behavioral;
RecFaces LLC. Types of Biometrics: Complete Guide. *RecFaces.com* [online]. 2020 [cit. 30. 10. 2022]. Dostupné z: https://recfaces.com/articles/types-of-biometrics; a
NOORIALA Amir. The difference between physical and behavioral biometrics, and which you should be using. *Information-age.com* [online]. 2021 [cit. 30. 10. 2022]. Dostupné z: https://www.information-age.com/difference-between-physical-and-behavioural-biometrics-which-you-should-be-using-123496929/; a
SHARMA, Mridula a Haytham ELMILIGI. *Biometrics: Past, Present and Future.* In: SARFRAZ, Muhammad, editor. *Recent Advances in Biometrics. Behavioral* [online]. Londýn: IntechOpen. 2022 [online]. [cit. 30. 10. 2022]. ISBN: 978-1-80355-458-7. Dostupné z: https://www.intechopen.com/chapters/80748;

(ii) **účinnost** – behaviorální biometrika se prozatím jeví jako velmi účinná v detekci podvodných jednání a podstatným způsobem snižuje čas potřebný pro odlišení legitimního uživatele od podvodníka;

(iii) **vysoká míra přesnosti** – v případě analýzy rozsáhlého množství dat dosahuje poměrně vysokých hodnot přesnosti;

(iv) **pasivita** – analýza dat a identifikace uživatele probíhá na pozadí bez vědomí uživatele a pro identifikaci není zapotřebí konkrétní úkon uživatele;

(v) **dynamika ověření** – na rozdíl od statických prvků ověření, které jsou schopny provést ověření pouze k jednomu konkrétnímu okamžiku a jsou tak schopny pouze určit, že prvek ověření je správný, nikoliv však, že jej použila ta správná osoba, lze díky průběžné analýze chování uživatele v rámci konkrétní relace legitimně určit, že se jedná o konkrétního uživatele po celou její dobu;

(vi) **bezpečnost** – zatímco je v praxi možné získat kopie cizích tělesných biometrických údajů a zneužít je, tak se naopak jeví jako velmi náročné až prakticky nerealistické precizně napodobit chování uživatele tak, aby to software s umělou inteligencí nerozpoznal, přičemž v případě jakýchkoliv nesrovnalostí či anomálií lze automaticky nastavit povinnost vyžadování dodatečného autentizačního prvku;

(vii) **ochrana osobních údajů** – vzhledem ke své povaze je behaviorální biometrie z pohledu sběru citlivých osobních údajů méně invazivní, jelikož sbírá velké množství jednotlivě nevýznamných druhů dat a primárně pracuje s daty, které jsou již v dnešní době o uživatelích běžně zpracovávána při jejich online aktivitách;

(viii) **nízké technologické požadavky na straně uživatele** – behaviorální data mohou být o uživateli sbírána bez ohledu na použití konkrétního zařízení a nekladou tak velký požadavek na konkrétní funkcionality jednotlivých zařízení jako některé jiné způsoby; a

(ix) **lepší výsledky v čase** – vzhledem k použití strojového učení a umělé inteligence bude s narůstajícím množstvím zpracovaných dat míra bezpečnosti stoupat.

Naopak je třeba upozornit na následující slabé stránky:[206]

(i) **sběr velkého množství dat** – pro úspěšné uplatnění behaviorální biometrie je zapotřebí analyzovat rozsáhlé množství dat a tato dále zpracovávat, aby bylo možné určit vzorce chování, vytvořit a pravidelně aktualizovat digitální profil každého uživatele a dále sbírat a analyzovat data o jednotlivých relacích, kde dochází k analýze podvodných jednání a ověření identity uživatelů;

(ii) **nákladnost implementace a provozu** – jedná se o technicky velmi náročné řešení, které může být nejen pro malé a střední podniky nákladově velmi zatěžující;

(iii) **nutnost přizpůsobování se změnám chování uživatele** – jelikož se chování uživatele mění v čase, je zapotřebí kontinuálně tyto změny sledovat a systém se musí těmto změnám přizpůsobovat;

(iv) **přesnost** – tuto vlastnost je nezbytné uvést i jako nevýhodu, a to vzhledem ke skutečnosti, že chování uživatele se může nenadále měnit (např. vlivem únavy, nemoci, emočního stavu nebo díky vlivu návykových látek);

(v) **ochrana osobních údajů** – obdobně jako v bodě výše je aspekt ochrany soukromí současně nevýhodou, protože vzhledem k velkému množství nasbíraných dat se objevují obavy o dostatečné míře ochrany osobních údajů uživatelů a není prozatím zcela jasné, jaký k této technologii bude většinový postoj uživatelů.

[206] Tamtéž.

5.1.2. Behaviorální biometrie v rámci SCA

EBA opakovaně uvedla (příkladem lze uvést Q&A 5620[207] či stanovisko EBA k implementaci Nařízení RTS[208]), že behaviorální biometrie spadá pod prvek inherence a behaviorální procesy vytvořené tělem lze za splnění obecných podmínek použít jako jeden z prvků SCA. Jako příklad EBA uvedla informace o tom, jakým způsobem uživatel používá počítač nebo webovou stránku, způsob psaní uživatele na zařízení nebo jeho dynamika psaní na klávesnici. EBA v rámci Q&A 5620 dále uvedla, že je možné, aby poskytovatelé platebních služeb získávali behaviorální data a informace o nakládání uživatele s jeho zařízením způsobem, který chrání jeho soukromí, nevyužívá citlivé údaje a současně předchází/eliminuje riziko podvodů. Ve stanovisku EBA k revizi Směrnice PSD2 nicméně EBA uvedla, že behaviorální biometrie vztahující se například k platebním návykům, analýze vztahu k životnímu prostředí, času transakce atp. nenaplňuje požadavek prvku inherence, protože nesouvisí s lidským tělem a jeho vlastnostmi, a zároveň uvedla, že není zcela jasné, jaký je současný vztah behaviorální biometrie a aplikace Nařízení GDPR.[209]

Je tak otázkou, jakým způsobem mohou nyní poskytovatelé platebních služeb behaviorální biometrii používat a jak by bylo vhodné právní úpravu případně v budoucnu upravit, aby bylo lépe dosaženo zvýšené ochrany a zachování uživatelského zážitku.

---

[207] European Banking Authority. Single Rulebook Q&A. Use of behavioural data for SCA. *Eba.europa.eu* [online]. 2020 [cit. 02. 11. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5620

[208] European Banking Authority. Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC. *Eba.europa.eu* [online]. 2018 [cit. 02. 11. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2137845/0f525dc7-0f97-4be7-9ad7-800723365b8e/Opinion%20on%20the%20implementation%20of%20the%20RTS%20on%20SCA%20and%20CSC%20%28EBA-2018-Op-04%29.pdf

[209] European Banking Authority. Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2). *Eba.europa.eu* [online]. 2022 [cit. 02. 11. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2022/Opinion%20od%20PSD2%20review%20%28EBA-Op-2022-06%29/1036016/EBA%27s%20response%20to%20the%20Call%20for%20advice%20on%20the%20review%20of%20PSD2.pdf

Za stávající situace mohou poskytovatelé platebních služeb použít kategorii behaviorální biometrie, která přímo nějakým způsobem souvisí s lidským tělem, jako prvek inherence a za splnění ostatních podmínek jej mohou použití v rámci SCA. Zbývající údaje, které EBA nyní nepovažuje jako spadající pod prvek inherence, mohou být využity v rámci analýzy rizik dle článku 2 Nařízení RTS. V této souvislosti je vhodné uvést, že poskytovatel platební služby může dle § 257 ZPS zpracovávat osobní údaje bez souhlasu subjektů těchto údajů, pokud tyto zpracovává výlučně pro účely předcházení podvodným jednáním v oblasti platebního styku, jejich vyšetřování a odhalování. Toto ustanovení by se nicméně dle mého názoru nemělo vykládat příliš extenzivně. V neposlední řadě si lze představit situaci, kdy poskytovatel platební služby nastaví procesy analýzy transakčních rizik tak, že v rámci nich bude spoléhat na práci s behaviorální biometrií, která by tak mohla sloužit jako podklad pro uplatnění výjimky z povinnosti požadovat SCA.

Jako problematické vnímám rozřazení druhů biometrických údajů na vhodné/nevhodné pro použití prvku inherence. V praxi může být velmi složité určit, jestli v rámci analýzy chování uživatele došlo k jeho ověření právě na základě toho či onoho prvku nebo skupiny prvků, protože dochází ke kontinuálnímu zpracovávání rozsáhlého množství dat o uživateli. Omezovat řešení na použití pouze některých druhů údajů může dle mého názoru nelogicky zužovat prostor pro technologické inovace, jejichž zachování je uváděno jako jeden z hlavních cílů regulace.

Zároveň by mělo být postaveno na jisto, jestli lze behaviorální biometrii používat pro účel analýzy rizik podvodných jednání nebo jako prvek ověření. Používat řešení založená na behaviorální biometrii se jeví jako velmi vhodné pro předcházení podvodným jednáním, nicméně vzhledem k některým jejím vlastnostem a potenciálu této technologie by nemuselo omezením jejího použití pouze pro účel předcházení podvodným jednáním dojít k využití úplnému využití. Jsem proto názoru, že tato technologie by měla být nadále rozvíjena, regulátorem podporována a mohla by v rámci povinnosti použít SCA hrát v budoucnu významnější roli. Právní úprava by se dle mého názoru mohla v budoucnu ubírat následujícím způsobem:

- stávající povinnost použít dva prvky z různých kategorií SCA by mohla být opuštěna a za podmínky dosažení vyšší úrovně bezpečnosti by mělo být umožněno použít dva prvky ze stejné kategorie. Alternativně by mohl být

rozdělen prvek inherence na biometrii tělesnou a biometrii behaviorální, protože kombinace těchto dvou prvků bude v budoucnu vysoce pravděpodobně dosahovat vyšší úrovně bezpečnosti oproti použití prvků z jiných kategorií;

- neměl by být opomenut fakt, že behaviorální biometrie je jako jediná ze stávajících prvků schopna dynamickým způsobem ověřovat identitu uživatele a oproti statickým prvkům je schopna nejen ověřit shodu daného prvku, ale taktéž osoby, která tento prvek zadává. Jako taková má s jistou mírou pravděpodobnosti vyšší šanci dosáhnout maximální úrovně předcházení podvodných jednání za současného zachování uživatelského zážitku, který při používání platebních služeb nebude omezován dodatečnými úkony v souvislosti s ověřováním jednotlivých prvků. Z tohoto důvodu by se nastavení regulace mělo vyvíjet způsobem, který bude pro účel ověření totožnosti uživatele reflektovat vývoj technologií a preferovat využití dynamického způsobu ověření před statickým k jednomu referenčnímu bodu. S ohledem na vývoj této technologie by úprava SCA mohla proběhnout některým z následujících způsobů:

    (i) SCA by se mohlo zaměřit primárně na použití behaviorální biometrie a podobných technologií jako jediného prvku ověření, který by však v sobě musel mít povinně zabudovaný mechanismus automatického spuštění dodatečného ověření na základě některého z dalších (stávajících) prvků, pokud by skóre shody stávajícího a předchozího chování uživatele nedosahovalo požadovaných hodnot (hranice by v takovém případě musela být nastaveno velmi vysoko, ideálně někde v rozmezí 95–99 %);

    (ii) druhým řešením by mohlo být zavedení behaviorální biometrie jako povinného prvku SCA s možností poskytovatele platební služby si druhý prvek zvolit ze zbývajících kategorií dobrovolně;

    (iii) dalším řešením by mohla být povinnost zavést behaviorální biometrii mimo SCA, přičemž by sloužila pouze jako podpora a doplnění prvků stávajících (nebyla by tak akceptována jako prvek inherence), toto řešení by bylo pravděpodobně nejbezpečnější, ale zároveň by bylo velmi nákladné a současně by nevedlo ke snížení požadavků kladených

na poskytovatele a nemělo by ani pozitivní vliv na samotný uživatelský zážitek; nebo

(iv) si lze alternativně představit situaci, kdy povinnost uplatnit SCA bude možná jedním ze dvou způsobů – poskytovatel provede ověření uživatele na základě dynamického způsobu ověření jako jediného požadovaného prvku, nebo na základě použití stávajících statických prvků, kdy bude možné si zvolit kombinaci dvou ze tří prvků, tak jako je tomu nyní.

Jako praktický příklad účinnosti této technologie lze uvést australskou banku, která implementovala řešení společnosti BioCatch spočívající v použití behaviorální biometrie s cílem zlepšit profilování rizika a snížení frikce uživatelského zážitku v online prostředí. Výsledkem bylo údajně více jak 90 % rozpoznání podvodných jednání před samotným provedením platební transakce, identifikace více než 2.000 podvodných účtů a snížení případů krádeže identity taktéž o více než 90 %. Z pohledu ekonomického dopadu bylo kvantifikováno, že výstrahy generované z modelů detekce podvodů společnosti BioCatch pomohly zabránit ztrátě ve výši 970 tisíc australských dolarů během jediného týdne.[210] V jiném případě naopak jedna z největších britských bank ušetřila během sledovaného čtyřměsíčního období díky aplikaci technologie založené na behaviorální biometrii ve vztahu k hlasovým podvodům v průměru okolo 250 až 500 tisíc liber za každý měsíc jejího používání.[211]

Domnívám se, že potenciál této technologie je velmi slibný a dle mého názoru by tento potenciál měl být bedlivě sledován regulátory. Pokud by tato technologie svůj potenciál naplnila a z pohledu přesnosti, účinnosti a bezpečnosti by vysoce převyšovala ostatní prvky, tak si lze představit zavedení povinnosti její aplikace pro určité typy platebních služeb za současného zrušení povinnosti aplikovat SCA. Jelikož však deregulace

[210] BioCatch. Large Australian Financial Services Organization Disrupts Mule Operations and Stops Over 90% of Fraudulent Payments Using Behavioral Biometrics & Device Intelligence. *BioCatch.com* [online]. 2022 [cit. 02. 11. 2022]. Dostupné z: https://www.biocatch.com/hubfs/Case_Studies/CS-AUBank-Stops-ATO-Mules.pdf

[211] BioCatch. Top 5 UK Bank Saves £500K per Month in Fraud Losses by Preventing Social Engineering Voice Scams Using Behavioral Insights. *BioCatch.com* [online]. 2022 [cit. 02. 11. 2022]. Dostupné z: https://www.biocatch.com/hubfs/New%20Boilerplate/BC%20CS%20APP%20Fraud%20V2%20NBP.pdf

není způsob, kterým by se jednotlivé členské státy a EU jako celek v posledních letech ubírala, tak toto řešení v rozsahu zrušení povinnosti aplikovat SCA považuji za málo pravděpodobné a jako realističtější vidím některý z navrhovaných směrů vývoje výše. V každém případě lze shrnout, že by tato technologie mohla být v budoucnu přínosná jak pro poskytovatele platebních služeb, tak pro jejich uživatele.

5.2. SCA mimo území EHP

V rámci posouzení účelnosti zavedení regulace SCA na území EU považuji za vhodné analyzovat, jestli existují některé jiné země mimo členských zemí EU a zemí EHP, které zavedly povinnost vyžadovat SCA nebo jinou obdobu dvoufázového ověření, anebo jestli je v tomto ohledu EU průkopníkem a je při nastavování regulatorního rámce pro finanční instituce působící na unijním trhu v tomto ohledu důslednější. Níže tak uvádím příklady několika zemí a srovnávám jejich vztah k vyžadování dvoufázového ověření v rámci elektronického platebního styku.

(i) **Austrálie** – v roce 2016 tato země zvažovala zavedení jisté obdoby SCA, a to ve formě zavedení povinnosti používat při ověřování totožnosti osob nejčastěji používaný protokol 3D Secure, nicméně australská komise pro hospodářskou soutěž a spotřebitele (*The Australian Competition and Consumer Commission*) se proti tomuto návrhu ostře postavila a doporučila jeho nepřijetí, a to především z důvodů údajného rizika omezení volné soutěže na australském trhu a vysokých nákladů, které by zavedení takové regulace provázelo. Dále se objevila řada stížností zmiňujících, že by zavedení této povinnosti narušilo spotřebitelský zážitek, a proto by obchodníci mohli přicházet o prodeje. Nad rámec těchto důvodů k tomuto návrhu australská komise uvedla, že by sice regulace tohoto typu mohla mít pozitivní přínos například ve formě snížení množství podvodů, ale že míra takového přínosu je nejistá. Prozatím tak obdobná regulace na území Austrálie neplatí.[212]

[212] Australian Competition and Consumer Commission. ACCC proposes to deny authorisation to APCA for 3D Secure arrangements. *Accc.gov.au* [online]. 2016 [cit. 4. 12. 2022]. Dostupné z: https://www.accc.gov.au/media-release/accc-proposes-to-deny-authorisation-to-apca-for-3d-secure-arrangements

(ii) **Indie** – regulace s podobnými znaky SCA byla zavedena v Indii, která již po několik let od regulovaných subjektů na finančních trzích vyžaduje v případě elektronických plateb a souvisejících převodů peněžních prostředků více faktorové ověření a tuto regulaci průběžně přizpůsobuje vývojům na trhu. Například v roce 2016 zavedla tzv. opt-in režim (uživatel má sám možnost zvolit si aplikaci výjimky) u plateb nižších než 2000 indických rupií. Povinnost vyžadovat více faktorové ověření se bude od 1. dubna 2023 nově aplikovat taktéž na společnosti, jejichž předmětem je správa majetkových aktiv, a bude spočívat v povinnosti vyžadovat dvoufázové ověření u elektronických transakcí spočívajících v úpisu a zpětnému odkupu aktiv.[213]

(iii) **Japonsko** – i přes velikost ekonomiky této země zde místní regulátor povinnost dvoufázového ověření nevyžaduje a jakákoli aplikace je pouze na dobrovolné bázi.

(iv) **Kanada** – povinnost vyžadovat dvoufázové ověření neplatí taktéž v této severoamerické zemi. Některé velké místní banky nicméně začaly v posledních letech zavádět dvoufázové ověření dobrovolně.[214] Kanadský úřad pověřence pro ochranu osobních údajů, který je místní obdobou českého Úřadu

[213] Reserve Bank of India. Master Direction on Digital Payment Security Controls. *Rbi.org.in* [online]. 2021 [cit. 4. 12. 2022]. Dostupné z: https://www.rbi.org.in/scripts/FS_Notification.aspx?Id=12032&fn=2&Mode=0#MD;
Mint. RBI eases two-factor authentication for online card transactions up to Rs2,000. *Livemint.com in* [online]. 2016 [cit. 4. 12. 2022]. Dostupné z: https://www.livemint.com/Industry/bJmdHvAuLVC5af1O0NCE0O/RBI-eases-rules-for-online-card-payments-up-to-Rs2000.html; a
The Economic Times. Sebi extends two-factor authentication for mutual fund subscription transactions. *Economictimes.indiatimes.com* [online]. 2022 [cit. 4. 12. 2022]. Dostupné z: https://economictimes.indiatimes.com/markets/stocks/news/sebi-extends-two-factor-authentication-for-mutual-fund-subscription-transactions/articleshow/94566748.cms?from=mdr

[214] Swift SMS Gateway. Canadian Banking Moves Toward Two-Factor Authentication (2FA). Swiftsmsgateway.com [online]. 2021 [cit. 4. 12. 2022]. Dostupné z: https://www.swiftsmsgateway.com/2021/07/27/canadian-banking-moves-toward-two-factor-authentication-2fa/

pro ochranu osobních údajů, povinnost vyžadovat dvoufázové ověření všem subjektům (čili nejen finančním) alespoň doporučuje.[215]

(v) **Spojené království Velké Británie a Severního Irska –** tato země s velmi rozvinutým finančním systémem se po vystoupení z EU rozhodla jít v této oblasti regulace stejným směrem jako EU a přijata víceméně shodnou úpravu SCA, jako platí na území EU. Tato začala platit od března roku 2022, kdy dotčeným subjektům stanovuje povinnost vyžadovat použití alespoň dvou prvků z kategorií *znalost*, *vlastnictví* a *inherence* pro online přístup k platebnímu účtu, iniciaci platební transakce a jiné úkony učiněné prostřednictvím vzdáleného přístupu, u nichž existuje riziko podvodného jednání. Pozitivně lze vnímat lokální postoj k behaviorální biometrii, kterou při aplikaci řešení v rámci SCA jednotlivým poskytovatelům obecně doporučuje například UK Finance, obchodní sdružení pro sektor bankovnictví a finančních služeb ve Spojeném království reprezentující zájmy více než 300 britských společností.[216]

(vi) **Spojené státy americké** – dvoufázové ověření není povinné ani ve Spojených státech amerických, které jsou v oblasti financí hlavním světovým hráčem. Je zde nicméně patrná snaha v některých oblastech ekonomiky povinnost více faktorového ověření vyžadovat či alespoň doporučovat. Úřad pro finanční ochranu spotřebitelů (*Consumer Financial Protection Bureau*) v srpnu 2022 americkým bankám doporučil vyžadovat více faktorové ověření z důvodu ochrany dat spotřebitelů. Nesplnění této povinnost by mohlo dle tohoto úřadu ohrozit bezpečnost spotřebitelských dat a vést k případné odpovědnosti

[215] Office of Privacy Commissioner of Canada. Guidelines for identification and authentication. *Priv.gc.ca* [online]. 2016 [cit. 4. 12. 2022]. Dostupné z: https://www.priv.gc.ca/en/privacy-topics/identities/identification-and-authentication/auth_061013/

[216] UK Finance Limited. Strong customer authentication – frequently asked questions. *Ukfinance.org.uk* [online]. 2022 [cit. 5. 12. 2022]. Dostupné z: https://www.ukfinance.org.uk/our-expertise/payments/strong-customer-authentication/strong-customer-authentication-frequently-asked-questions

dle místního zákona zaměřeného na finanční ochranu spotřebitelů.[217] Dále ze uvést prezidentský dekret z roku 2021 stanovující základní standardy v oblasti kyberbezpečnosti vyžadující více faktorové ověření pro americké organizace a dodatele softwaru pro místní vládu.[218] I když není povinnost vyžadovat dvoufázové ověření v elektronickém styku prozatím povinná, lze alespoň pozorovat trend směřující k jeho dobrovolné aplikaci. Prozatím však není jasné, zdali bude tento požadavek stanoven v budoucnu povinně či nikoliv.

(vii) **Turecko** – tato jihoevropská země se rozhodla jít v tomto směru obdobnou cestou jako EU, kdy dne 15. března 2020 zveřejnila turecká agentura pro bankovní regulaci a dohled nařízení o informačních systémech bank a službách elektronického bankovnictví (číslo: 31069), které vstoupilo v platnost a účinnost dne 1. července 2020. Podle článku 34 tohoto nařízení mají banky při poskytování služeb elektronického bankovnictví, včetně transakcí, které nemají finanční důsledky (jako např. zobrazení informací o klientovi), autentizační mechanismus sestávající se z nejméně dvou nezávislých složek a autentizačních údajů. Tyto složky mají být tvořeny dvěma prvky zákazníka z kategorií *zná*, *vlastní* nebo *má biometrickou charakteristiku*. Turecká právní

[217] Consumer Financial Protection Bureau. CFPB Takes Action to Protect the Public from Shoddy Data Security Practises. *Consumerfinance.gov* [online]. 2022 [cit. 5. 12. 2022]. Dostupné z: https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-to-protect-the-public-from-shoddy-data-security-practices/; a
Consumer Financial Protection Bureau. Consumer Financial Protection Circular 2022-04. *Consumerfinance.gov* [online]. 2022 [cit. 5. 12. 2022]. Dostupné z: https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/

[218] The Wall Street Journal. President Biden Signs Cybersecurity Executive Order to Boost Federal Defenses Against Hacks. *Wsj.com* [online]. 2021 [cit. 5.12.2022]. Dostupné z: https://www.wsj.com/articles/president-biden-signs-cybersecurity-executive-order-to-boost-federal-defenses-against-hacks-11620859243?mod=article_inline

úprava také obdobně jako úprava v EU klade důraz zejména na bezpečnost v elektronickém platebním styku a ochranu citlivých údajů uživatelů.[219]

Na výše uvedených příkladech jsem se snažil demonstrovat, že regulatorní snaha EU o zajištění zvýšené bezpečnosti v oblasti elektronického platebního styku prostřednictvím zavedení důslednějších požadavků na ověření totožnosti osob při konkrétních úkonech není ve světě ojedinělá. Jistou obdobu úpravy SCA můžeme pozorovat například ve Spojeném království, Indii nebo Turecku. EU tak není jediná, která sleduje trendy v oblasti platebního styku a snaží se nespoléhat pouze na samotné tržní prostředí, ale aktivně nastavuje pravidla pro zvýšení ochrany spotřebitelů a jejich finančních prostředků. Pohledem spotřebitele lze tuto snahu vnímat převážně pozitivně, a to i přesto, že může být požadavek na časté a opakované ověřování totožnosti považován za rušivý během spotřebitelského zážitku při online nakupování, přístupu k platebnímu účtu nebo při využívání jiných služeb, za které uživatelé elektronicky platí. V obecné rovině tak můžeme snahu o regulaci v této oblasti ze strany EU i jiných států vzhledem k důvodům jejího zavedení požadovat z tohoto konkrétního pohledu za účelnou.

Na druhou stranu existuje řada ekonomicky i finančně vyspělých států, které potřebu zavádět regulaci dvoufázového ověřování v elektronickém platebním styku prozatím nesdílí. Mezi takové se řadí Austrálie, Japonsko, Kanada nebo Spojené státy americké, které se všechny podle měřítka velikosti celkového HDP řadí mezi patnáct největších ekonomik na světě.[220] Nabízí se tak otázka, jestli je vzhledem k poměrně významné nákladovosti nezbytné zavádět požadavek dvoufázového ověření jako povinnost. Jelikož případné ztráty a jiné negativní dopady způsobené podvody budou v konečném důsledku dopadat především na samotné poskytovatele finančních služeb, je poměrně pochopitelné, že se tyto státy prozatím spoléhají na tržní prostředí a inovace, prostřednictvím kterých

[219] OneSpan Inc. The financial regulatory landscape in Turkey is modernising quickly. *Onespan.com* [online]. 2020 [cit. 4. 12. 2022]. Dostupné z: https://www.onespan.com/topics/two-factor-authentication?ad=blog-text; a
T.C. Cumhurbaşkanlığı Külliyesi (T.C. Resmi Gazete). *Resmigazete.gov.tr* [online]. 2020 [cit. 4. 12. 2022]. Dostupné z: https://www.resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm

[220] The World Bank. GDP (current US$). *Data.worldbank.org* [online]. 2022 [cit. 5. 12. 2022]. Dostupné z: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?most_recent_value_desc=true

klíčoví hráči jako Visa či MasterCard zavádějí praxí široce přijímané standardy bezpečnosti při placení.

Argumentem ve prospěch tržního prostředí může být také motivace poskytovatelů platebních služeb. Ve zdravém konkurenčním prostředí jsou totiž jednotliví soutěžitelé (poskytovatelé platebních služeb) na trhu platebního styku automaticky motivováni snahou zajistit pro své klienty maximální kvalitu služeb, do které bezpochyby spadá i míra zabezpečení jejich dat a finančních prostředků. Pokud by totiž došlo k prolomení jejich bezpečnostních opatření, klienti by přišli o svá data nebo peníze a daná země by současně v těchto situacích neměla nastavena pravidla pro částečnou či úplnou náhradu takto ukradených peněžních prostředků, tak by negativní dopad na reputaci dotčeného poskytovatele mohl takového poskytovatele do budoucna připravit o část jeho byznysu z důvodu přechodu stávajících i potenciálních zákazníků ke konkurenční společnosti.

Bez ohledu na výše uvedené můžeme v online prostředí pozorovat jasný trend spočívající v nastavení vyšších bezpečnostních standardů, a to i mimo oblast placení. Dnes je již poměrně běžné, že v rámci přístupů k e-mailovým schránkám, online účtům u jednotlivých obchodníků nebo poskytovatelů služeb nebo při používání jednotlivých aplikací v chytrých telefonech je po uživatelích vyžadováno (nebo je jim to alespoň umožněno) nastavení dvoufázového ověření. Pokud bychom se v budoucnu dostali do situace, kdy pro převážnou většinu uživatelů bude tato praxe naprosto běžná a nebudou se nad ní s udivením pozastavovat a považovat ji za překvapující či omezující, nemělo by v takové situaci být problematické dvoufázové ověření vyžadovat povinně i po poskytovatelích platebních služeb. Při rozhodování, jestli prostřednictvím právní regulace tuto povinnost zavést a jakým způsobem to učinit, půjde v konečném důsledku vždy o to, jestli míra podvodů, nedostatečná míra zabezpečení a rizika z nich plynoucí a s nimi související převáží nad potenciálními přínosy takto nově zavedené regulace.

5.3. Úskalí právní úpravy SCA

V této kapitole se zaměřím na zhodnocení několika oblastí, které považuji z hlediska právní úpravy SCA za problematické. Jak již bylo zmíněno v předchozích kapitolách, tak od doby schválení a účinnosti Směrnice PSD2 vydala EBA řadu stanovisek, kterými adresovala různé problematické aspekty navržené právní úpravy SCA v rámci Směrnice PSD2 a Nařízení RTS, a zároveň obdržela velké množství dotazů v rámci Q&A procesu

k těmto právním předpisům. Z těchto skutečností lze dovozovat, že právní úprava SCA a její výklad je místy nejednoznačný, a proto by v některých aspektech měla být právní úprava zpřesněna či upravena. V následujících podkapitolách se budu některým z nich postupně věnovat.

5.3.1. Odpovědnost a sankce

První oblastí, která je dle mého názoru problematickou, je stávající nastavení odpovědnosti a případných sankcí za nedodržení povinnosti osoby oprávněné poskytovat platební služby vyžadovat od uživatelů SCA. Jak již bylo uvedeno v kapitole 3 (Silné ověření klienta), jedinou formou sankce za nedodržení povinnosti vyžadovat SCA ve stanovených případech je odpovědnost osoby oprávněné poskytovat platební služby za ztrátu z neautorizované platební transakce dle § 182 ZPS, která se neuplatní pouze v případech, kdy plátce jednal podvodně. Takto nastavený sankční způsob se mi jeví jako problematický především ze dvou důvodů.

Prvním z těchto důvodů je skutečnost, že v některých případech si neautorizovanou platební transakci, a tedy související odpovědnost za porušení povinnosti ve vztahu k SCA, lze obtížně představit. Jako příklad můžeme uvést situaci, kdy platební službou bude poskytnutí služby informování o platebním účtu, při které dochází pouze ke sdělování informací o platebním účtu a typicky nebude možné v daném prostředí provádět platební transakce. Ve chvíli, kdy by poskytovatel takové služby nevyžadoval SCA, tak je fakticky vyloučena možnost jej za tuto skutečnost penalizovat.

Druhý důvod je spíše koncepční. Ve chvíli, kdy se členské státy EU rozhodly zavést takto významnou regulaci, která byla velmi složitá a nákladná na implementaci (tomuto tématu se budu ještě blíže věnovat v kapitole 5.4 (*Analýza dopadů zavedení SCA, zhodnocení regulace*), tak považuji za nedostatečné nástroje, kterými by mohl na poskytovatele platebních služeb příslušný regulátor dohlížet a vynucovat dodržování úpravy. Pokud totiž bylo záměrem spolehnout se pouze na odpovědnost z neautorizované platební transakce, nabízí se logicky otázka, jestli je celá úprava SCA vlastně nezbytná, protože i bez ní by poskytovatel nesl riziko za neautorizované transakce a byl by ekonomicky i konkurenčním tržním prostředním motivován dobrovolně implementovat dodatečná bezpečnostní opatření, díky kterým by takovým situacím předcházel a mitigoval své případné ztráty a ohrožení své reputace. Pokud tedy akceptujeme názor, že je třeba zajistit zvýšenou ochranu uživatelů

v elektronickém platebním styku a snažit se omezit prostřednictvím nastavení dodatečných regulatorních pravidel rizika podvodů, neměla by právní úprava zůstat ve formě specifických povinností bez zajištění účinné možnosti vynutit si jejich dodržování a vymáhat sankce za případy jejich porušení.

Příprava a vyjednávání právní úpravy na úrovni členských států EU je vždy především politická, a proto nemusí být nezbytně populární nastavovat robustní sankční mechanismy, které budou v praxi pro jednotlivé členské země znamenat dodatečnou práci (a tedy i dodatečné náklady) pro jejich státní aparát, který by na dodržování této úpravy musel dohlížet a byl povinen jakékoliv případné sankce vymáhat. Tento mechanismus by nicméně nebyl ojedinělý, protože již na unijní úrovni funguje například v oblasti hospodářské soutěže nebo ochrany osobních údajů. Na druhou stranu je třeba říci, že případné porušení poskytovat SCA nebude v převážné většině případů dosahovat intenzity a závažnosti, které by dosahovalo porušení regulatorních povinností v těchto dvou oblastech. Jako logické se v takovém případě jeví ponechání sankční úpravy na jednotlivých členských zemích a k tomuto závěru se i kloním. To však neznamená, že by Směrnice PSD2 či Nařízení RTS nemohly alespoň v části jejich odůvodnění i tak obsahovat ve vztahu k sankcím nějaký základní rámec nebo konkrétní doporučení.

Na základě výše uvedeného se domnívám, že by česká právní úprava v ZPS měla obsahovat alespoň základní úpravu přestupků ve vztahu k SCA. ZPS dnes již v § 233 obsahuje přestupky osob oprávněných poskytovat platební služby v oblasti bezpečnosti spočívající v nesplnění oznamovací povinnosti ohledně hlášení bezpečnostních a provozních incidentů nebo v porušení informační povinnosti hlásit bezpečnostní a provozní rizika a podvodná jednání. Za oba tyto přestupky může ČNB udělit pokutu až do výše 1.000.000 Kč. Úprava ve vztahu k SCA by mohla být rozšířena například o povinnost osoby oprávněné poskytovat platební služby poskytnout ČNB na základě její žádosti ve stanovené lhůtě informace o nastavených mechanismech SCA a o aktuálně požadovaných výjimkách. V případě porušení této povinnosti by se dotčená osoba oprávněná poskytovat platební služby mohla dopustit obdobného přestupku jako ve dvou výše zmíněných případech a mohla by v takovém případě být sankcionována obdobně. Tato povinnost by navazovala na a doplňovala články 2 a 3 Nařízení RTS, podle kterých musí poskytovatelé platebních služeb zavést mechanismy sledování transakcí, vést o nich potřebnou dokumentaci, vyhodnocovat je a na žádost příslušných orgánů jim poskytovat zprávy

o auditu, během kterého je předkládáno hodnocení a zpráva o souladu bezpečnostních opatření s právní úpravou.

Dále by bylo vhodné zavést v souvislosti se SCA dva další přestupky. První za porušení povinnosti vyžadovat SCA v případech stanovených právní úpravou a druhý za porušení povinností v souvislosti s použitím výjimek z povinnosti vyžadovat SCA dle Nařízení RTS (bylo by samozřejmě možné tyto spojit a uvést jako dvě alternativní situace v rámci jednoho přestupku). Tyto přestupky by opět měly platit pouze pro osoby oprávněné poskytovat platební služby a systematicky by tak bylo vhodné je podřadit pod výše zmíněný § 233 ZPS. Sankce by však v tomto případě měla být dle mého názoru vyšší, a to vzhledem k jiným maximálním hranicím stanoveným pro některé další přestupky v rámci ZPS. Např. vydavatel elektronických peněz malého rozsahu může být v případě přestupku spočívajícím v neuplatnění systému řízení bezpečnostních a provozních rizik dle § 100 odst. 1 písm. d) ZPS sankcionován až do výše 5.000.000 Kč.[221] Správce informací o platebním účtu může být za přestupek spočívající v neuplatňování řídícího a kontrolního systému v souladu s § 48 ZPS sankcionován do výše 10.000.000 Kč.[222] Dále lze uvést přestupky poskytovatele služby dynamické směny měn, který může být za přestupky spočívající v neuplatňování systému vyřizování stížností a reklamací uživatelů, nesplnění informační povinnosti či neoznámení změny údajů sankcionován do výše 5.000.000 Kč.[223] Jako rozumná by se mi v kontextu výše uvedených a dalších přestupků stanovených v ZPS jevila hranice v rozmezí 5-10 milionů Kč, stanovená dle míry a intenzity konkrétního porušení. Projednávání takových přestupků by mělo spadat pod ČNB, a to v souladu s § 236 odst. 1 písm. b) ZPS.

Zavedením výše uvedených přestupků by byl dle mého názoru ČNB dán vhodný nástroj, kterým by mohla efektivněji dohlížet a kontrolovat činnost osob oprávněných poskytovat platební služby a díky kterému by měla možnost lépe zajišťovat ochranu a bezpečnost uživatelů ve vztahu k SCA. Vůči poskytovatelům by tato regulatorní změna neměla nic podstatného měnit, protože pokud své povinnosti již nyní řádně plní, tak by se jich tato změna v praxi nijak významně nedotkla. Bylo by však nutné počítat s dodatečnými

[221] § 228 odst. 4 písm. b) ZPS

[222] § 227 odst. 2 písm. b) ZPS

[223] § 233a odst. 2 písm. b) ZPS

náklady na straně ČNB, které by však neměly být významné a měly být vyváženy právě možností tento nástroj vůči poskytovatelům používat a lépe tak dohlížet na soulad jejich činnosti s právní úpravou.

5.3.2. Obecnost úpravy

Další oblastí, kterou považuji za problematickou, je celková obecnost úpravy. Nastavením maximálně neutrálního textu se zákonodárce snažil naplnit požadavek na technologickou neutralitu, nicméně v řadě případů je výklad tohoto textu problematický. Díky této obecnosti EBA čelila velkému množství dotazů vztahujícím se k SCA a současně byla nucena vydat řadu stanovisek, aby postavila na jisto některé problematické otázky. Převážnou část záležitostí se díky odpovědím a stanoviskům EBA sice podařilo úspěšně vyjasnit, nicméně problematická je především skutečnost, že odpovědi a stanoviska EBA nejsou právně závazná. V této souvislosti lze zmínit poměrně nedávný rozsudek SDEU[224], ve kterém SDEU uvedl, že obecné pokyny EBA nejsou právně závazné a příslušné orgány musí oznámit EBA, zda se jimi řídí nebo se jimi řídit hodlají, případně uvést důvody, proč tak nečiní nebo činit nehodlají. Obecné pokyny EBA zároveň nelze považovat za předpis, který má závazné právní účinky vůči finančním institucím, nicméně tyto musí vynaložit veškeré úsilí, aby se jimi řídily, a pokud tak nečiní, tak musí dané sdělit konkrétní důvody. Jelikož se ve vztahu k SCA nejednalo ani o formu obecných pokynů, je výše nastíněný problém o to závažnější.

Dále vnímám jako problematické, že poskytovatelům ve vztahu k SCA nestačí seznámit se pouze se samotným textem právní úpravy, ale musí poměrně složitě dohledávat a procházet na webu EBA všechna související stanoviska a nižší stovky otázek a zkoumat, jestli se v nich neobjevuje nějaká pro ně relevantní informace. Z tohoto důvodu považuji úpravu v některých částech za poměrně nepřehlednou, což může poskytovatelům a dalším dotčeným subjektům způsobovat značné náklady v oblasti compliance. Nepřímým důsledkem této situace může být vytvoření dodatečné bariéry pro vstup na tento trh, protože náklady na právní zastoupení mohou být vzhledem ke komplexnosti této problematiky poměrně značné. V opačném případě budou poskytovatelé preventivně raději volit situaci,

[224] Rozsudek SDEU ze dne 15. 7. 2021, Fédération bancaire française (FBF) v. Autorité de contrôle prudentiel et de résolution (ACPR), C-911/19, ECLI:EU:C:2021:599, body 41-49. Dostupné z: https://curia.europa.eu/juris/liste.jsf?language=cs&num=C-911/19

kdy budou nadměrně vyžadovat SCA ve všech situacích, kdy si jeho aplikací nebudou absolutně jistí, což jednak nejspíš nebylo záměrem zákonodárce a jednak bude tento přístup způsobovat díky zvýšené frikci horší uživatelský zážitek, a může tak v důsledku vést k nižším tržbám jednotlivých subjektů.

V kontextu výše uvedeného by tak dávalo smysl zavést či zpřesnit některé definice a pojmy používané ve Směrnici PSD2 či Nařízení RTS a současně některé závěry EBA přenést alespoň do části odůvodnění těchto předpisů, aby došlo k celkovému zpřehlednění právní úpravy.

Jako příklad lze uvést absenci definice elektronické platební transakce, kterou jsem se zabýval v podkapitole 4.1.2 (*Elektronická platební transakce*) a se kterou se v rámci úpravy SCA opakovaně pracuje a nebyla ve Směrnici PSD2 definována. Dále by měla být vyjasněna role behaviorální biometrie jako prvku inherence, ke které jsem se již blíže vyjadřoval v kapitole 5.1 (*Behaviorální biometrie*). Jako další příklad lze uvést definici platební transakce na dálku, která je nyní definována jako „*platební transakce iniciovaná po internetu nebo prostřednictvím zařízení, které lze použít k dálkové komunikaci*“[225] a je použita ve Směrnici PSD2 v rámci jednoho z případu použití SCA (zde podotýkám, že tato textace nebyla převzata do českého zákona). Problematická je tato definice například ve vztahu k mobilním telefonům, kdy v rámci Q&A 4788[226] EBA uvedla, že transakce, ke kterým je dán platební příkaz prostřednictvím telefonického příkazu, nespadají do působnosti SCA, což jde proti výslovnému znění této definice.

5.3.3. Jednotlivé prvky SCA

Dalším aspektem, nad kterým by stálo za to se v budoucnu při přípravě novelizace právní úpravy zamýšlet, je požadavek na vyžadování dvou prvků SCA ze dvou různých kategorií. Například prvek z kategorie znalost může být v některých případech poměrně snadno prolomitelný a o jeho bezpečnosti lze polemizovat. Tento názor lze ilustrovat

[225] Článek 4 odst. 6 Směrnice PSD2

[226] European Banking Authority. Single Rulebook Q&A. Treatment of electronic bookings similar to Mail Order and Telephone Orders (MO-TO) transactions. *Eba.europa.eu* [online]. 2019 [cit. 29. 10. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4788

na výsledcích řady anket, dotazníků a studií ohledně používání hesel a nákladní s nimi. Zjištěno bylo například následující:[227]

- 43 % lidí uvedlo, že sdílelo svá hesla s jinou osobou (typicky svým partnerem);
- bylo zjištěno, že 59 % používá snadno zjistitelné osobní údaje ve svých heslech (jako např. datum narození);
- 20 % lidí uvedlo, že někdy sdílelo heslo ke svému e-mailovému účtu s jinou osobou;
- až 45 % uvedlo, že by v případě zneužití jejich údajů změnilo své heslo, a to navzdory skutečnosti, že 40 % připustilo, že jejich údaje již byly historicky odhaleny a 47 % uvedlo, že díky tomu přišlo o peníze; nebo
- bylo zjištěno, že více než 40 milionů uživatelů služeb Microsoftu opakovaně používalo stejná hesla pro více svých účtů.

Poskytovatelé určitě mohou uživatelům dávat v tomto ohledu řadu doporučení, nicméně pravděpodobně nelze očekávat, že se jimi automaticky budou všichni řídit. Řada uživatelů bude například používat zašifrované správce hesel, nicméně v případě jejich prolomení přijdou o všechna hesla najednou. Je proto na zvážení, jestli by ve chvíli, kdy dva prvky z kategorie inherence/biometrických údajů (například kombinace biometrie tělesné a biometrie chování) mohou dosahovat mnohem vyšší míry zabezpečení oproti například tradičnímu použití hesla a zařízení s vygenerováním jednorázového kódu, neměla regulace tyto skutečnosti reflektovat a měla umožnit použití inovativních řešení, která mohou být pro uživatele bezpečnější a budou od nich v menší míře vyžadovat dodržování doporučovaných zásad bezpečnosti. V tomto směru bych v budoucnu uvítal posílení role prvku inherence/biometrických údajů.

[227] Comparitech Limited. 25+ Password statistics (that may change your password habits). *Comparitech.com* [online]. 2022 [cit. 10. 12. 2022]. Dostupné z: https://www.comparitech.com/blog/information-security/password-statistics/

5.3.4. Biometrie a GDPR

Při každém zpracovávání biometrických údajů, jako jednoho ze tří prvků SCA, je třeba brát v potaz skutečnost, že zpracování těchto údajů za účelem jedinečné identifikace osoby spadá dle článku 9 Nařízení GDPR do kategorie tzv. zvláštní kategorie osobních údajů. Zpracování takových údajů je v obecné rovině zakázáno a povoleno je pouze ve výjimečných případech, z nichž pro účely SCA bude relevantní především výslovný souhlas uživatele s jejich zpracováním. Na toto ustanovení se nicméně nemohou poskytovatelé spoléhat bez dalšího, jak ukázalo nedávné rozhodnutí Úřadu pro ochranu osobních údajů[228], v němž se úřad zabýval situací, kdy banka zpracovávala při elektronickém uzavírání smluv o poskytování úvěru s klienty za účelem uzavření a uchování smluvní dokumentace též biometrický podpis klientů, který dle názoru úřadu nebyl nezbytný ani pro uzavření příslušné smlouvy, ani pro její plnění. Tuto praxi úřad vyhodnotil jako v rozporu se zásadou minimalizace údajů a bance uložil pokutu ve výši 250 tisíc korun. Pro poskytovatele platebních služeb ve vztahu k SCA dané rozhodnutí znamená, že by pravděpodobně neměli obligatorně vyžadovat použití prvku inherence bez možnosti nahradit jej jinou možností a při návrhu vhodných řešení by neměli brát úpravu ochrany osobních údajů na lehkou váhu.

Výše uvedené rozhodnutí demonstruje další poměrně významnou překážku při nastavování mechanismů SCA, protože v případě použití jednoho ze tří prvků musí poskytovatelé získávat výslovný souhlas všech dotčených uživatelů a nelze tak konkrétní řešení automaticky plošně aplikovat. Jak již bylo zmíněno výše, používání biometrických údajů se prozatím jeví jako bezpečnější oproti například standardnímu heslu, avšak významné omezení v nakládání s těmito údaji může do budoucna omezovat inovace, a to především v oblasti behaviorální biometrie. Zároveň není zcela jasné, kde leží hranice při zpracovávání údajů získávaných v rámci behaviorální biometrie v kontextu Nařízení GDPR, a zákonodárce či příslušný regulátor by měli v tomto směru pomoci poskytovatelům platebních služeb buď formou stanovení konkrétních pravidel pro jejich využití v rámci SCA nebo alespoň poskytnutím konkrétních výkladových pravidel. Individuálně totiž takové údaje

[228] Rozhodnutí Úřadu pro ochranu osobních údajů ze dne 21. 3. 2019, č. j. UOOU-10138/18-8. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=34470

citlivé být nemusí, nicméně dohromady mohou být schopny poměrně přesně určit totožnost určité osoby.

Bude samozřejmě záležet, jakým směrem se budou technologie vyvíjet, nicméně již nyní můžeme pozorovat v online prostředí tendenci k častějšímu využívání biometrických údajů v rámci bezpečnostních opatření. Poskytovatelé platebních služeb tak musejí velmi pečlivě vyvažovat požadavky obou těchto právních úprav. Znova se tak nabízí otázka, jestli zavedení právní úpravy SCA bylo i v tomto kontextu opravdu účelné, protože například subjekty působící na americkém trhu těmto omezením nečelí a jejich prostor pro vymýšlení inovativních řešení je významně větší a v jistém smyslu i levnější, což může mít negativní vliv na konkurenceschopnost evropských společností.

5.4. Analýza dopadů zavedení SCA, zhodnocení regulace

V poslední kapitole této práce se budu věnovat analýze dopadů zavedení SCA, zejména dopadu na obchodníky a posouzení, jestli nastavení pravidel SCA dosáhlo zamýšleného účelu snížení míry a objemu podvodů v elektronickém platebním styku. Současně se budu zabývat procesem implementace této regulace, který na trhu neprobíhal zrovna hladce. Závěrem poté zhodnotím právní úpravu SCA jako takovou.

5.4.1. Proces zavedení SCA a jeho implementace

Směrnici PSD2, která zavedla povinnost požadovat SCA, měly členské státy povinnost transponovat do své právní úpravy do 13. ledna 2018. Nařízení RTS, které bylo přijato dne 27. listopadu 2017, poté vstoupilo v účinnost od 14. září 2019. Implementace řešení podporujících SCA poskytovateli platebních služeb nicméně neprobíhala bez obtíží. Dne 19. září 2019, čili necelý týden po tom, co vstoupilo Nařízení RTS v účinnost, obdržela EBA dopis od Ecommerce Europe[229], asociace reprezentující více než 150 tisíc společností prodávajících zboží nebo poskytujících služby na území Evropy, ve kterém tato asociace požádala EBA o dodatečných 18 měsíců (36 měsíců v některých specifických případech) pro dokončení implementace řešení podporujících použití SCA. Jedním z důvodů

[229] Ecommerce Europe. Ecommerce Europe co-signs a Joint-Industry Letter on European SCA implementation. *Ecommerce-europe.eu* [online]. 2019 [cit. 10. 12. 2022]. Dostupné z: https://ecommerce-europe.eu/publication/ecommerce-europe-co-signs-a-joint-industry-letter-on-european-sca-implementation/

nepřipravenosti byla skutečnost, že EBA vydala své stanovisko k jednotlivým prvkům SCA, kterým se snažila vyjasnit některé problematické aspekty, až v červnu roku 2019, a jednotliví poskytovatelé platebních služeb tak nebyli včas připraveni.

V reakci na dopis Ecommerce Europe a další podněty vydala EBA v říjnu téhož roku stanovisko ohledně nejzazšího data pro migraci SCA ve vztahu ke karetním platbám v oblasti e-commerce.[230] V něm uvedla, že z odpovědí na její dotazníky vyplynulo, že poskytovatelé platebních služeb by měli být schopni zajistit implementaci SCA do konce první poloviny roku 2020 a že většina obchodníků bude potřebovat dodatečných 3 až 9 měsíců, aby implementovala do svých systémů řešení umožňující použití SCA. V důsledku této skutečnosti se EBA rozhodla odložit termín pro implementaci řešení podporujících SCA na 31. prosince 2020. Česká veřejnost byla o skutečnosti, že od 1. ledna 2021 by všichni poskytovatelé platebních služeb a další subjekty podílející se na zpracování platebních transakcí (vč. obchodníků a provozovatelů platebních bran), informována ČNB počátkem roku 2021 prostřednictvím sdělení na jejích webových stránkách.[231]

V polovině roku 2021 následně EBA vydala souhrnnou zprávu o údajích poskytnutých poskytovateli platebních služeb o jejich připravenosti aplikovat SCA pro karetní platební transakce v e-commerce.[232] Tato data ukázala, že převážné většině zúčastněných subjektů se podařilo implementovat řešení podporující SCA, kdy bylo zjištěno, že k dubnu 2021:

---

[230] European Banking Authority. Opinion of the European Banking Authority on the deadline for the migration to SCA for e-commerce card-based payment transactions. *Eba.europa.eu* [online]. 2019 [cit. 02. 11. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2622242/e8b3ec84-c1c6-4e9a-96ea-3575361dc230/Opinion%20on%20the%20deadline%20for%20the%20migration%20to%20SCA.pdf?retry=1

[231] Česká národní banka. Silné ověření uživatele u plateb kartou na internetu od 1. 1. 2021. *Cnb.cz* [online]. 2021 [cit. 10. 12. 2022]. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/vykon-dohledu/upozorneni-pro-verejnost/Silne-overeni-uzivatele-u-plateb-kartou-na-internetu-od-1.-1.-2021/

[232] European Banking Authority. EBA REPORT on the data provided by PSPs on their readiness to apply strong customer authentication for e-commerce card-based payment transactions. *Eba.europa.eu* [online]. 2021 [cit. 02. 11. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2021/1014781/Report%20on%20the%20data%20provided%20by%20PSPs%20on%20their%20readiness%20to%20apply%20SCA.pdf

- 99 % obchodníků v EU podporuje SCA;
- 94 % všech platebních karet v EU podporuje SCA;
- 82 % všech uživatelů platebních služeb je zapojeno do řešení SCA;
- 92 % žádostí o ověření pravosti karet v elektronickém obchodě, které nahlásili poskytovatelé tzv. acquiringu, splňuje požadavky SCA; a
- 89 % iniciovaných platebních transakcí založených na kartách v elektronickém obchodě nahlášených vydavateli je v souladu s požadavky SCA.

Výše uvedeným popisem procesu implementace řešení podporujících SCA jsem se snažil demonstrovat, že i přesto, že měli poskytovatelé téměř tři roky na přípravu a implementaci řešení podporujících SCA, se nepodařilo dosáhnout úplné připravenosti celého trhu, kdy ani přes prodloužení původních lhůt stále nebylo celkem 18 % uživatelů součástí některého z řešení podporujících SCA a 11 % iniciovaných elektronických platebních transakcí nebylo v souladu s těmito požadavky. Je tak zřejmé, že proces zavedení této úpravy byl velmi složitý a obnášel celou řadu nejasností a komplikací, kterým musely jednotlivé tržní subjekty čelit. Zavedením požadavku vyžadovat od uživatelů SCA tak zjevně došlo k významnému zásahu do každodenního fungování poskytovatelů platebních služeb a do podnikání subjektů podílejících se na zpracování platebních transakcí (především obchodníků), když ani za takto dlouhé období nebyla řada z nich schopna přizpůsobit svoji činnost této nové právní úpravě. Hodnoty pohybující se na úrovni přibližně 90 % sice vyvolávají dojem úspěšné implementace, nicméně tomu tak ve skutečnosti nebylo, jak bude blíže rozvedeno v následující podkapitole.

5.4.2. Dopady zavedení SCA

V předchozí podkapitole byla ilustrována složitost dlouhého procesu implementace řešení podporujících SCA. Důsledky tohoto procesu, kterým se budu věnovat na následujících řádcích, jsou relevantní především ve dvou oblastech, (i) v dopadu na podnikání poskytovatelů platebních služeb a dalších subjektů podílejících se na zpracování platebních transakcí (především obchodníků) a (ii) v dopadu na objemy a míru podvodů, kvůli kterým byla regulace zavedena.

Britská společnost CSMPI poskytující poradenské služby v oblasti plateb, financí a souvisejících podvodů od roku 2011 po dobu několika měsíců před a po termínu pro implementaci řešení podporujících SCA, který stanovila EBA (tj. 31. prosinci 2020), vydávala pravidelně měsíční reporty na téma dopadů zavedení SCA ve dvanácti zemích, a to především na základě testovacích dat od jejich klientů, mezi které údajně patří řada velkých hráčů v oblasti maloobchodů. V těchto reportech CSMPI jsou zajímavé především dvě metriky, a to **míra selhání** (anglicky: *failure rate*), znamenající součet míry opuštění a poklesu obchodů, a **množství ohrožených obchodů** (anglicky: *sales at risk*), znamenající hodnotu všech obchodů s platbami bez přítomnosti karty – CNP plateb, které nemusí proběhnout díky problémům se SCA.

Míra selhání se v letech před zavedením SCA u obchodů s CNP platbami pohybovala v jednotkách procent, přičemž v únoru 2021 byl průměr ve dvanácti sledovaných zemích vysokých 31 %, kdy některé ze zemí dosahovaly hodnot mnohem vyšších, a to například Itálie – 47 %, Španělsko – 37 %, Německo – 36 %. Švédsko, které ze sledovaných zemí dosahovalo nejlepších hodnot, se i tak pohybovalo na úrovni 17 %. Odhad CSMPI ve vztahu k celkovému objemu ohrožených ročních tržeb u obchodů s CNP platbami na území Evropy za rok 2021, u kterých hrozí, že nedojde z důvodu SCA zákazníky k jejich dokončení, byl v únoru 2021 stanoven na astronomických 96 miliard EUR. Za klíčový důvod výše uvedených problémů byla považována výkonnost technologie EMVCo 3D-Secure verze 2 (3DS2), autentizačního protokolu, který byl vybrán pro podporu téměř všech online karetních transakcí v Evropě (320,9 mld. EUR v roce 2019).[233]

K tomu dále CSMPI uvedlo, že mnoho bank vydávajících karty tento protokol zatím nepodporovalo, a i tam, kde vydavatelé 3DS2 podporovali, byla zákaznická zkušenost často špatná. Ze zdrojů CMSPI a údajů z testování prodejců také vyplynulo, že i úspěšné ověření mohlo trvat až 60 sekund a v některých případech i v průměru více než dvě minuty. Takové hodnoty dle CMSPI představují značné riziko pro prodeje a budou mít citelný dopad na maloobchodníky všech velikostí. Zároveň je pravděpodobné, že takto vysoká míra selhání

[233] CMSPI. SCA Report – Latest December Updates. *Cmspi.com* [online]. 2021 [cit. 11. 12. 2022]. Dostupné z: https://cmspi.com/eur/en/resources/content/sca-report-latest-december-updates/; a
CMSPI. Strong Customer Authentication (SCA) – Impact Assessment – February 2021. *Cmspi.com* [online]. 2021 [cit. 11. 12. 2022]. Dostupné z: https://cmspi.com/eur/en/resources/content/strong-customer-authentication-sca-impact-assessment-february-2021/

postihne nejvíce malé obchodníky, protože zákazníci si často spojují dlouhou dobu načítání u plateb a související chybovost právě s tímto obchodníkem. Pokud tedy menší obchodníci, kteří mají k dispozici méně zdrojů a jsou schopni vyčlenit menší množství zdrojů na informační technologie, nebudou schopni nabídnout zákazníkům bezproblémové odbavení jejích obchodů, pak tyto zákazníky pravděpodobně získají největší obchodníci v Evropě, kteří jsou schopni lépe optimalizovat vlastní náklady a budou schopni věnovat těmto řešením více péče i zdrojů.[234]

Mezi strukturální problémy, které byly po zavedení SCA na trhu registrovány asociací Ecommerce Europe, které způsobovaly zmatení na straně zákazníků a které vedly k nedokončení obchodů, patřily následující:[235]

- problémy s dostupností, použitelností nebo nesprávným výkladem dostupných výjimek – zejména těch, které jsou založeny na analýze transakčních rizik. Na řadě trhu byli obchodníci svědky toho, že vydavatelé zpochybňovali žádosti o výjimky a vynucovali si silné ověření zákazníka, i když nebylo vyžadováno;

- problémy se zpožděním mezi vydavatelovou stránkou pro ověření a potvrzovací stránkou obchodníka pro zákazníky;

- problémy s řádným zavedením řešení 3D Secure vydavateli karet; a

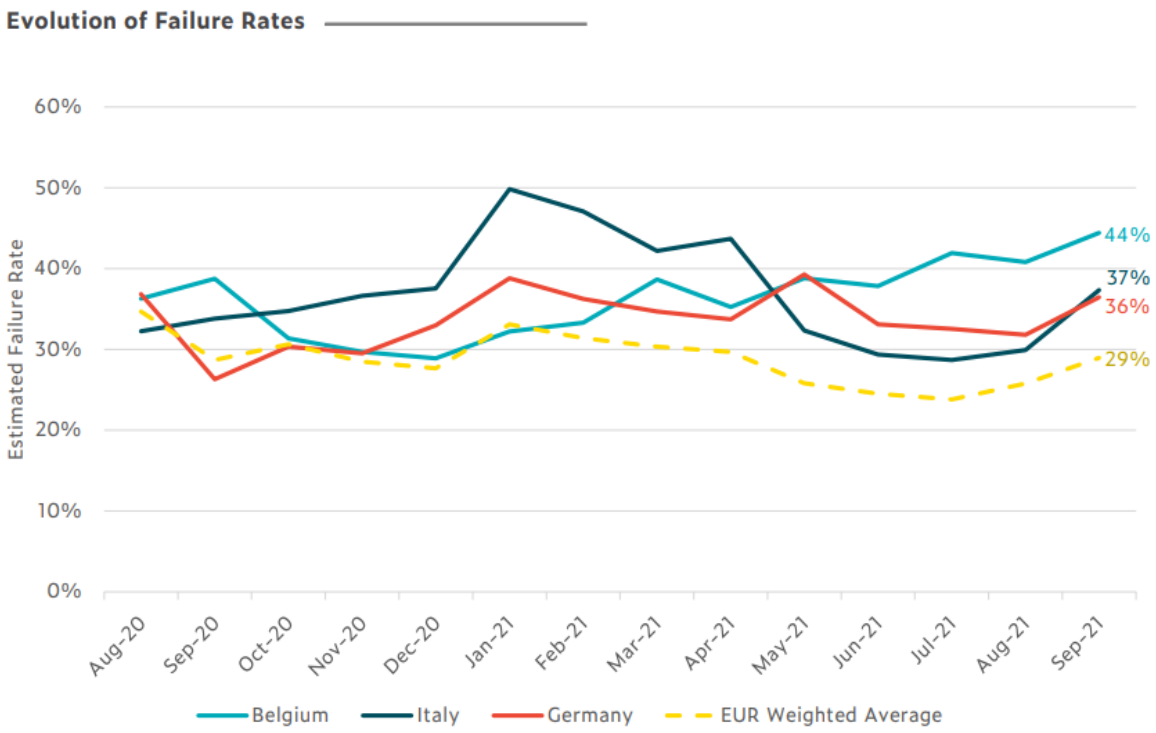
- problémy s poskytovateli serverů pro kontrolu přístupu (těmito jsou typicky vydavatelé karet, kteří je musí zavést, aby mohli dostávat zprávy v rámci řešení 3D Secure), kteří neřešili problémy vyvstávající z ověřovacích procesů.

Problémy s mírou opuštění obchodů z kraje roku 2021 zmiňovala také společnost Nethone, poskytující digitální řešení v oblasti e-commerce, podle které analytici odhadují

[234] Tamtéž

[235] Ecommerce Europe. Retail Joint Letter on measuring the impact of SCA April 2021. *Ecommerce-europe.eu* [online]. 2021 [cit. 11. 12. 2022]. Dostupné z: https://web.archive.org/web/20211026061453/https://www.eurocommerce.eu/media/196158/20210430%20Retail%20Joint%20Letter%20on%20measuring%20the%20impact%20of%20SCA%20April%202021%20-%20EBA.pdf

tuto míru v průměru na 20 % a v některých případech až 60 %.[236] Pro srovnání je vhodné uvést i poslední report společnosti CMSPI s daty za září 2021, dle kterého byla průměrná míra selhání ve sledovaných zemích stále na velmi vysokých 29 % (jednalo se o nárůst oproti 26 % ze srpna téhož roku). Odhadovaná hodnota ohrožených obchodů za rok 2021 s daty za prvních 9 měsíců tohoto roku činila stále astronomických 90 miliard EUR.[237] Níže uvedená tabulka CMSPI ilustruje vývoj míry selhání v období po nabytí účinnosti Nařízení RTS, kdy byla postupně zaváděna řešení podporující SCA.[238]



Obdobnou zkušenost se zavedením SCA jako v EU zaznamenali ve Spojeném království, kde byla obdobná právní úprava zavedena s účinností od března 2021. Přes 99 % obchodníků zaznamenalo zvýšení míry selhání obchodů o více než 5 % (průměr byl 37 %). Zároveň třetina dotázaných subjektů uvedla, že nová regulace má negativní dopad na zákaznickou zkušenost. Během prvního měsíce po zavedení SCA bylo ve Spojeném

[236] Nethone. PSD2 SCA exemptions: transaction risk analysis (TRA). *Nethone.com* [online]. 2021 [cit. 11. 12. 2022]. Dostupné z: https://nethone.com/post/psd2-sca-exemptions-transaction-risk-analysis-tra

[237] CMSPI. Strong Customer Authentication (SCA) – Impact Assessment – September 2021. *Cmspi.com* [online]. 2021 [cit. 11. 12. 2022]. Dostupné z: https://cmspi.com/eur/en/resources/content/strong-customer-authentication-sca-impact-assessment-september-2021/

[238] Tamtéž.

království odmítnuto celkem 664 tisíc elektronických platebních transakcí v celkové hodnotě 130 milionů liber, což denně činí cca 22 tisíc transakcí v celkové hodnotě 4,3 milionu liber.[239]

Dalším dopadem zavedení SCA, který negativně zasáhl obchodníky, bylo zavedení nových poplatků v souvislosti s implementací a používáním řešení podporujících SCA, které opětovně navýší jejich náklady. Tyto poplatky jsou obchodníkům účtovány za dodatečné ověření některých údajů v rámci platební transakce.[240]

V kapitole 3.1 (Bezpečnost a vývoj právní úpravy) jsem odkazoval na reporty ECB ohledně podvodů s platebními kartami. V rámci nich byly zkoumány především dvě metriky – celková hodnota všech CNP podvodů a podíl CNP plateb na celkovém objemu podvodů. Ve svém sedmém reportu z roku 2021 ECB uvedla, že v roce 2018 byla celková hodnota CNP podvodů ve výši 1,43 miliard EUR a tato v roce 2019 narostla na 1,5 miliardy EUR. Podíl CNP plateb na celkovém objemu činil v těchto letech 79 % a 80 %. Na níže uvedené tabulce je zároveň vidět, že podíl hodnoty podvodných transakcí na celkovém objemu měl v letech 2009-2019 mírně klesající tendenci, a to i přes zjevný nárůst celkové hodnoty těchto podvodů.[241]

[239] Nuapay. EML Open Banking Uncovers A 37% Increase In Payment Declines Following SCA Implementation. *Nuapay.com* [online]. 2022 [cit. 11. 12. 2022]. Dostupné z: https://www.nuapay.com/en/resources/in-the-news/eml-open-banking-uncovers-a-37-increase-in-payment-declines-following-sca-implementation/; a
Barclaycard. Retailers losing out on £4.3million in sales each day as new SCA rules block non-compliant online transactions. *Home.barclaycard* [online]. 2022 [cit. 11. 12. 2022]. Dostupné z: https://home.barclaycard/press-releases/2022/04/retailers-losing-out-on-4-3-million-in-sales-each-day/

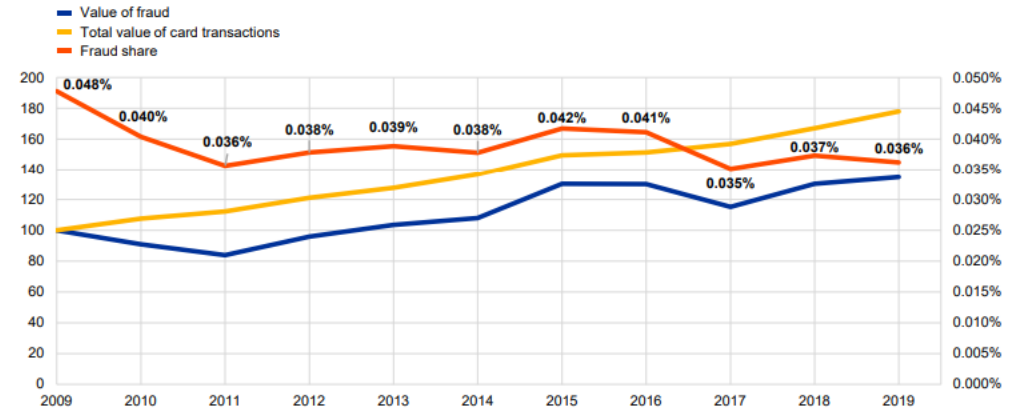
[240] CMSPI. The New Ecommerce Fees: Why European Merchants Need to Act. *Cmspi.com* [online]. 2022 [cit. 11. 12. 2022]. Dostupné z: https://cmspi.com/eur/en/resources/content/the-new-ecommerce-fees-why-european-merchants-need-to-act/

[241] EUROPEAN CENTRAL BANK. Seventh Report on Card Fraud. *Ecb.europa.eu* [online]. 2021 [cit. 11. 12. 2022]. https://www.ecb.europa.eu/pub/pdf/cardfraud/ecb.cardfraudreport202110~cac4c418e8.en.pdf

Chart A

Total value of card fraud using cards issued within SEPA

(left-hand scale: 2009 value = 100; right-hand scale: value of fraud as a share of the value of transactions)

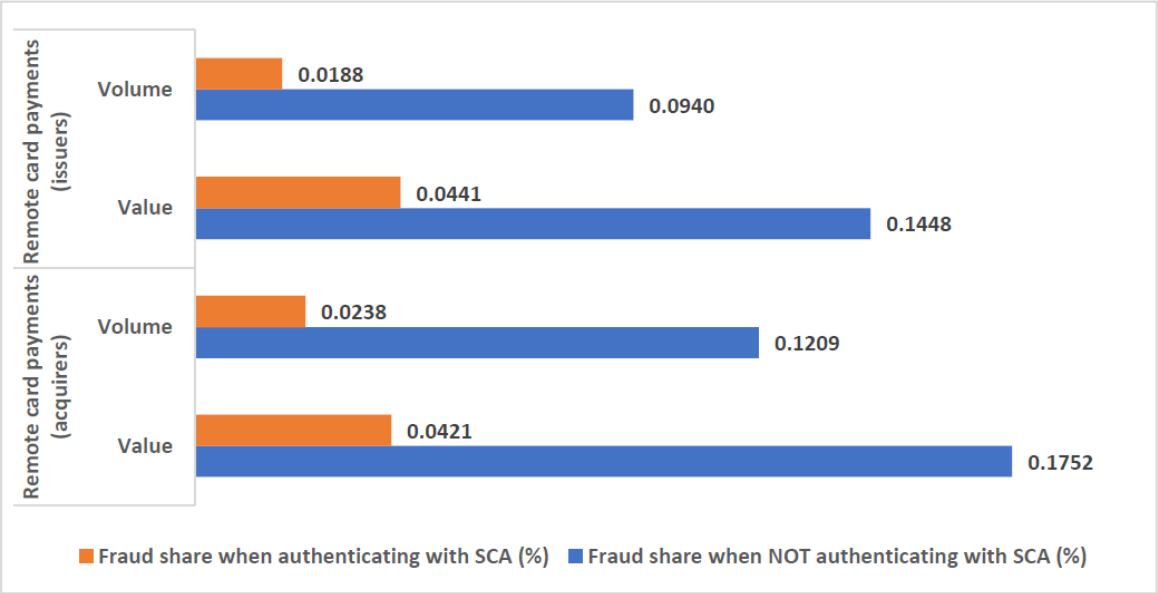


Source: All reporting card payment scheme operators for each year.

Efekt dopadu zavedení SCA na objem a míru podvodů lze očekávat až v datech za rok 2020 a roky následující. K těmto prozatím nebyl vydán nový report ECB, nicméně počátkem roku 2022 byl zveřejněn diskuzní dokument EBA obsahující předběžná data za obě poloviny roku 2020. V případě plateb kartou ukazují údaje za druhé pololetí roku 2020, že podíl podvodů na celkovém objemu a hodnotě plateb je vyšší u plateb, které nejsou ověřeny pomocí SCA, ve srovnání s platbami ověřenými pomocí SCA. Řečeno v číslech z výše uvedeného plyne, že podíl podvodů při platbách kartou s použitím SCA na celkovém objemu a hodnotě transakcí je o 70-80 % nižší než u plateb kartou bez SCA (viz níže uvedený graf).[242]

[242] European Banking Authority. Discussion Paper on payment fraud data received under PSD2. *Eba.europa.eu* [online]. 2022 [cit. 11. 12. 2022]. Dostupné z: https://www.eba.europa.eu/eba-publishes-discussion-paper-its-preliminary-observations-selected-payment-fraud-data-under

Figure 8: Fraud rate for remote card payments reported by issuers and acquirers, with and without SCA



Tento vztah se projevil obdobně také u plateb kartou bez dálkového přístupu a také zejména u přeshraničních karetních plateb s protistranami mimo území EHP, tedy mimo oblast působnosti právní regulace SCA. Neprojevil se však v rámci elektronických platebních příkazů zadaných dálkově. Zde byla míra podvodů v případě použití SCA v druhém pololetí 2020 až 4x vyšší oproti platebním příkazům, při nichž SCA použito nebylo. Jako možné vysvětlení byla uvedena teorie, že takové platby bez použití SCA mohou být platbami s nižším rizikem (jako např. platby s nízkou hodnotou). Tato skutečnost by se nicméně mohla projevit i u jiných typů plateb, což tato teorie nevysvětluje.[243]

Nad rámec výše uvedeného byl zajímavý závěr týkající se karetních plateb provedených na dálku, u nichž nejčastějším druhem podvodu byla krádež údajů o kartě představující 75 % hodnoty podvodných plateb SCA a 60 % hodnoty podvodných plateb jiných než SCA ve 2. pololetí 2020. To lze vysvětlit druhy podvodů jako je např. phishing. V těchto případech dle názoru EBA nemusí být ověřování pomocí SCA při prevenci tohoto typu podvodu účinné.[244]

Konkrétní data, na nichž bude blíže ilustrován dopad zavedení SCA na celkový objem a míru podvodů v souvislosti s CNP platbami bohužel prozatím nejsou k dispozici. Z předběžných dat lze pozorovat jistý náznak ukazující, že zavedení SCA by mohl pozitivně

[243] Tamtéž.

[244] Tamtéž.

ovlivnit míru těchto podvodů. Zjištěná data nicméně nebyla konzistentní ve všech případech a budeme muset počkat na další report ECB, abychom se dozvěděli bližší podrobnosti.

Srovnání celkové hodnoty obchodů, o něž mohou přijít obchodníci z důvodu zavedení SCA, s celkovou hodnotou podvodů s CNP platbami považuji za velmi zajímavé. Jelikož je riziko ztráty tržeb v desetinásobcích celkové hodnoty CNP podvodů, nejeví se z tohoto pohledu zavedení úpravy SCA jako příliš účelné. Bohužel nemáme k dispozici data o tom, jestli uživatelé následně uskuteční nákupy jinde (např. v kamenných obchodech), a lze tak pouze spekulovat o validitě výše uvedeného srovnání. Proporcionalita těchto hodnot je však přinejmenším zarážející.

Výše bylo ilustrováno, že zavedení požadavku SCA do praxe bylo velmi zdlouhavé a pravděpodobně velmi nákladné pro řadu subjektů podílejících se na zpracování platebních transakcí a že i přes více než roční prodloužení stanovené lhůty nebyla řada poskytovatelů platebních služeb a dalších osob podílejících se na zpracování plateb schopna řešení podporující SCA včas implementovat. Pro země, v nichž obdobná úprava prozatím neplatí (např. Spojené státy), může být tato unijní zkušenost společně s daty o dopadu na podnikání obchodníků argumentem, proč obdobnou úpravu prozatím nezavádět a prozatím se snažit hledat alternativní řešení.

Jedním z nezamýšlených dopadů zavedení SCA může být odchod uživatelů od menších obchodníků z důvodu méně povedené implementace díky nižším investovaným nákladům k těm větším, kteří jsou schopni nová řešení finančně lépe vstřebat, jak bylo naznačeno v jednom z reportů společnosti CMSPI výše. Toto bude podpořeno také zavedeným nových poplatků souvisejících s implementací řešení podporujících SCA, které budou opět lépe vstřebávat větší společnosti.

V neposlední řadě nemůžeme vyloučit situaci, kdy zavedení úpravy SCA bude mít v nadcházejících letech jako nepřímý důsledek přesun některých menších společností působících v oblasti platebního styku z důvodu úspory nákladů do zemí, kde na ně nejsou kladeny tak vysoké regulatorní požadavky (např. do Spojených států amerických). Stěží si lze představit situaci, kdy by právě z důvodu vyšších regulatorních nároků a vyšších souvisejících nákladů významněji docházelo k opačnému trendu (s výjimkou společností, které se budou specializovat právě na poskytování řešení podporujících SCA a které se budou snažit na nově regulaci získat nové klienty a vydělat).

5.4.3. Zhodnocení právní úpravy

Právní úprava SCA je poměrně komplexní regulací, která stanoví poskytovatelům platebních služeb povinnost vyžadovat dvoufázové ověření uživatelů při řadě úkonů v elektronickém platebním styku. Těmto poskytovatelům je zároveň umožněno dobrovolně aplikovat kteroukoliv z devíti výjimek a vyhnout se tak povinnosti SCA vyžadovat. Nad rámec povinnosti vyžadovat SCA musí poskytovatelé zavést bezpečnostní mechanismy pro sledování transakcí. V případě porušení povinnosti vyžadovat SCA mohou být poskytovatelé v plném rozsahu odpovědní za jakoukoliv ztrátu způsobenou neautorizovanou platební transakcí.

Jak již bylo uvedeno výše, právní úprava je na řadě míst poměrně obecná či nejasná a z tohoto důvodu čelila EBA velkému množství dotazů zaměřených především na její výklad a aplikaci. Za pomocí nástroje Q&A a vydávání stanovisek se EBA snažila dotčeným subjektům poskytnout co největší množství relevantních informací, aby tito byli schopni aplikovat řešení podporující SCA v souladu s touto regulací. Vzhledem k rozsahu těchto dotazů a stanovisek se však bohužel úprava stala poměrně nepřehlednou a bylo by vhodné některé závěry reflektovat v samotných právních předpisech.

Dále je dle mého názoru úprava problematická z pohledu nastavení sankčních mechanismů, které považuji za nedostatečné. Pokud je zájem členských států na bezpečnosti elektronického platebního styku a velmi nízké míře podvodných plateb v této oblasti natolik vysoký, že se rozhodne zavést takto významnou právní úpravu, měla by být taková právní úprava doprovázena nástroji, kterými budu příslušní regulátoři mít možnost její dodržování vynucovat. Řešením této situace by alespoň na úrovni České republiky bylo zavedení nových přestupků osob oprávněných poskytovat platební služby za nedodržení povinností ve vztahu k SCA v rámci ZPS.

Oblastí, která může v budoucnu z pohledu bezpečnosti elektronického platebního styku hrát důležitou roli, je behaviorální biometrie. Ta se snaží analyzovat chování uživatelů a na základě stovek či tisíců různých dat o jejich konkrétních činnostech v online prostředí, které jsou kontinuálně sbírána, analyzována a při dostatečném množství mohou vytvářet jedinečný digitální profil konkrétní osoby. Sběr takových dat může být citlivý z pohledu ochrany osobních údajů, avšak z pohledu ověřování totožnosti uživatelů může být při nastavení zabezpečení těchto údajů velmi slibný. Bude velmi zajímavé sledovat,

jakým směrem se bude tato technologie vyvíjet a jestli bude tento případný vývoj reflektován v účinné právní úpravě.

Proces implementace řešení podporujících SCA byl velmi složitý a byl provázen řadou komplikací, díky kterým musela být prodloužena finální lhůta pro jejich zavedení. Prozatím nemáme k dispozici dostatečné množství dat, ze kterých by bylo možné činit konkrétní závěry, nicméně z těch předběžných se na první pohled zdá, že by míra a objem podvodů mohly díky zavedení SCA v souladu s původním cílem klesat. Na druhou stranu tato regulace významným způsobem zasáhla obchodníky prodávající zboží nebo poskytující služby v online prostředí, kteří mohou díky svojí či cizí nezdařené implementaci SCA čelit poměrně významné míře ztracených obchodů z důvodu zvýšené frikce, problémům při ověřování totožnosti a celkově horšímu uživatelskému zážitku při placení za jejich zboží/služby. Tato skutečnost se může nepříznivě dotknout především menších obchodníků, jejichž finanční zdroje vynaložené na technická řešení zdaleka nedosahují těch, které mají k dispozici střední a větší podniky.

Z pohledu dopadů na obchodníky se mi úprava vůči těmto subjektům nejeví jako proporcionální, a to především když vezmeme v potaz, že cílem byla ochrana uživatelů a zamezení míry podvodů o hodnotě násobně nižší, než je potenciální výše ztrát z nedokončených obchodů pro tyto obchodníky. Prozatím je nicméně brzy na to, abychom učinili jednoznačné závěry, a je tak třeba vyčkat na aktuálnější a ucelenější data, abychom byli schopni lépe vyhodnotit, jestli proporcionality bylo dosaženo či nikoliv. Zároveň pokud by se ukázalo, že míra a objem podvodů klesnou pouze o jednotky či nižší desítky procent, tak by se celá úprava mohla ukázat jako neúčelná, nemající toužený efekt ani přes dlouhé roky příprav a pouze stanovující nadbytečné regulatorní povinnosti, které stojí celý dotčený trh nemalé časové i finanční náklady.

Za stávající situace se totiž musí dotčené subjekty rozhodnout, jaká zvolit řešení a metody, aby tato splňovala přinejmenším následující podmínky – budou v souladu se všemi požadavky právní úpravy, způsobí co nejmenší frikci či jinak co nejméně negativně ovlivní uživatelský zážitek, budou citlivé k ochraně osobních údajů uživatelů, a to celé za situace, kdy by mělo dojít ke znemožnění zneužití použitých údajů uživatelů a snížení míry podvodů. Bude tak velmi zajímavé sledovat zveřejnění dalších reportů ECB ohledně karetních podvodů

a jakýchkoliv dalších dat a informací, které nám poskytnout lepší vzhled do dopadů úpravy SCA.

6. Závěr

V této rigorózní práci jsem se věnoval právní úpravě SCA a jako cíl jsem si stanovil především vytvoření přehledu stávající právní úpravy, její analýzu a celkové zhodnocení, návrh řešení potenciálně problematických částí, srovnání úpravy s několika státy mimo území EHP a zhodnocení možného budoucího vývoje této regulace. Cíl tak považuji za naplněný a na následujících řádcích uvádím stručné shrnutí hlavních závěrů podrobněji rozvedených v textu samotné rigorózní práce.

Právní úprava SCA byla na území EU zavedena prostřednictvím Směrnice PSD2, kterou členské státy postupně transponovaly do svých právních řádů. Na tuto směrnici navázala Evropská komise přijetím Nařízení RTS, prostřednictvím kterého byly stanoveny regulační technické normy týkající se oblasti SCA. V České republice je povinnost použít SCA stanovena na základě § 223 ZPS pro osoby oprávněné poskytovat platební služby v situacích, kdy plátce (i) přistupuje ke svému platebnímu účtu prostřednictvím internetu, (ii) dává platební příkaz k elektronické platební transakci, (iii) provádí jiný úkon, který je spojen s rizikem podvodného jednání v oblasti platebního styku, zneužitím platebního prostředku nebo informací o platebním účtu, nebo (iv) požaduje informace o platebním účtu prostřednictvím poskytovatele služby informování o platebním účtu.

SCA spočívá v použití alespoň dvou na sobě nezávislých prvků ze tří různých kategorií, kterými jsou (i) údaje známé pouze uživateli, (ii) věci mající uživatel ve své moci a (iii) biometrické údaje uživatele a které byly v této rigorózní práci podrobně rozebrány. Ověřovací postup musí bránit zneužití těchto prvků, přičemž případné prolomení jednoho z nich nesmí ohrozit prvek jiný. Právní úprava SCA současně umožňuje osobě oprávněné poskytovat platební služby využít aplikace některé z celkem devíti výjimek z použití SCA, mezi které řadíme například transakce s důvěryhodnými příjemci, opakující se transakce, bezkontaktní platby v místě prodeje či použití tzv. analýzy transakčních rizik.

Po několika letech od přijetí právní úpravy SCA již lze pozorovat některá úskalí této regulace, která mohou být v praxi problematická. Tato se EBA jako příslušný regulátor snaží postupně adresovat v rámci svých stanovisek a doporučení, která nicméně nedosahují právní závaznosti sekundárních právních předpisů EU. Za úskalí regulace lze zmínit především obecnost úpravy, která v některých klíčových částech působí poskytovatelům platebních

služeb výkladové potíže a díky níž EBA čelila velkému množství dotazů ze strany těchto subjektů. Z tohoto důvodu by právní úprava měla být v některých oblastech zpřesněna či upravena a některé závěry EBA by měly být reflektovány přímo v samotných předpisech. Dále lze zmínit například aspekt odpovědnosti a poměrně nedostatečné nastavení sankčních mechanismů, kdy porušení povinností použít SCA není sankciováno v žádném jiném případě mimo neautorizované platební transakce, což se vzhledem k celkové povaze úpravy a míře požadavků kladených na poskytovatele platebních služeb nejeví jako dostatečné. Tuto situaci by na úrovni České republiky bylo možné řešit zavedením dodatečných přestupků ve vztahu k SCA. V nejbližších letech lze očekávat, že by v rámci další novelizace Směrnice PSD2 mohlo dojít také k zpřesnění některých aspektů týkajících se SCA.

Ač se jedná o poměrně úzce vymezenou regulaci, která na první pohled nemusí působit nikterak významně, tak její zavedení významným způsobem ovlivnilo nejen samotné poskytovatele platebních služeb, ale především také obchodníky a oblast e-commerce. Jednak zavedení této právní úpravy doprovázela řada problémů, díky kterým musela být částečně o rok odložena její účinnost, a jednak bylo přizpůsobení se požadavkům této regulace pravděpodobně velmi nákladné pro řadu subjektů podílejících se na zpracování platebních transakcí.

Prozatím nemáme dostatečné množství relevantních dat pro reálné zhodnocení dopadů zavedení regulace SCA na míru CNP podvodů, předběžná data nicméně ukazují, že k určitému poklesu zde pravděpodobně došlo. Současně se však objevují prvotní data ohledně rizik ztráty tržeb z důvodu vyžadování SCA (které má v řadě případů za následek horší uživatelský zážitek spojený se zvýšenou frikcí či neúspěšnému provedení platby), která převyšují celkovou hodnotu CNP podvodů v desetinásobcích. Tato data lze stěží ověřit a současně neobsahují informace o tom, zdali nákup vůbec uskutečněn nebyl, anebo zdali došlo k následnému nákupu zákazníky u jiných obchodníků či v kamenných obchodech. Z těchto důvodu lze tak polemizovat o validitě tohoto srovnání, nicméně proporcionalita těchto předběžných dat je přinejmenším zarážející. Bude dozajista zajímavé sledovat publikování dat nových, především v rámci dalšího ECB reportu ohledně karetních podvodů, díky kterým bude následně možné lépe zhodnotit účelnost celé úpravy, protože jakýkoliv závěr by pouze na základě těchto předběžných dat byl předčasný.

Jedním ze současných trendů v oblasti bezpečnosti elektronického platebního styku, který v budoucnu pravděpodobně vzroste na důležitosti a může ovlivnit směr budoucí regulace, je zavádění behaviorální biometrie. Ta se zaměřuje na vlastnosti, které se v životě naučíme díky interakci se svým okolním prostředím a přírodou a které utváří různé vzorce chování, které společně charakterizují jedinečný profil každého jedince. Na základě analýzy těchto vzorců chování za pomoci umělé inteligence a metody strojového učení dochází ke kontinuálnímu sběru a analýze dat o chování uživatele, díky kterým je možno ověřit totožnost takového uživatele dynamickým způsobem, tj. po celou dobu, kdy je činnost uživatele sledována. Lze tak například s jistou mírou pravděpodobnosti ověřit jeho totožnost po celou dobu jedné platební relace, nikoliv pouze v době zadání platebního příkazu, a to způsobem, který je pasivní, probíhá v pozadí a nenarušuje uživatelský zážitek.

V souvislosti s používáním této technologie se prozatím jako problematická jeví míra nasbíraných dat o uživatelích a obava z nedostatečné ochrany jejich osobních údajů, na druhou stranu se již objevují předběžná data o účinnosti této technologie, která současně uvádí, že její zavedení zákazníkům ušetřilo nemalé peníze. Potenciál biometrie chování v oblasti bezpečnosti platebního styku se do budoucna jeví jako velmi slibný a lze očekávat její postupné zlepšování a rozšíření jejího používání. Pokud by se tato technologie ukázala jako přesná, účinná, bezpečná a svými kvalitami převyšující ostatní prvky SCA, tak lze v regulatorní rovině potenciálně očekávat postupný přechod k pasivnímu, dynamickému způsobu ověřování totožnosti uživatele oproti dnešnímu statickému, který umožňuje jeho totožnost ověřit pouze k jednomu konkrétnímu okamžiku.

Vzhledem k elektronizaci celého platebního styku lze do budoucna v mezinárodním měřítku očekávat zvýšený důraz na jeho bezpečnost. Řada ekonomicky významných zemí se prozatím rozhodla nejít cestou zavedení povinného SCA a jejich představitelé budou jistě sledovat další reporty ECB ohledně karetních podvodů, které pro ně mohou být inspirací nebo také důvodem hledání alternativního řešení. S rozvojem technologií umělé inteligence a strojového učení lze v budoucnu očekávat stále sofistikovanější metody podvodníků, kterým je zapotřebí preventivně předcházet nastavením pravidel a zavedením technologických opatření, která budou dostatečným způsobem chránit jak spotřebitele, tak celý systém jako takový.

Seznam použitých zkratek

AML směrnice – směrnice Evropského parlamentu a Rady (EU) 2015/849 ze dne 20. května 2015 o předcházení využívání finančního systému k praní peněz nebo financování terorismu, o změně nařízení Evropského parlamentu a Rady (EU) č. 648/2012 a o zrušení směrnice Evropského parlamentu a Rady 2005/60/ES a směrnice Komise 2006/70/ES

AML zákon – zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu

ČNB – Česká národní banka

EBA – Evropský orgán pro bankovnictví

ECB – Evropská centrální banka

EHP – Evropský hospodářský prostor

EU – Evropská unie

Nařízení GDPR – nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

Nařízení RTS – nařízení Evropské komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace

OZ – zákon č. 89/2012 Sb., občanský zákoník

SCA – silné ověření uživatele

SDEU – Soudní dvůr Evropské unie

SecuRe Pay – Evropské fórum pro bezpečnost spotřebitelských plateb

Směrnice PSD – Směrnice Evropského parlamentu a Rady 2007/64/ES ze dne 13. listopadu 2007 o platebních službách na vnitřním trhu, kterou se mění směrnice 97/7/ES, 2002/65/ES, 2005/60/ES a 2006/48/ES a zrušuje směrnice 97/5/ES

Směrnice PSD2 – 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

Zákon o ČNB – zákon č. 6/1993 Sb., o České národní bance

ZPS – zákon č. 370/2017 Sb., o platebním styku

ZPS 2009 – zákon č. 284/2009 Sb., o platebním styku

Seznam použitých zdrojů

(A) ODBORNÁ LITERATURA

(1) BAKEŠ, Milan, Marie KARFÍKOVÁ, Petr KOTÁB, Hana MARKOVÁ a kol. *Finanční právo*. 6. vydání. Praha: C. H. Beck, 2012. ISBN 978-80-7400-440-7.

(2) BERAN, Jiří, Daniela DOLEŽALOVÁ, Dalibor STRNADEL a Alice ŠTĚPÁNOVÁ. *Zákon o platebním styku. Komentář*. Praha: C. H. Beck, 2011. ISBN 978-80-7400-369-1.

(3) BERAN, Jiří, Tomáš NÝDRLE a Dalibor STRNADEL. *Zákon o platebním styku. Komentář*. 1. vydání. Praha: Wolters Kluwer ČR, 2020. ISBN 978-80-7598-788-4.

(4) BLAKSTAD, Sofie a Robert ALLEN. *Fintech Revolution. Universal inclusion in the new financial ecosystem*. Londýn: Palgrave Macmillan, 2018. ISBN: 978-3-319-76013-1.

(5) DVOŘÁK, Petr. *BANKOVNICTVÍ pro bankéře a klienty*. 3. vydání. Praha: Linde Praha, a.s., 2005. ISBN 80-7201-515-X.

(6) HULMÁK, Milan a kol. *Občanský zákoník VI. Závazkové právo. Zvláštní část (§ 2055–3014)*. 1. vydání. Praha: C. H. Beck, 2014. ISBN 978-80-7400-287-8.

(7) JANOVEC, Michal. Postavení dohledu nad finančním trhem v systému finančního práva. *Bulletin-advokacie.cz* [online]. 2014 [cit. 05. 03. 2022]. Dostupné z: http://www.bulletin-advokacie.cz/postaveni-dohledu-nad-financnim-trhem-v-systemu-financniho-prava

(8) JÍLEK, Josef. *Finance v globální ekonomice I. Peníze a platební styk*. 1. vydání. Praha: GRADA Publishing, a.s., 2013. ISBN 978-80-247-3893-2.

(9) KUČEROVÁ, Alena; Ludmila NOVÁKOVÁ, Vanda FOLDOVÁ, František NONNEMANN a Daniel POSPÍŠIL. *Zákon o ochraně osobních údajů. Komentář*. 1. vydání. Praha: C. H. Beck, 2012. ISBN 978-80-7179-226-0.

(10) LAVICKÝ, Petr a kol. *Občanský zákoník I. Obecná část (§ 1–654). Komentář*. 2. vydání. Praha: C. H. Beck, 2022. ISBN 978-80-7400-852-8.

(11) MÁČE, Miroslav. *Platební styk – klasický a elektronický*. 1. vydání. Praha: GRADA Publishing, a.s., 2006. ISBN 80-247-1725-5.

(12) MÁLEK, Petr, Gabriela OŠKRDALOVÁ a Petr VALOUCH. *Osobní finance*. 1. vydání. Brno: Ekonomicko-správní fakulta Masarykovy Univerzity, 2010. ISBN 978-80-210-5157-7.

(13) MARVANOVÁ, Marie, Martin HOUDA a kol. *Platební styk (aneb platební a zajišťovací instrumenty ve vnitřním a zahraničním obchodě)*. Brno, E.P.B.K, 1993. ISBN 80-901627-0-3.

(14) MATEJKA, Ján, Alžběta Krausová a Güttler Vojen. Biometrické údaje a jejich právní režim. *Revue pro právo a technologie* [online]. 2018, č. 17, s. 91. [cit. 12. 08. 2022]. Dostupné z: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=nrptembrhbpxe4dul4ytox3tl44tc&groupIndex=5&rowIndex=0#

(15) NOORIALA Amir. The difference between physical and behavioral biometrics, and which you should be using. *Information-age.com* [online]. 2021 [cit. 30. 10. 2022]. Dostupné z: https://www.information-age.com/difference-between-physical-and-behavioural-biometrics-which-you-should-be-using-123496929/

(16) PALMA, David a MONTESSORO, Pier Luca. *Biometric-Based Human Recognition Systems: An Overview*. In: SARFRAZ, Muhammad, editor. *Recent Advances in Biometrics. Behavioral* [online]. Londýn: IntechOpen. 2021 [online]. [cit. 30. 10. 2022]. ISBN: 978-1-80355-458-7. Dostupné z: https://www.intechopen.com/chapters/80748

(17) PETROV, Jan, Michal VÝTISK, Vladimír BERAN a kol. *Občanský zákoník. Komentář*. 2. vydání. Praha: C. H. Beck, 2022. ISBN: 978-80-7400-747-7.

(18) POLOUČEK, Stanislav a kol. *Bankovnictví*. 2. vydání. Praha: C. H. Beck, 2013. ISBN 978-80-7400-491-9.

(19) PROCTOR, Charles. *The Law and Practise of International Banking*. Londýn: Oxford University Press, 2010. ISBN 978-0-19-929186-1

(20) REES Megan. The Future of User Authentication: A Guide to Behavioral Biometrics. *Expertinsights.com* [online]. 2022 [cit. 30. 10. 2022]. Dostupné z: https://expertinsights.com/insights/a-guide-to-behavioral-biometrics/

(21) REVETT, Kenneth. *Behavioral Biometrics. A Remote Access Approach*. Chichester, UK: John Wiley & Sons Ltd, 2008. ISBN: 978-0-470-51883-0.

(22) SAEED, Khalid, Marcin ADAMSKI, Tapalina BHATTASALI, Mohammad K. NAMMOUS, Piotr PANASIUK, Mariusz RYBNIK a Soharab H. SHAIKH. *New directions in behavioral biometrics.* Boca Raton: CRC Press, Taylor & Francis Group, LLC. 2017. ISBN 978-14987-8462-7.

(23) SARFRAZ, Muhammad, editor. *Recent Advances in Biometrics. Behavioral* [online]. Londýn: IntechOpen. 2022 [online]. [cit. 30. 10. 2022]. ISBN: 978-1-80355-458-7. Dostupné z: https://www.intechopen.com/chapters/80748

(24) SCHLOSSBERGER, Otakar. *Platební služby.* 1. vydání. Praha: Management Press, s. r. o., 2012. ISBN 978-80-7261-238-3.

(25) SCHLOSSBERGER, Otakar a Marcela SOLDÁNOVÁ. *Platební styk*. 3. vydání. Praha: Bankovní institut, a.s., 2005. ISBN 80-7265-072-6.

(26) SHARMA, Mridula a Haytham ELMILIGI. *Biometrics: Past, Present and Future.* In: SARFRAZ, Muhammad, editor. *Recent Advances in Biometrics. Behavioral* [online]. Londýn: IntechOpen. 2022 [online]. [cit. 30. 10. 2022]. ISBN: 978-1-80355-458-7. Dostupné z: https://www.intechopen.com/chapters/80748

(27) ŠENKÝŘOVÁ, Bohuslava a kol. *Bankovnictví.* 1. vydání. Praha: Vysoká škola finanční a správní, o.p.s., 2010. ISBN 978-80-7408-029-6.

(28) TOMÍŠEK, Jan. Právní jednání biometrickými prostředky v elektronickém bankovnictví. *Právní rozhledy* [online]. 2018, č. 5, s. 160. [cit. 12. 08. 2022]. Dostupné z: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=nrptembrhbpxa4s7gvpxgxzrgyya&groupIndex=2&rowIndex=0

(29) WANG Liang, Xin GENG. *Behavioral biometrics for human identification*. Hershey: IGI Global, 2010. ISBN 978-1-60566-726-3.

(B) ONLINE ZDROJE

(1) Australian Competition and Consumer Commission. ACCC proposes to deny authorisation to APCA for 3D Secure arrangements. *Accc.gov.au* [online]. 2016 [cit. 4. 12. 2022]. Dostupné z: https://www.accc.gov.au/media-release/accc-proposes-to-deny-authorisation-to-apca-for-3d-secure-arrangements

(2) Barclaycard. Retailers losing out on £4.3million in sales each day as new SCA rules block non-compliant online transactions. *Home.barclaycard* [online]. 2022 [cit. 11. 12. 2022]. Dostupné z: https://home.barclaycard/press-releases/2022/04/retailers-losing-out-on-4-3-million-in-sales-each-day/

(3) BioCatch. Large Australian Financial Services Organization Disrupts Mule Operations and Stops Over 90% of Fraudulent Payments Using Behavioral Biometrics & Device Intelligence. *BioCatch.com* [online]. 2022 [cit. 02. 11. 2022]. Dostupné z: https://www.biocatch.com/hubfs/Case_Studies/CS-AUBank-Stops-ATO-Mules.pdf

(4) BioCatch. Top 5 UK Bank Saves £500K per Month in Fraud Losses by Preventing Social Engineering Voice Scams Using Behavioral Insights. *BioCatch.com* [online]. 2022 [cit. 02. 11. 2022]. Dostupné z: https://www.biocatch.com/hubfs/New%20Boilerplate/BC%20CS%20APP%20Fraud%20V2%20NBP.pdf

(5) CMSPI. SCA Report – Latest December Updates. Cmspi.com [online]. 2021 [cit. 11. 12. 2022]. Dostupné z: https://cmspi.com/eur/en/resources/content/sca-report-latest-december-updates/

(6) CMSPI. Strong Customer Authentication (SCA) – Impact Assessment – February 2021. *Cmspi.com* [online]. 2021 [cit. 11. 12. 2022]. Dostupné z: https://cmspi.com/eur/en/resources/content/strong-customer-authentication-sca-impact-assessment-february-2021/

(7) CMSPI. Strong Customer Authentication (SCA) – Impact Assessment – September 2021. *Cmspi.com* [online]. 2021 [cit. 11. 12. 2022]. Dostupné z: https://cmspi.com/eur/en/resources/content/strong-customer-authentication-sca-impact-assessment-september-2021/

(8) CMSPI. The New Ecommerce Fees: Why European Merchants Need to Act. *Cmspi.com* [online]. 2022 [cit. 11. 12. 2022]. Dostupné z: https://cmspi.com/eur/en/resources/content/the-new-ecommerce-fees-why-european-merchants-need-to-act/

(9) Comparitech Limited. 25+ Password statistics (that may change your password habits). *Comparitech.com* [online]. 2022 [cit. 10. 12. 2022]. Dostupné z: https://www.comparitech.com/blog/information-security/password-statistics/

(10) Consumer Financial Protection Bureau. CFPB Takes Action to Protect the Public from Shoddy Data Security Practices. Consumerfinance.gov [online]. 2022 [cit. 5. 12. 2022]. Dostupné z: https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-to-protect-the-public-from-shoddy-data-security-practices/

(11) Consumer Financial Protection Bureau. Consumer Financial Protection Circular 2022-04. *Consumerfinance.gov* [online]. 2022 [cit. 5. 12. 2022]. Dostupné z: https://www.consumerfinance.gov/compliance/circulars/circular-2022-04-insufficient-data-protection-or-security-for-sensitive-consumer-information/

(12) Česká národní banka. ABO – systém pro vedení účtů a provádění plateb. *Cnb.cz* [online]. 2019 [cit. 06. 03. 2022]. https://www.cnb.cz/cs/platebni-styk/sluzby-pro-klienty/abo-system-pro-vedeni-uctu-a-provadeni-plateb/

(13) Česká národní banka. ARAD – Systém časových řad. *Cnb.cz* [online]. 2019 [cit. 06. 03. 2022]. Dostupné z: https://www.cnb.cz/cnb/STAT.ARADY_PKG.STROM_SESTAVY?p_strid=AAAE

(14) Česká národní banka. Dohledové sdělení č. 2/2021 K možnosti používat výjimku ze silného ověření klienta v případech zabezpečených platebních procesů a protokolů společnosti. *Cnb.cz* [online]. 2021 [cit. 27. 10. 2022]. Dostupné z: https://www.cnb.cz/export/sites/cnb/cs/dohled-financni-trh/.galleries/vykon_dohledu/dohledove_benchmarky/download/dohledove_sdeleni_2021_02.pdf

(15) Česká národní banka. Popis systému CERTIS. *Cnb.cz* [online]. 2019 [cit. 06. 03. 2022]. https://www.cnb.cz/cs/platebni-styk/certis/popis-systemu-certis/

(16) Česká národní banka. Pravidla platebního systému CERTIS. *Cnb.cz* [online]. 2019 [cit. 06. 03. 2022]. Dostupné z: https://www.cnb.cz/cs/platebni-styk/certis/pravidla-platebniho-systemu-certis/

(17) Česká národní banka. Silné ověření uživatele u plateb kartou na internetu od 1. 1. 2021. *Cnb.cz* [online]. 2021 [cit. 10. 12. 2022]. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/vykon-dohledu/upozorneni-pro-verejnost/Silne-overeni-uzivatele-u-plateb-kartou-na-internetu-od-1.-1.-2021/

(18) EBA CLEARING. The Company. *Ebaclearing.eu* [online]. 2017 [cit. 06. 03. 2022]. https://www.ebaclearing.eu/about-eba-clearing/at-a-glance/the-company/

(19) Ecommerce Europe. Ecommerce Europe co-signs a Joint-Industry Letter on European SCA implementation. *Ecommerce-europe.eu* [online]. 2019 [cit. 10. 12. 2022]. Dostupné z: https://ecommerce-europe.eu/publication/ecommerce-europe-co-signs-a-joint-industry-letter-on-european-sca-implementation/

(20) Ecommerce Europe. Retail Joint Letter on measuring the impact of SCA April 2021. *Ecommerce-europe.eu* [online]. 2021 [cit. 11. 12. 2022]. Dostupné z: https://web.archive.org/web/20211026061453/https://www.eurocommerce.eu/media/196158/20210430%20Retail%20Joint%20Letter%20on%20measuring%20the%20impact%20of%20SCA%20April%202021%20-%20EBA.pdf

(21) European Banking Authority. Discussion Paper on payment fraud data received under PSD2. *Eba.europa.eu* [online]. 2022 [cit. 11. 12. 2022]. Dostupné z: https://www.eba.europa.eu/eba-publishes-discussion-paper-its-preliminary-observations-selected-payment-fraud-data-under

(22) European Banking Authority. EBA REPORT on the data provided by PSPs on their readiness to apply strong customer authentication for e-commerce card-based payment transactions. *Eba.europa.eu* [online]. 2021 [cit. 02. 11. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2021/1014781/Report%20on%20the%20data%20provided%20by%20PSPs%20on%20their%20readiness%20to%20apply%20SCA.pdf

(23) European Banking Authority. Final guidelines on the security of the internet payments. *Eba.europa.eu* [online]. 2014 [cit. 30. 07. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/934179/f27bf266-580a-4ad0-aaec-59ce52286af0/EBA-GL-2014-12%20%28Guidelines%20on%20the%20security%20of%20internet%20payments%29_Rev1.pdf

(24) European Banking Authority. Final Report. Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2). *Eba.europa.eu* [online]. 2017 [cit. 25. 10. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1761863/314bd4d5-ccad-47f8-bb11-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%28EBA-RTS-2017-02%29.pdf

(25) European Banking Authority. Letter from Olivier Guersent, on the Commission intention to amend the draft RTS on SCA and CSC. *Eba.europa.eu* [online]. 2017 [cit. 26. 10. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1863077/efbf06e1-b0e9-4481-88e5-b70daa663cb9/%28EBA-2017-E-1315%29%20Letter%20from%20O%20Guersent%2C%20FISMA%20re%20Commission%20intention%20to%20amend%20the%20draft%20RTS%20on%20SCA%20and%20CSC%20-Ares%282017%292639906.pdf

(26) European Banking Authority. Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2). *Eba.europa.eu* [online]. 2022 [cit. 02. 11. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2022/Opinion%20od%20PSD2%20review%20%28EBA-Op-2022-06%29/1036016/EBA%27s%20response%20to%20the%20Call%20for%20advice%20on%20the%20review%20of%20PSD2.pdf

(27) European Banking Authority. Opinion of the European Banking Authority on the deadline for the migration to SCA for e-commerce card-based payment transactions. *Eba.europa.eu* [online]. 2019 [cit. 02. 11. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2622242/e8b3ec84-c1c6-4e9a-96ea-3575361dc230/Opinion%20on%20the%20deadline%20for%20the%20migration%20to%20SCA.pdf?retry=1

(28) European Banking Authority. Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2. *Eba.europa.eu* [online]. 2019 [cit. 07. 08. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf

(29) European Banking Authority. Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC. *Eba.europa.eu* [online]. 2018 [cit. 07. 08. 2022]. Dostupné z: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2137845/0f525dc7-0f97-4be7-9ad7-800723365b8e/Opinion%20on%20the%20implementation%20of%20the%20RTS%20on%20SCA%20and%20CSC%20%28EBA-2018-Op-04%29.pdf

(30) European Banking Authority. Single Rulebook Q&A. *Eba.europa.eu* [online]. 2018 [cit. 06. 08. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa

(31) European Banking Authority. Single Rulebook Q&A. Applicability of SCA to 'card payments initiated by the payee only'. *Eba.europa.eu* [online]. 2018 [cit. 29. 10. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4031

(32) European Banking Authority. Single Rulebook Q&A. Authentication code. *Eba.europa.eu* [online]. 2018 [cit. 26. 10. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4141

(33) European Banking Authority. Single Rulebook Q&A. Definition of payee for dynamic linking. *Eba.europa.eu* [online]. 2019 [cit. 26. 10. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4556

(34) European Banking Authority. Single Rulebook Q&A. Display of incorrect authentication factors in case of failed authentication attempts. *Eba.europa.eu* [online]. 2018 [cit. 26. 10. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4041

(35) European Banking Authority. Single Rulebook Q&A. Dynamic linking: transactions for which the final amount is unknown and may be lower or higher than authenticated amount. *Eba.europa.eu* [online]. 2020 [cit. 29. 10. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5133

(36) European Banking Authority. Single Rulebook Q&A. Independence of the elements for SCA. *Eba.europa.eu* [online]. 2020 [cit. 29. 10. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5619

(37) European Banking Authority. Single Rulebook Q&A. Length of authentication codes. *Eba.europa.eu* [online]. 2019 [cit. 07. 08. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4053

(38) European Banking Authority. Single Rulebook Q&A. "Push based" authentication and SCA requirements. *Eba.europa.eu* [online]. 2019 [cit. 07. 08. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2019_4984

(39) European Banking Authority. Single Rulebook Q&A. Qualification of SMS OTP as an authentication factor. *Eba.europa.eu* [online]. 2018 [cit. 07. 08. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4039

(40) European Banking Authority. Single Rulebook Q&A. Signature on a paper slip from a payment terminal, as a factor in a two-factor SCA. *Eba.europa.eu* [online]. 2018 [cit. 29. 10. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4237

(41) European Banking Authority. Single Rulebook Q&A. Signature performed on the screen of a digital device as a factor in a two-factor SCA. *Eba.europa.eu* [online]. 2018 [cit. 29. 10. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2018_4238

(42) European Banking Authority. Single Rulebook Q&A. Tokenised card details as a SCA possession element. *Eba.europa.eu* [online]. 2019 [cit. 07. 08. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4827

(43) European Banking Authority. Single Rulebook Q&A. Treatment of electronic bookings similar to Mail Order and Telephone Orders (MO-TO) transactions. *Eba.europa.eu* [online]. 2019 [cit. 29. 10. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4788

(44) European Banking Authority. Single Rulebook Q&A. Use of behavioural data for SCA. *Eba.europa.eu* [online]. 2020 [cit. 02. 11. 2022]. Dostupné z: https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2020_5620

(45) EUROPEAN CENTRAL BANK. ECB releases final Recommendations for the security of internet payments and starts public consultation on payment account access services. *Ecb.europa.eu* [online]. 2013 [cit. 29. 07. 2022]. https://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html

(46) EUROPEAN CENTRAL BANK. Eurosystem mission. *Ecb.europa.eu* [online]. 2015 [cit. 06. 03. 2022]. Dostupné z: https://www.ecb.europa.eu/ecb/orga/escb/eurosystem-mission/html/index.en.html

(47) EUROPEAN CENTRAL BANK. First ECB report on card fraud shows chips have increased the security of physical transactions. *Ecb.europa.eu* [online]. 2012 [cit. 30. 07. 2022]. https://www.ecb.europa.eu/press/pr/date/2012/html/pr120725_1.en.html

(48) EUROPEAN CENTRAL BANK. Recommendations for the security of internet payments. *Ecb.europa.eu* [online]. 2013 [cit. 29. 07. 2022]. https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf

(49) EUROPEAN CENTRAL BANK. Report on Card Fraud. *Ecb.europa.eu* [online]. 2012 [cit. 30. 07. 2022]. https://www.ecb.europa.eu/pub/pdf/cardfraud/cardfraudreport201207en.pdf

(50) EUROPEAN CENTRAL BANK. Seventh Report on Card Fraud. *Ecb.europa.eu* [online]. 2021 [cit. 11. 12. 2022]. https://www.ecb.europa.eu/pub/pdf/cardfraud/ecb.cardfraudreport202110~cac4c418e8.en.pdf

(51) EUROPEAN CENTRAL BANK. Third Report on Card Fraud. *Ecb.europa.eu* [online]. 2014 [cit. 29. 07. 2022]. https://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201402en.pdf

(52) EUROPEAN CENTRAL BANK. What is TARGET2? *Ecb.europa.eu* [online]. 2008 [cit. 06. 03. 2022]. https://www.ecb.europa.eu/paym/target/target2/html/index.en.html

(53) European Commission. Payment services directive – frequently asked questions. *Ec.europa.eu* [online]. 2018 [cit. 06. 08. 2022]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/memo_15_5793

(54) International Biometrics + Identity Association. Behavioral Biometrics. *Ibia.org* [online]. 2017 [cit. 30. 10. 2022]. Dostupné z: https://www.ibia.org/download/datasets/3839/Behavioral;

(55) Ministerstvo vnitra České republiky. Cestovní doklady s biometrickými prvky (CDBP). *Mvcr.cz* [online]. 2022 [cit. 12. 08. 2022]. Dostupné z: https://www.mvcr.cz/clanek/cestovni-doklady-s-biometrickymi-prvky-cdbp.aspx?q=Y2hudW09MQ%3D%3D

(56) Mint. RBI eases two-factor authentication for online card transactions up to Rs2,000. *Livemint.com in* [online]. 2016 [cit. 4. 12. 2022]. Dostupné z: https://www.livemint.com/Industry/bJmdHvAuLVC5af1O0NCE0O/RBI-eases-rules-for-online-card-payments-up-to-Rs2000.html

(57) Nethone. PSD2 SCA exemptions: transaction risk analysis (TRA). *Nethone.com* [online]. 2021 [cit. 11. 12. 2022]. Dostupné z: https://nethone.com/post/psd2-sca-exemptions-transaction-risk-analysis-tra

(58) Nuapay. EML Open Banking Uncovers A 37% Increase In Payment Declines Following SCA Implementation. *Nuapay.com* [online]. 2022 [cit. 11. 12. 2022]. Dostupné z: https://www.nuapay.com/en/resources/in-the-news/eml-open-banking-uncovers-a-37-increase-in-payment-declines-following-sca-implementation/

(59) Office of Privacy Commissioner of Canada. Guidelines for identification and authentication. *Priv.gc.ca* [online]. 2016 [cit. 4. 12. 2022]. Dostupné z: https://www.priv.gc.ca/en/privacy-topics/identities/identification-and-authentication/auth_061013/

(60) OneSpan Inc. Behavioral Biometrics. *Onespan.com* [online]. 2022 [cit. 30. 10. 2022]. Dostupné z: https://www.onespan.com/topics/behavioral-biometrics

(61) OneSpan Inc. The financial regulatory landscape in Turkey is modernising quickly. *Onespan.com* [online]. 2020 [cit. 4. 12. 2022]. Dostupné z: https://www.onespan.com/topics/two-factor-authentication?ad=blog-text

(62) Policie České republiky. Kriminalistická daktyloskopie. *Policie.cz* [online]. 2022 [cit. 12. 08. 2022]. Dostupné z: https://www.policie.cz/clanek/kriminalisticka-daktyloskopie-266095.aspx

(63) RecFaces LLC. Behavioral Biometrics: Explaining in Detail. *RecFaces.com* [online]. 2021 [cit. 30. 10. 2022]. Dostupné z: https://recfaces.com/articles/what-are-behavioral-biometrics

(64) RecFaces LLC. Types of Biometrics: Complete Guide. *RecFaces.com* [online]. 2020 [cit. 30. 10. 2022]. Dostupné z: https://recfaces.com/articles/types-of-biometrics

(65) Reserve Bank of India. Master Direction on Digital Payment Security Controls. *Rbi.org.in* [online]. 2021 [cit. 4. 12. 2022]. Dostupné z: https://www.rbi.org.in/scripts/FS_Notification.aspx?Id=12032&fn=2&Mode=0#MD

(66) Sdružení pro bankovní karty (SBK). Souhrnná statistika SBK. *Bankovnikarty.cz* [online]. 2022 [cit. 06. 03. 2022]. Dostupné z: http://www.bankovnikarty.cz/pages/czech/profil_statistiky.html

(67) Sveriges Riksbank. The payment market is being digitized – Cash is losing ground. *Riskbank.se* [online]. 2020 [cit. 06. 03. 2022]. Dostupné z: https://www.riksbank.se/en-gb/payments--cash/payments-in-sweden/payments-in-sweden-2020/1.-the-payment-market-is-being-digitalised/cash-is-losing-ground/the-use-of-cash-is-declining/

(68) Swift SMS Gateway. Canadian Banking Moves Toward Two-Factor Authentication (2FA). Swiftsmsgateway.com [online]. 2021 [cit. 4. 12. 2022]. Dostupné z: https://www.swiftsmsgateway.com/2021/07/27/canadian-banking-moves-toward-two-factor-authentication-2fa/

(69) T.C. Cumhurbaşkanlığı Külliyesi (T.C. Resmi Gazete). *Resmigazete.gov.tr* [online]. 2020 [cit. 4. 12. 2022]. Dostupné z: https://www.resmigazete.gov.tr/eskiler/2020/03/20200315-10.htm

(70) The Economic Times. Sebi extends two-factor authentication for mutual fund subscription transactions. *Economictimes.indiatimes.com* [online]. 2022 [cit. 4. 12. 2022]. Dostupné z: https://economictimes.indiatimes.com/markets/stocks/news/sebi-extends-two-factor-authentication-for-mutual-fund-subscription-transactions/articleshow/94566748.cms?from=mdr

(71) The Payments Association. Physical biometrics vs. Behavioral biometrics. *Thepaymentsassociation.org* [online]. 2021 [cit. 30. 10. 2022]. Dostupné z: https://thepaymentsassociation.org/article/physical-biometrics-vs-behavioral-biometrics/

(72) The Wall Street Journal. President Biden Signs Cybersecurity Executive Order to Boost Federal Defenses Against Hacks. *Wsj.com* [online]. 2021 [cit. 5.12.2022]. Dostupné z: https://www.wsj.com/articles/president-biden-signs-cybersecurity-executive-order-to-boost-federal-defenses-against-hacks-11620859243?mod=article_inline

(73) The World Bank. GDP (current US$). *Data.worldbank.org* [online]. 2022 [cit. 5. 12. 2022]. Dostupné z: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?most_recent_value_desc=true

(74) TheGlobalEconomy.com. Percent people with debit cards – Country rankings. *TheGlobalEconomy.com* [online]. 2017 [cit. 06. 03. 2022]. Dostupné z: https://www.theglobaleconomy.com/rankings/people_with_debit_cards/

(75) UK Finance Limited. Strong customer authentication – frequently asked questions. *Ukfinance.org.uk* [online]. 2022 [cit. 5. 12. 2022]. Dostupné z: https://www.ukfinance.org.uk/our-expertise/payments/strong-customer-authentication/strong-customer-authentication-frequently-asked-questions

(C) PRÁVNÍ PŘEDPISY

(1) Nařízení Evropského Parlamentu a Rady (EU) 2021/1230 ze dne 14. července 2021 o přeshraničních platbách v Unii.

(2) Nařízení Evropské komise v přenesené pravomoci (EU) 2018/389 ze dne 27. listopadu 2017, kterým se doplňuje směrnice Evropského parlamentu a Rady (EU) 2015/2366, pokud jde o regulační technické normy týkající se silného ověření klienta a společných a bezpečných otevřených standardů komunikace.

(3) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

(4) Nařízení Evropského parlamentu a Rady (EU) 2015/847 ze dne 20. května 2015 o informacích doprovázejících převody peněžních prostředků a o zrušení nařízení (ES) č. 1781/2006.

(5) Nařízení Evropského parlamentu a Rady (EU) 2015/751 ze dne 29. dubna 2015 o mezibankovních poplatcích za karetní platební transakce.

(6) Nařízení Evropské Centrální Banky (EU) č. 1409/2013 ze dne 28. listopadu 2013, o statistice platebního styku.

(7) Nařízení Evropského parlamentu a Rady (EU) č. 260/2012 ze dne 14. března 2012, kterým se stanoví technické a obchodní požadavky pro úhrady a inkasa v eurech a kterým se mění nařízení (ES) č. 924/2009.

(8) Směrnice Evropského parlamentu a Rady (EU) 2019/2177 ze dne 18. prosince 2019, kterou se mění směrnice 2009/138/ES o přístupu k pojišťovací a zajišťovací činnosti a jejím výkonu (Solventnost II), směrnice 2014/65/EU o trzích finančních nástrojů a směrnice (EU) 2015/849 o předcházení využívání finančního systému k praní peněz nebo financování terorismu.

(9) Směrnice Evropského parlamentu a rady (EU) 2018/843 ze dne 30. května 2018, kterou se mění směrnice (EU) 2015/849 o předcházení využívání finančního systému k praní peněz nebo financování terorismu a směrnice 2009/138/ES a 2013/36/EU.

(10) 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.

(11) Směrnice Evropského parlamentu a Rady (EU) 2015/849 ze dne 20. května 2015 o předcházení využívání finančního systému k praní peněz nebo financování terorismu, o změně nařízení Evropského parlamentu a Rady (EU) č. 648/2012 a o zrušení směrnice Evropského parlamentu a Rady 2005/60/ES a směrnice Komise 2006/70/ES.

(12) Směrnice Evropského parlamentu a Rady 2014/92/EU ze dne 23. července 2014 o porovnatelnosti poplatků souvisejících s platebními účty, změně platebního účtu a přístupu k platebním účtům se základními prvky.

(13) Směrnice Evropského parlamentu a Rady 2007/64/ES ze dne 13. listopadu 2007 o platebních službách na vnitřním trhu, kterou se mění směrnice 97/7/ES, 2002/65/ES, 2005/60/ES a 2006/48/ES a zrušuje směrnice 97/5/ES.

(14) Smlouva o fungování Evropské unie 2012/C 326/01.

(15) Vyhláška č. 401/2021 Sb., o předkládání některých výkazů v oblasti platebního styku České národní bance.

(16) Vyhláška č. 150/2019 Sb., o hlášení bezpečnostních a provozních rizik v oblasti platebního styku.

(17) Vyhláška č. 141/2018 Sb., o hlášení závažných bezpečnostních a provozních incidentů osobami oprávněnými poskytovat platební služby.

(18) Vyhláška č. 74/2018 Sb., o službách spojených s platebním účtem, na které se vztahuje jednotné označení.

(19) Vyhláška č. 7/2018 Sb., o některých podmínkách výkonu činnosti platební instituce, správce informací o platebním účtu, poskytovatele platebních služeb malého rozsahu, instituce elektronických peněz a vydavatele elektronických peněz malého rozsahu.

(20) Zákon č. 370/2017 Sb., o platebním styku.

(21) Zákon č. 277/2013 Sb., o směnárenské činnosti.

(22) Zákon č. 89/2012 Sb., občanský zákoník.

(23) Zákon č. 136/2011 Sb., o oběhu bankovek a mincí.

(24) Zákon č. 284/2009 Sb., o platebním styku.

(25) Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu.

(26) Zákon č. 229/2002 Sb., o finančním arbitrovi.

(27) Zákon č. 29/2000 Sb., o poštovních službách, ve znění pozdějších předpisů.

(28) Zákon č. 87/1995 Sb., o spořitelních a úvěrních družstvech.

(29) Zákon č. 6/1993 Sb., o České národní bance.

(30) Zákon č. 586/1992 Sb., o daních z příjmů.

(31) Zákon č. 21/1992 Sb., o bankách.

(32) Zákon č. 191/1950 Sb., směnečný a šekový.

(D) JUDIKATURA

(1) Rozhodnutí Úřadu pro ochranu osobních údajů ze dne 21. 3. 2019, č. j. UOOU-10138/18-8. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=34470

(2) Rozsudek SDEU ze dne 15. 7. 2021, Fédération bancaire française (FBF) v. Autorité de contrôle prudentiel et de résolution (ACPR), C-911/19, ECLI:EU:C:2021:599, body 41-49. Dostupné z: https://curia.europa.eu/juris/liste.jsf?language=cs&num=C-911/19

(3) Rozsudek SDEU ze dne 4. 10. 2018, ING-DiBa Direktbank Austria, C-191/17, ECLI:EU:C:2018:809. Dostupné z: https://curia.europa.eu/juris/liste.jsf?language=cs&num=C-191/17

(E) OSTATNÍ ZDROJE

(1) Důvodová zpráva k zákonu č. 284/2009 Sb., o platebním styku. 2009. Dostupné z: www.beck-online.cz.

(2) Důvodová zpráva k zákonu č. 370/2017 Sb., o platebním styku. 2017. Dostupné z: www.beck-online.cz.

(3) Konzultace s JUDr. Tomášem Sejkorou, Ph.D. ze dne 9. září 2022, 26. září 2022, 5. ledna 2023 a 17. ledna 2023.

Právní regulace silného ověření uživatele

Abstrakt

Předmětem této rigorózní práce je právní úprava silného ověření uživatele. Jejím cílem je vytvořit přehled stávající právní úpravy silného ověření uživatele, poukázat na případné nedostatky této regulace, navrhnout související řešení a zhodnotit dopady a účelnost jejího zavedení. V úvodní části se autor nejdříve věnuje popisu stávající právní úpravy platebního styku, druhům platebních systémů, díky kterým dochází k zúčtování plateb v elektronickém platebním styku, dále rozboru jednotlivých platebních služeb dle zákona o platebním styku a osobám oprávněným je poskytovat. Závěrem této části autor popisuje stručný historický vývoj úpravy a uvádí přehled účinných právních předpisů této v oblasti na území České republiky a Evropské unie.

V další části se autor věnuje samotnému konceptu silného ověření uživatele, vývoji jeho právní úpravy, jejímu srovnání na unijní a české úrovni a poté rozboru jeho jednotlivých prvků z kategorií znalost, držení a inherence a požadavku na jejich vzájemnou nezávislost. Navazuje část zaměřující se na rozbor jednotlivých situací, při nichž je osobám oprávněným poskytovat platební služby stanovena povinnost použít silné ověření uživatele. Součástí této části je taktéž výčet všech devíti výjimek z povinnosti vyžadovat silného ověření uživatele.

V poslední části se autor nejprve věnuje tématu behaviorální biometrie, jejím druhům a rozboru jejích kladů a záporů. Poté následuje analýza stávající i možné budoucí role behaviorální biometrie v souvislosti se silným ověřením uživatele a bezpečností elektronického platebního styku. Dále autor rámcově srovnává jednotlivé úpravy ve vybraných státech mimo Evropskou unii a na těchto příkladech ilustruje roli silného ověření uživatele v mezinárodním měřítku. Na toto srovnání mezinárodních úprav navazuje analýza některých úskalí stávající právní regulace a úvahy nad možnostmi jejich řešení. Závěrem se poté autor věnuje analýze dopadů zavedení této právní úpravy a jejím dopadům na oblast elektronického platebního styku.

Klíčová slova:

dvoufázové ověření, silné ověření uživatele, bezpečnost v elektronickém platebním styku

Legal regulation of the strong customer authentication

Abstract

The subject of this rigorous thesis is the legal regulation of strong customer authentication. Its aim is to create an overview of the existing legal regulation of strong user authentication, to point out the shortcomings of this regulation, to propose related solutions and to evaluate the impact and effectiveness of its adoption. In the introductory part, the author first describes the existing legal regulation of payment transactions, the types of payment systems under which electronic payments are settled and analyses the individual payment services under the Czech payment transactions act and the persons authorized to provide them. The author concludes this section with a brief historical development of the regulation and an overview of the effective legislation in this area both in the Czech Republic and the European Union.

In the next part, the author discusses the concept of strong customer authentication, the development of its legal regulation, its comparison at the EU and Czech level and then analyses its individual elements from the categories of knowledge, possession and inherence and the requirement for their mutual independence. This is followed by an analysis of the specific situations in which people authorized to provide payment services are obliged to use strong customer authentication. This section also includes a list of all nine exceptions to the strong customer authentication obligation.

In the last part, the author first discusses the topic of behavioral biometrics, its types and provides an analysis of its pros and cons. This is followed by an analysis of the current and potential future role of behavioral biometrics in the context of strong user authentication and electronic payments security. Next, the author makes a framework comparison of the different legal regimes in countries outside the EU to illustrate the international role of strong customer authentication. The comparison of international regulations is followed by an analysis of some of the pitfalls of the current legal regulation and reflections on viable solutions. Finally, the author then analyses the impact of the introduction of this legislation and its implications for the field of electronic payments.

Key words:

Two-factor authentication, strong customer authentication, electronic payments security