semptembar 2022
godina 15, broj 58

Udruženje banaka
Crne Gore

Association of
Montenegrin Banks

Bankar

ISSN 1800-7465

Štedi vrijeme i novac

NLB **Klik**

Banka je uvijek sa vama, samo kliknite.

Brzo i bezbjedno plaćajte preko NLB Klik mobilnog bankarstva.

Saznajte više na
www.nlb.me

Za sve što dolazi.

NLB Banka

Uvodna riječ glavnog urednika

Poštovani čitaoci,

Pred nama je još jedan broj časopisa Bankar, sa temama koje su aktuelne u poslovanju banaka. Izabrani su tekstovi autora koji se bave zelenom energijom u finansijama odnosno ekološki održivim razvojem i prosperitetom, ali i otvorenim bankarstvom, ili PSD2 direktivom gdje regulativa za cilj ima podstaknuti tehnološke inovacije i njihovu implementaciju u sistem monetarnih transakcija. Konciznim tekstom obrađene su psihološki i operativno prevarne radnje u finansijama sa posebnim osvrtom na bankarsko poslovanje. Iz Letonije imamo upozorenje da je lažne telefonske pozive "iz banke" primilo 55% Letonaca. Ukupno je 2021. godine u četiri najveće banke u Letoniji otkriveno 3.180 slučajeva telefonskih prevara, kojima je ukradeno 4.950.333 eura. Interesantan tekst imamo u vezi stava Vrhovnog suda EU koji je pooštrio smjernice o čuvanju podataka u borbi protiv kriminala.

Koliko su inovacije prisutne možemo vidjeti iz teksta Udruženja banaka Češke gdje umjesto broja računa u internet, ili mobilnom bankarstvu, dovoljno će biti unijeti broj mobilnog telefona primaoca uplate. Upoznajemo vas i sa razmatranjem Švajcarskog parlamenta u tretiranju bankarske tajne. Špansko Udruženje banaka upozorava da egzogeni faktor kao što je rat, ili kontinuirani rast cijena energije povlači za sobom kratkoročna ograničenja ponude i tražnje, sa većom neizvjesnošću za budućnost, odnosno kada i najbolje finansiranje nije dovoljno. Sa druge strane iz Italijanskog Udruženja banaka zahtjevaju da se banke ne opterećuju dodatnim kapitalnim zahtjevima uz kreiranje pravila za održivo finansiranje, važnost kompletiranja Bankarske unije i Unije tržišta kapitala na "pragmatičniji" način. Pažnju na sebe skreće tekst koji ukazuje na tradicionalne funkcije novca kao što su standard vrijednosti, posrednik razmjene i rezerva vrednosti, u širem okviru i uloga monetarne inovacije, kriptovaluta i identifikaciju, četvrtu funkciju novca.

Sigurni smo da će kako profesionalci iz banaka, tako i naši čitaoci iz drugih sfera života, naći tekstove koji mogu obogatiti ugao posmatranja u bankarskom poslovanju.

S poštovanjem,
Glavni i odgovorni urednik
mr Bratislav Pejaković

Foreword of the Secretary General

Dear Readers,

We present another issue of the magazine Bankar, with topics that are current in the banking business. The articles of this issue are dealing with, inter alia, green energy in finance, i.e. ecologically sustainable development and prosperity, open banking, and PSD2 directive, where the regulation aims to encourage technological innovations and their implementation in the system of monetary transactions. Fraudulent activities in finance are featured in another article, psychologically and operationally, paying special attention on banking operations. A warning from Latvia says that 55% of Latvians have received fake phone calls "from the bank". In total, in 2021, 3,180 cases of telephone fraud were detected in the four largest banks in Latvia, from which 4,950,333 euros were stolen. We also bring you an interesting article on the position of the EU Supreme Court, which tightened the guidelines on data retention in the fight against crime.

The article brought to you by the Czech Banking Association shows the importance of innovations nowadays, where instead of the account number required for internet or mobile banking, it will be enough to enter the mobile phone number of the recipient of the payment. We also introduce you to the consideration of the Swiss Parliament in the treatment of bank secrecy. The Spanish Association of Banks warns that an exogenous factor such as war, or the continuous rise in energy prices entails short-term restrictions on supply and demand, with greater uncertainty for the future, i.e., when even the best financing is not enough. On the other hand, the Italian Banking Association demands that banks should not be burdened with additional capital requirements while creating rules for sustainable financing, as well as the importance of completing the Banking Union and the Capital Market Union in a more "pragmatic" way. The next article draws attention to the traditional functions of money such as the standard of value, the medium of exchange and reserve of value, as well as the role of monetary innovation in a broader framework, cryptocurrencies and the identification as the fourth function of money.

We are confident that both the bankers and our readers from other spheres of life will find articles that can enrich the angle of observation in banking business.

With respect,
Editor-in-Chief
Bratislav Pejaković, MSc

BANKAR
Broj 58 / septembar 2022.

IZDAVAČ
Udruženje banaka Crne Gore
Novaka Miloševa bb/3 Podgorica
Tel: +382 20 232-028
www.ubcg.info

Časopis izlazi kvartalno u elektronskoj formi.

Rješenjem Ministarstva kulture, sporta i medija časopis Bankar je upisan u Evidenciju medija - štampani mediji 17. marta 2008, pod rednim brojem 641.

Prilozi
- tekstovi se dostavljaju u elektronskom obliku na e-mail adrese: udruzenjebanaka@t-com.me, gorankapor@hotmail.com; maksimalna dužina teksta do 25.000 karaktera.
- reklame po normativima UBCG na e-mail: latkovic@gmail.com

BANKAR
Časopis Udruženja banaka Crne Gore
Broj 58 / septembar 2022.

Sadržaj / Contents

Rens van Tilburg, direktor Laboratorije za održive finansije na Univerzitetu Utreht

Banke da pređu sa analize na akciju

Rens van Tilburg, direktor Laboratorije za održive finansije na Univerzitetu Utreht, smatra da 2022. godina predstavlja godinu klimatske istine. Finansijske institucije će ove godine izraditi akcione planove o tome kako će svoje bilanse uskladiti sa Pariskim klimatskim ciljevima za 2030. Mapiranje klimatskih i ekoloških rizika koje klijenti – a samim tim i banke imaju – igra glavnu ulogu.

Banke su na dobrom putu, kaže Van Tilburg: „Ali neka banke sada uglavnom pripisuju više posljedica svemu što već znamo. Banke se opraštaju od kompanija koje se ne slažu sa tranzicijom održivosti, već su još uvijek previše ograničene, a cijene klimatskih rizika treba da budu mnogo veće."

Poplave, oluje sa gradom, suše, šumski požari, propadanje usjeva... Klimatske promjene i degradacija životne sredine nanose konkretnu, fizičku štetu kompanijama i domaćinstvima, što se pretvara u rizik za finansijera. Zbog istih klimatskih promjena i degradacije životne sredine, mnoge kompanije moraju sada da ulažu kako bi mogle da nastave (održivo) poslovanje na dugi rok – to su takođe rizici i za finansijera.

„Finansijske institucije će ove godine izraditi akcione planove o tome kako će svoje bilanse uskladiti sa Pariskim klimatskim ciljevima za 2030.

Pitanje kako tačno takvi klimatski i ekološki rizici utiču na bilanse banaka – to pitanje jedva da se dugo postavljalo, počinje Rens van Tilburg: „Kao nezavisna grupa naučnika, Laboratorija za održive finansije može da postavi i pokuša da odgovori na tako teška pitanja. Stoga, mi smo 2013. godine istraživali ideju o„balonu ugljendioksida“: ako pretpostavimo da u jednom potezu idemo u održivi svijet, šta se onda događa s vrijednošću kompanija za plin, ugalj i naftu? Razvili smo scenarije i mapirali koje bi banke u Evropi mogle biti pogođene time.“

OGROMAN UTICAJ

Van Tilburg: "Predvidjeli smo ogroman uticaj. Takođe smo vidjeli da mnoge finansijske institucije ne uzimaju u obzir predstojeću tranziciju održivosti. Na primjer, ako pogledate kreditnu sposobnost velike naftne kompanije, velika je razlika da li pretpostavljate da kompanija može da podigne sve akcije u zemlji i da ih proda. Ili da to nije moguće jer dolazi do prevelikog ispuštanja CO2 u vazduh, tako da ne možemo ostvariti pariške klimatske ciljeve. U međuvremenu su takve kompanije cijenjene na berzama i njihova kreditna sposobnost se procjenjuje pod pretpostavkom da su sve te akcije prodate."

„Naš zaključak u to vrijeme je bio da finansijske institucije poklanjaju premalo pažnje uticaju tranzicije

Rens van Tilburg, director
of Sustainable Finance Lab at Utrecht University

Banks to move from analysis to action

2022 is the year of climate truth, according to Rens van Tilburg, director of the Sustainable Finance Lab at Utrecht University. This year, financial institutions will come up with action plans on how they will bring their balance sheets in line with the Paris Climate Goals for 2030. Mapping climate and environmental risks that customers – and therefore banks – run plays a major role.

Banks are on the right track, says Van Tilburg: "But let banks now mainly attach more consequences to everything we already know. Banks are saying goodbye to companies that do not go along with the sustainability transition. But still too limited and climate risks need to be priced much more."

Floods, hailstorms, drought, forest fires, crop failures... Climate change and environmental degradation cause concrete, physical damage to businesses and households, which translates into risks for the financier. Due to the same climate change and environmental degradation, many companies have to invest now in order to be able to continue to do business (sustainably) in the long term – these are also risks for the financier in question.

The question of how exactly such climate and environmental risks affect the balance sheets of banks - that question was hardly asked for a long time, rens van Tilburg begins: "As an independent group of scientists, the Sustainable Finance Lab is able to ask and try to answer such difficult questions. In 2013, we therefore investigated the idea of the 'carbon bubble': suppose we go to a sustainable world in one go, what happens to the value of gas, coal and oil companies? We developed scenarios and mapped out which banks in Europe could be affected."

HUGE IMPACT

Van Tilburg: "We foresaw a huge impact. And also saw that many financial institutions do not take into account the upcoming sustainability transition. For example, if you look at the creditworthiness of a large oil company, it makes quite a difference whether you assume that the company can bring up all the stocks in the ground and sell them. Or that that is not possible, because too much CO2 goes into the air, so that we cannot achieve the Paris Climate Goals. In the meantime, such companies are valued on the stock exchanges and their creditworthiness is estimated on the assumption that all those stocks are sold."

"Financial institutions pay too little attention to the impact of the sustainability transition on their balance sheets, was our conclusion at the time. Supervisory

„This year, financial institutions will come up with action plans on how they will bring their balance sheets in line with the Paris Climate Goals for 2030

6 *„Postoje određene kompanije od kojih se banke sada opraštaju zbog ekoloških i/ili klimatskih rizika. Međutim, to je još uvijek vrlo ograničeno, a cijene klimatskih rizika rijetko se određuju*

održivosti na njihove bilanse. Nadležni organ Centralne banke Holandije (DNB) za superviziju brzo je shvatio da se ovo pitanje dotiče njihove primarnefunkcije: osigurati da banke takođe pravilno upravljaju ovim rizicima. DNB je sproveo istragu i Evropski nadležni organ za ECB superviziju je prije dvije godine izrazio svoja očekivanja o načinu na koji banke oblikuju svoje upravljanje klimatskim rizicima. U svom nedavnom izvještaju, ECB je pokazala kako više od 100 najvećih banaka u Evropi rade: nijedna od tih banaka ne radi sasvim kako treba, 20% ne radi baš ništa i nema planova da to poboljša."

IZNENAĐEN

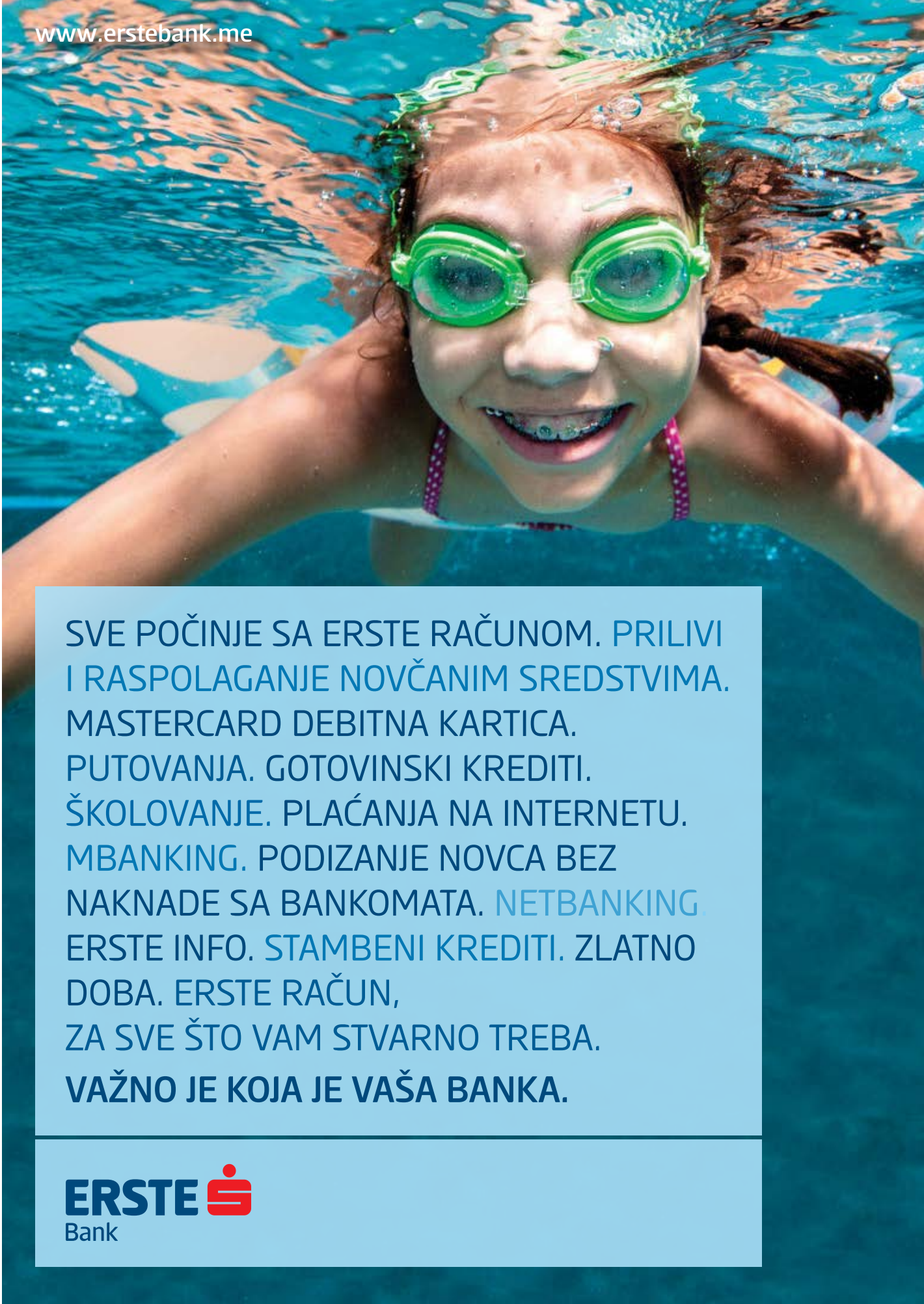
Van Tilburg: "Bio sam prilično iznenađen ovim procentima. O ovoj temi govorimo već godinama. Postoje mnoge studije i odavno se zna koji su najveći rizici u ovoj oblasti. Podaci i metode još nijesu savršeni, ali počnimo pripisivati posljedice svemu što već znamo. Postoje određene kompanije od kojih se banke sada opraštaju zbog ekoloških i/ili klimatskih rizika. Međutim, to je još uvijek vrlo ograničeno, a cijene klimatskih rizika rijetko se određuju. Iako je upravljanje rizicima osnovna nadležnost banaka,očekivanja nadležnih organa za superviziju takođe pružaju dovoljne smjernice. A na raspolaganju su bezbrojne metode i instrumenti. Dakle, to nije ono što koči banke. Ipak, zasad samo je sektor uglja rekao zbogom. Ali razvijanje novih polja u blizini nafte i plina takođe nije kompatibilno sa Klimatskim sporazumom. Prema tome, ne treba da to finansirate zbog tranzicionih rizika kojima se tada izlažete. U okviru sektora se zna i što su zeleni predvodnici, a što fosilni zaostaci. Proizvođač automobila koji je propustio električnu revoluciju zaslužuje uz odobreni kredit pozamašnu dodatnu premiju za tranzicioni rizik. Isto važi i za mala i srednja preduzeća, uključujući poljoprivredu, za kompanije koje imaju relativno visoke emisije. Banke se i dalje previše ugledaju jedni na druge. Od pomisli: ako budem vodeći, onda bih mogao propustiti prihod koji imaju konkurenti, pa što svijet na kraju ima od toga? Neću to učiniti dok i ti to ne učiniš. Stoga bih očekivao da će holandske banke zatražiti od ECB-a da strože prati upravljanje klimatskim rizikom. Ovo stavlja konkurenciju koja još uvijek ulaže kao da se klimatske promjene ne događaju u nepovoljan položaj i time povećava opseg za sprovođenje dobrog upravljanja rizicima."

AMBICIJA JE DOBRA

Van Tilburg pozitivno gleda na saradnju finansijskog sektora u okviru Finansijskog sektora za klimatske obaveze koji je izdat 2019. godine: „Ambicija je dobra. Ali sada vidim i banke koje se bore s pitanjem kako će ispuniti postavljene klimatske ciljeve. Ovo se može vidjeti i u prvom izvještaju o napretku prošle godine. Stoga će 2022. godina predstavljati godinu klimatske istine. Tada finansijske institucije donose akcione planove o tome kako će razvijati svoje bilanse u skladu sa onim što je potrebno za postizanje Pariskih klimatskih ciljeva. Zatim mora biti jasno šta će to značiti u smislu emisije CO2 kompanija koje finansiraju banke.I veoma važno: koje će akcije banke preduzeti u tom cilju.Možemo li podstaknuti kompanije da smanje emisiju CO2 ili ćemo reći zbogom njima?"

GRANICA

„Kao svijet, moramo učiniti sve što možemo da ograničimo klimatske i ekološke rizike što je više moguće. Banke igraju važnu ulogu u tome. Od banaka se može očekivati da gledaju naprijed, vide rizike i procjenjuju ih. Tako da klijenti ovdje i sad shvate: ej bolje je sada da preduzmemo mjere kako bi počeli da poslujemo na održiv način. Ili da stavimo solarne panele na krov. Banke su pokazale da to mogu. Na primjer, sa obavezom stavljanja oznake C od 2023. godine na komercijalne nekretnine koje finansiraju. Banke bi takođe mogle da preuzmu vođstvo kada je riječ o održivosti malih i srednjih preduzeća. U isto vrijeme, postoji i ograničenje onoga što banke mogu učiniti. Propisi bi bili od velike pomoći, kao što je obavezna energetska oznaka skok prilikom selidbe – pitanje koje sve više postavlja Udruženje banaka Holandije. Svakako je potrebno više vladinih akcija da bi se ova tranzicija dogodila."


www.erstebank.me
SVE POČINJE SA ERSTE RAČUNOM. PRILIVI I RASPOLAGANJE NOVČANIM SREDSTVIMA. MASTERCARD DEBITNA KARTICA. PUTOVANJA. GOTOVINSKI KREDITI. ŠKOLOVANJE. PLAĆANJA NA INTERNETU. MBANKING. PODIZANJE NOVCA BEZ NAKNADE SA BANKOMATA. NETBANKING. ERSTE INFO. STAMBENI KREDITI. ZLATNO DOBA. ERSTE RAČUN,
ZA SVE ŠTO VAM STVARNO TREBA.
VAŽNO JE KOJA JE VAŠA BANKA.
ERSTE
Bank


Zapad Banka
GOTOVINSKI
NENAMJENSKI
KREDIT
• Fiksna kamatna stopa
• Jednostavna procedura
• Brza realizacija
do 25.000 EUR
do 96 mjeseci
+382 20 69 0000
info@zapadbanka.me
www.zapadbanka.me

authority De Nederlandsche Bank (DNB) quickly realised that this issue touches on their primary mandate: to ensure that banks also manage these risks properly. DNB conducted an investigation and the European supervisory authority ECB expressed its expectations two years ago about the way in which banks shape their climate risk management. In its recent report, the ECB showed how the more than 100 largest banks in Europe are doing: none of those banks are doing quite right, 20% are doing nothing at all and have no plans to improve it."

„Banks are saying goodbye to companies that do not go along with the sustainability transition. But still too limited and climate risks need to be priced much more

SURPRISED

Van Tilburg: "I was quite surprised about these percentages. We've been talking about this topic for years now. There are many studies and it has long been known what the biggest risks in this area are. The data and methods are not yet perfect, but let's start attaching consequences to everything we already know. There are certain companies that banks are now saying goodbye to because of the environmental and/or climate risks. But it is still very limited and the pricing of climate risks is only done sparsely. While managing risks is the core competence of banks. The expectations of the supervisory authorities also provide sufficient guidance. And there are countless methods and instruments available. So that's not what's holding banks back. Yet, for the time being, only the coal sector has said goodbye. But developing new fields near oil and gas is also incompatible with the Climate Agreement. So you should not want to finance that because of the transition risks that you then run. Within sectors, it is also known what the green frontrunners are and what the fossil laggards are. Credit for a car manufacturer that is missing the electric revolution deserves a hefty extra transition risk premium. The same applies to SMEs, including agriculture, for companies that have relatively high emissions. Banks still look at each other too much. From the thought: if I lead the way, then I might miss out on income that competitors do have, so what does the world ultimately get out of that? I won't do it until you do it too. I would therefore expect the Dutch banks to ask the ECB to monitor climate risk management more strictly. This puts the competition that still banks as if there is no climate change going on at a disadvantage and thus increases the scope to conduct good risk management itself."

AMBITION IS GOOD

Van Tilburg is positive about the cooperation of the financial sector within the Climate Commitment Financial Sector that was issued in 2019: "The ambition is good. But I now also see banks struggling with the question of how they will meet the set Climate Goals. This is also visible in the first progress report last year. 2022 will therefore be the year of climate truth. Then financial institutions come up with action plans on how they will develop their balance sheets in line with what is needed to achieve the Paris Climate Goals. Then it must become clear what that will mean in terms of the CO2 emissions of companies that are financed by banks. And very important: what actions banks will take to this end. Can we encourage companies to reduce CO2 emissions or are we going to say goodbye to them?"

BOUNDARY

"As a world, we must do everything we can to limit climate and environmental risks as much as possible. Banks play an important role in this. Banks can be expected to look ahead, see risks and price them. So that customers in the here and now realize: hey, it's better to take measures now. To start doing business sustainably now. Or to put solar panels on my roof. Banks have shown that they can do it. For example, with the Label C obligation from 2023 on commercial real estate financed by them. Banks could also take more of the lead when it comes to making SMEs more sustainable. At the same time, there is also a limit to what banks can do. Regulations would help enormously, such as a mandatory energy label jump when moving house – something that is increasingly being raised by the Dutch Banking Association. More government action is certainly needed to make this transition happen."

Miodrag Džodžo,
ABC TECH

PSD2 u Crnoj Gori

ABC TECH je vodeći regionalni provajder naprednih bankarskih rješenja, i prvi je na području Republike Hrvatske napravio zaokruženo PSD2 rješenje koje je sada u primeni u dvije banke (Partner banka i Nova Hrvatska banka). U tijeku je implementacija ovog rješenja u Slatinskoj banci. ABC TECH Rješenje PSD2 u celosti ispunjava rigorozne standarde ove direktive i dobilo je saglasnost Hrvatske Narodne Banke za upotrebu u bankarskom sistemu Republike Hrvatske.

„Druga Direktiva o platnim uslugama (PSD2) usvojena je prvenstveno zbog poticanja tehnološkog napretka i rješavanja pitanja besprijekornih i sigurnih platnih usluga

U sklopu konstantne težnje za unapređenjem EU tržišta financijskih usluga, od strane EK donesena je druga Direktiva o platnim uslugama na unutrašnjem tržištu (PSD2) usvojena prvenstveno zbog poticanja tehnološkog napretka odnosno radi rješavanja pitanja besprijekornih i sigurnih platnih usluga. Regulativa je za cilj imala potaknuti tehnološke inovacije i njihovu implementaciju u sistem monetarnih transakcija. Ovim su, pored uspostavljanja boljih sigurnosnih zahtjeva i poboljšanja zaštite korisnika platnih usluga, uvedena i regulisana dva nova osnovna platna servisa za sudionike izvan bankarskog sistema koja bankama sudionicama na tržištu EU mandatira otvaranje pristupa tekućim računima fizičkih i pravnih osoba:

- Usluge iniciranja plaćanja (PIS)
- Informacijske usluge računa plaćanja (AIS)

Informacijske usluge o platnom računu omogućava certificiranim entitetima (AISP) da krajnjim korisnicima nude agregirane – objedinjene informacije o jednom ili više računa za plaćanje koje vodi nekoliko pružatelja platnih usluga, a kojima se može pristupiti putem interneta preko interfejsa pružaoca platnih usluga. Korisniku platnih usluga je na taj način omogućen potpuni pregled cjelokupne finansijske situacije sa svih platnih računa koje korisnik posjeduje, ali je istovremeno omogućeno kreiranje novih usluga na tržištu gdje se ponajviše ističe usluga jednostavnijeg kreditnog skoringa analizom sada lako dostupnih podataka o korisnikovom tekućem računu (uz pristanak korisnika naravno).

PSD2 in Montenegro

ABC TECH is the leading regional provider of advanced banking solutions, and the first in the Republic of Croatia to create a comprehensive PSD2 solution that is now in use in two banks (Partner banka and Nova Hrvatska banka). The implementation of this solution is underway in Slatinska banka. ABC TECH Solution PSD2 fully meets the rigorous standards of this directive and has been authorised by the Croatian National Bank for use in the banking system of the Republic of Croatia.

Miodrag Jojo,
ABC TECH

As a part of the constant effort to improve the EU market of financial services, the second Directive on payment services in the internal market (PSD2) was adopted by the EC, primarily to encourage technological progress, i.e., to solve the issue of seamless and secure payment services. The aim of the regulation was to encourage technological innovations and their implementation in the system of monetary transactions. In addition to establishing better security requirements and improving the protection of payment service users, two new basic payment services for participants outside the banking system were introduced and regulated, which mandates banks participating in the EU market to open access to the current accounts of natural and legal persons:

▹ Payment Initiation Services (PIS)
▹ Payment Account Information Services (AIS)

Payment account information services enable certified entities (AISP) to offer end-users aggregated - consolidated information about one or more payment accounts maintained by several payment service providers, which can be accessed online through the payment service provider's interface. In this way, the user of payment services is provided with a complete overview of the entire financial situation from all the payment accounts that the user owns, but at the same time it is possible to create new services on the market, where the service of simpler credit scoring by analysing the now easily available data on the user's current account (with consent of the user) stands out.

„The Second Payment Services Directive (PSD2) was adopted primarily to encourage technological progress and to address the issue of seamless and secure payment services

„Banke koje se usklade sa PSD2 moraće da "otvore" svoja sučelja aplikacijskih programa novim provajderima platnih usluga, koji će moći pristupiti informacijama o korisničkom računu

Usluge iniciranja plaćanja omogućavaju nalogodavcu (kupcu) direktno pozivanje plaćanja sa svog računa putem PISP-a, bez posrednika u plaćanju (kao što su danas kartične kuće). U praksi to znači da se kroz navedenu regulativu sami trgovci mogu registrovati kao pružatelji servisa plaćanja u svoje ime, te vršiti plaćanja bez ikakvih posrednika, i što je najvažnije: bez naknada. Kod kupovine nekog artikla na web shop-u, Trgovac će inicirati transfer sredstava sa računa kupca na svoj račun, bez posrednika.

Uvođenjem novih platnih usluga, tržište je otvoreno za nove pružaoce usluga: pružaoce usluga inicijacije plaćanja (PISP) i pružaoce **usluga provajdera informacija o računu** (AISP).

Do sada su pristup podacima o korisničkom računu bile isključivo u vlasništvu banaka. Međutim, banke koje se usklade sa PSD2 će morati da "otvore" svoja sučelja aplikacijskih programa novim provajderima platnih usluga, koji će moći pristupiti informacijama o korisničkom računu (**samo putem ovog kanala**), pregledavati plaćanja i izdavati potvrde o stanju. Istovremeno, sigurnost pružanja ovih usluga strogo je regulirana tako da podaci ili resursi korisnika nisu ugroženi.

Takođe, PSD2 je uveo stroge sigurnosne zahtjeve za **pokretanje i obradu elektronskih platnih transakcija**. Ova direktiva usmjerava pružaoce platnih usluga da primjenjuju takozvanu "**Strong Customer Authentication (SCA)**" kada platilac inicira transakciju elektronskog plaćanja jer će to bolje zaštititi njihove podatke i smanjiti rizik od prevare.

Stoga će banke i drugi pružaoci platnih usluga morati da uspostave **i potrebnu infrastrukturu za jaču autentifikaciju korisnika.** Pored viših sigurnosnih zahtjeva, od provajdera platnih usluga se traži da upravljaju povezanim operativnim i sigurnosnim rizicima i prijavljuju incidente u vezi s tim. Uveden je rok za odgovaranje na pritužbe potrošača i skraćen rok (sa 12 na šest mjeseci) nakon kojeg korisnik platnih usluga može bez naknade otkazati okvirni ugovor.

Ova direktiva takođe identifikuje i detaljnije usluge koje nisu kategorisane kao usluge plaćanja. **Primjeri uključuju usluge kolektivne kupovine i trgovačke kartice** koje se mogu koristiti u ograničenoj mreži (poput kupovine u pojedinačnim trgovinama, maloprodajnim lancima i još mnogo toga).

Koji je krajnji benefit za Banke? Prvenstveno u kvalitetnijem screeningu potencijalnih novih klijenata kroz AIS uslugu, te predstavljanje novih i inovativnih usluga kroz PIS, gdje u suradnji s trgovcima mogu ostvariti razne benefite korištenjem direktnih sistema plaćanja bez kartičnih posrednika. Ali uzevši u obzir otvorenost sistema i napredne sigurnosne zahtjeve, mogućnosti inovacija su nebrojene.

Predloženi Zakon o izmjenama i dopunama Zakona o platnom prometu Crne Gore vodi ka usklađivanju sa opisanom PSD2 regulativom, uvode se novi provajderi platnih usluga, podstiče se tržišna konkurentnost, **omogućava dalji razvoj inovativnog mobilnog i internet platnog prometa**, povećava se sigurnost za elektronska plaćanja i pružatelje platnih usluga i očekuje se smanjenje cijene usluga platnog prometa za krajnje korisnike uz jednostavan, pristupačan i inovativan način plaćanja.


Uvijek otvorena banka
u tvom telefonu!
Izaberi Prva m-banking
PRVA BANKA CG
OSNOVANA 1901
ISKUSTVO ZA NOVO VRIJEME
Download on the
App Store
GET IT ON
Google Play

GOTOVINSKI KREDITI

Još povoljnije kamatne stope i duži rok otplate

ODOBRENJE U ROKU OD 24h

LOVĆEN BANKA AD

Kontakt centar: 19 993

Payment initiation services enable the principal (customer) to directly call payment from his account via PISP, without payment intermediaries (such as card houses today). In practice, this means that through the aforementioned regulation, merchants themselves can register as payment service providers in their own name, and make payments without any intermediaries, and most importantly: without fees. When purchasing an item on the web shop, the Merchant will initiate the transfer of funds from the customer's account to his account, without an intermediary.

With the introduction of new payment services, the market is opened to new service providers: Payment Initiation Service Providers (PISPs) and Account Information Service Providers (AISPs).

Until now, access to user account data was exclusively owned by banks. However, banks that comply with PSD2 will have to "open up" their application program interfaces to new payment service providers, who will be able to access customer account information (only through this channel), review payments and issue balance confirmations. At the same time, the security of the provision of these services is strictly regulated so that the user's data or resources are not endangered.

Also, PSD2 introduced strict security requirements for the initiation and processing of electronic payment transactions. This directive directs payment service providers to apply the so-called "Strong Customer Authentication (SCA)" when the payer initiates an electronic payment transaction, as this will better protect their data and reduce the risk of fraud.

Therefore, banks and other payment service providers will have to establish the necessary infrastructure for stronger user authentication. In addition to higher security requirements, payment service providers are required to manage the associated operational and security risks and report related incidents. A deadline for responding to consumer complaints was introduced a shortened deadline (from 12 to six months) after which the payment services user can cancel the framework agreement free of charge.

This directive also identifies in more detail services that are not categorized as payment services. Examples include collective purchasing services and merchant cards that can be used in a limited network (such as shopping at individual stores, retail chains, and more).

What is the ultimate benefit for Banks? Primarily in the better screening of potential new clients through the AIS service, and the presentation of new and innovative services through PIS, where in cooperation with merchants they can achieve various benefits by using direct payment systems without card intermediaries. But given the openness of the system and advanced security requirements, the possibilities for innovation are endless.

The proposed Law amending the Payment System Law of Montenegro leads to harmonization with the described PSD2 regulation, introduces new payment service providers, encourages market competition, enables further development of innovative mobile and internet payment transactions, increases security for electronic payments and payment service providers and the price of payment services for end users is expected to decrease with a simple, accessible and innovative payment method.

„Banks that comply with PSD2 will have to "open up" their application program interfaces to new payment service providers, who will be able to access customer account information

, generalni sekretar
Udruženja banaka
Crne Gore

Uzroci prevarnih radnji

Pritisak je nužni prvi korak koji uzrokuje da pojedinac ozbiljno razmišlja o prevari. Pritisci na prevaru često uključuju finansijske probleme: život iznad vlastitih mogućnosti, pohlepa, visok lični dug, slab kredibilitet lica, računi za liječenje, investicioni gubici, troškovi za školovanje djece, podcjenjivanje sposobnosti lokalnog supervizora itd. Prevara u finansijskim izvještajima često je vezana uz direktan pritisak, kao ostvarivanje targeta, ili kvalificiranje za bonuse.

„Pritisci na prevaru često uključuju finansijske probleme: život iznad vlastitih mogućnosti, pohlepa, dugovi, gubici, računi za liječenje, školovanje djece, itd.

Podsticaji, motivi prevarnih radnji, koji mogu biti raznih osnova, obično se realizuju potenciranjem velikog istraživanja i razvoja, kroz kapitalne investicije, plaćanjem dobavljača iznad tržišnih cijena, plaćanjem nerealizovanih, ali registrovanih obaveza, kroz novo vlasničko ulaganje i slično. Potom u dijelu kreditnih transakcija, može biti prevarna radnja u smislu odobravanje kredita bez obezbjeđenja koji se ispostave delikventnim, odobravanje kredita bez provjere istinitosti priložene dokumentacije, falsifikovanje pečata kompanija sa kojim se posluje, gdje mogu biti čak falsifikati pečata ministarstava (npr. ministarstava unutrašnjih poslova i odbrane, ili elektroprivrede, ili nekih telekomunikacionih kompanija gdje aplikanti nikad nijesu registrovani kao uposleni u tim firmama), gdje se odobre zajmovi po osnovu falsifikovanih dokumenata, milionskih vrijednosti u eurima.

Potom, prevarne radnje mogu biti kroz smanjenje, ili povećanje rezervacija na postojeći portfolio i time lažno prikazivanje mimo realnog rezultata, kao i

Bratislav Pejaković, Secretary General
Association of Montenegrin Banks

Causes of Fraudulent Activities

The pressure is crucial first step causing an individual to seriously consider the fraud. The motivation to commit fraud often includes financial problems: living beyond one's means, greed, high personal debt, poor personal credibility, medical bills, investment losses, children's education expenses, underestimating the abilities of the local supervisor, etc. Fraud in financial statements is often related to direct pressure, such as achieving targets or qualifying for bonuses.

Incentives and motives to commit fraudulent activities, which can be of various bases, are usually materialised by emphasizing large-scale research and development, through capital investments, paying the suppliers above market prices, paying unrealized but registered obligations, through new equity investment, and the like. In addition, fraudulent activities can appear in the part of credit transactions in the form of granting loans without security instruments that turn out to be delinquent, or granting loans without verifying the authenticity of the attached documentation, or forging the seals of companies with which we do business, or even forging of seals of ministries or companies (e.g. ministries of the interior and defence, or the electric power company, or some telecommunication companies where applicants have never been registered as employees in those companies). In those cases, loans are granted in millions of euros based on forged documents.

„The motivation to commit fraud often includes financial problems: living beyond one's means, greed, debts, losses, medical bills, children's education expenses, etc.

IZ BIJELE KNJIGE SAVJETA INOSTRANIH INVESTITORA

Zemlje Centralne i Istočne Evrope su se do sada susretale sa raznim modalitetima prevarnih radnji od kojih su najzastupljenije sljedeće: Određeni broj lica se organizuje i registruje firmu, a zatim pronalaze lica koja podnose zahtjeve za odobravanje kredita. Kao pokriće dobijaju potvrde o zaposlenju i visini primanja koje su falsifikat. Obično je i firma fiktivna. Biraju se lica sa društvenih margina, narkomani, lica iz kriminogenih sredina, ucijenjena lica koja pristaju da za relativno nisku nadoknadu obave ovaj posao za organizatora. Kada dobiju kredit takva sredstva se puštaju preko računa te firme kako bi se prikazalo da je račun aktivan. Iz tih sredstava isplaćuju se lica koja su dobila kredit u već ranije dogovorenom iznosu, a onda se obično jedna, ili dvije rate vraćaju, nakon čega se podižu preostala sredstva i gasi se firma.

zloupotrebom pozicija, aktivna i pasivna vremenska razgraničenja, ili kod situacije tzv. TREZOR, blagajna – valuta na putu. Potom, tu su problemi u neadekvatnim procedurama gdje su sumnjive transakcije – sumnja na pranje novca, off shore transakcije, ne dokumentovanost transakcije lokalne i sl. Potom, kastodi usluga sa računima na off-shore destinacijama, napad na račune koji su u stanju mirovanja duži vremenski period i falsifikati potpisa vlasnika računa, uz sledstvenu zloupotrebu službenog položaja i raspolaganjem ovim sredstvima. Kao prevarna radnja koja se odražava na bilanse mogu biti sudski procesi milionskih iznosa gdje su velike šanse za gubitak, ali se kod istog ne daju realne procjene, odnosno rezervacije, gdje pored interne procjene, značajna je i eksterna procjena revizora.

Lažni iskaz može nastati prikazom manjih prihoda,ili rashoda od kamata i naknada, različitih od realnih, ili jačim tarifiranjem od realnog prema izvoru sredstava, ili povećanjem troškova zaposlenih samo računovodstvenim prikazom, čime se značajno može umanjiti dobit, a time i porez. Problem nastaje ukoliko se realno ne prikaže kroz izvještaje, ili se značajno podcjeni, ali može i da se precjeni u zavisnosti od potrebe konkretni računovodstveni iskaz.

Anti Fraud aktivnosti Udruženja, biće pod jačim fokusom od dosadašnjih u cilju preventive dešavanja istih, a time i za očuvanjem finansijskog sistema Crne Gore na kvalitetnijem nivou.

Prevaru mogu izazvati uzastopni negativni tokovi novčani, gdje se menadžment želi prikazati uspješnijim nego što je. Nekompetencija menadžmenta može biti i kroz pogrešnu percepciju kretanja kamata, pa imamo uticaj pada, ili rasta kamatne stope na uspjeh poslovanja – gdje je isto posledica neadekvatnog upravljanja sredstvima, kada imamo i sistuacije da se iz kratkoročnih izvora plasiraju sredstva u dugoročne plasmane, mimo propisanog limita i time se ugrožava likvidnost.

Prevarne radnje izaziva loš rezultat uslijed zastarelosti proizvoda, pad potražnje kupaca u industriji, neuravnotežen bilans, ili neadekvatna struktura portfolija itd. Potom, menadžment zloupotrebljava pravo odluke po pitanju računovodstvenih izbora poput važnih procjena nenaplativih potraživanja, jemstava, garancija koje ne ispunjavaju standard, ili čak nijesu proknjižene, troškova na kraju razdoblja i tako dalje. Prevare u izvještavanju mogu izazvati i pritisak na menadžere, više ili niže rangirane, da ostvare očekivanja, gdje su u realnom poslovanju ispod budžetiranih, projektovanih, ili prognoziranih rezultata. Tu su i transakcije fakturisanja bez isporuka, fiktivna prodaja koja uključuje, ili fantomske kupce, ili stvarne kupce sa lažnim računima koji se knjiže u jednom izvještajnom razdoblju (precjenjivanje) a storniraju u slijedećem izvještajnom razdoblju. Prevarnu radnju mogu izazvati, značajne vanbilansne stavke, ili rezervisanja, visoki krediti pojedinačni, ili

ADRIATIC BANK

SIGURNA I OD POVJERENJA

US OWNED BANK

CAPITAL PLAZA, PODGORICA
ADRIATICBANK.COM

CUSTODY@ADRIATICBANK.COM
INVESTMENTS@ADRIATICBANK.COM
T +382 20 680 973
F +382 20 675 083

VAŠA USPJEŠNA INVESTICIJA, NAŠ JE POSAO
INVESTICIONO BANKARSTVO ADRIATIC BANK

Addiko mKredit

Preko vašeg mobilnog telefona

Bez troška obrade, isplata odmah

Addiko Bank

Gdje je 2+2=4

JER MI CIJENIMO SVOJE KLIJENTE
CUSTOMERS' FRIEND
ADDIKO

Detaljnije na addiko.me

Reprezentativni primjer: Za iznos kredita od 3.000€ sa rokom otplate od 72 mjeseca, nominalna kamatna stopa iznosi od 8,99% na godišnjem nivou, dok efektivna kamatna stopa iznosi od 9,37%. Ukupan iznos koji klijent plaća je 3.892,50€, dok je iznos mjesečnog anuiteta 54,06€. Ukupan iznos koji plaća klijent predstavlja zbir glavnice i ukupne kamate.

Moreover, fraudulent activities can appear through the reduction or the increase of provisions on the existing portfolio, thus falsely showing the real result, as well as through the misuse of financial positions in the balance sheet, prepayments and advances, or though cash register - currency in transit. Problems in inadequate procedures where there are suspicious transactions - suspicion of money laundering, off shore transactions, lack of documentation of local transactions can indicate the fraudulent activities. Other examples where these activities can appear are custody services provided for the accounts at off-shore destinations, attacks on accounts that are dormant for a long period of time and forgery of signatures of account holders, misusing simultaneously the official position and disposal of these funds. Lawsuits of millions of dollars with great chances of loss can appear as a fraudulent activity that is reflected on the balance sheets when realistic estimates or provisions are not given. In such a case, in addition to the internal auditor's assessment, the external auditor's assessment is also important.

A false statement can be created by presenting lower interest and fee income or expenses, which differ from the actual, or by charging tariffs that exceed the realistic according to the source of funds, or by increasing expenses of the employees only by accounting presentation, which can significantly reduce the profit, and thus the tax. The problem arises if it is not realistically presented through reports, or it is significantly underestimated, but it can also be overestimated depending on the need for a specific accounting statement.

Anti-fraud activities of the Association will be under a stronger focus than before in order to prevent them from happening, and thus to preserve the financial system of Montenegro at a higher quality level.

Fraud can be caused by consecutive negative cash flows, where management wants to present itself as more successful than it is. The incompetence of the management can also be through a wrong perception of interest rates, with the impact of a fall or rise in the interest rate on the success of the business, which is a consequence of inadequate management of funds. We also have situations where funds are placed from short-term sources into long-term placements, beyond the prescribed limit, thereby threatening the liquidity.

Fraudulent activities are caused by poor performance due to product obsolescence, decline in customer demand in the industry, unbalanced balance sheet, or inadequate portfolio structure, etc. If a management misuses its decision-making power regarding accounting choices, such as decisions on important estimates of uncollectible receivables, sureties, guarantees that do not meet standard or are not even posted, decision on end-of-period expenses, this can lead to a fraud. Frauds in reporting can also cause pressure on high- or low-ranked managers to achieve expectations, which are below budgeted, projected, or forecasted results in real business. Frauds can be committed when the transactions are invoiced without deliveries, in fictitious sales which involve either phantom customers or real customers with fake invoices that are posted in one reporting period (overstatements) and reversed in the next reporting period. Fraudulent activity can be caused by significant off-balance sheet items or provisioning; by granting loans to individuals in high amounts or to a group of connected persons that exceed statutory limits; high interest rates and reduced ability to obtain

FROM THE WHITE BOOK OF THE FOREIGN INVESTORS COUNCIL

The countries of Central and Eastern Europe have so far encountered various modalities of fraudulent activities, the most common of which are the following: A certain number of persons organize and register a company, and find persons who submit requests for loan approval. As a cover, they receive certificates of employment and amount of income, which are falsified. Usually, the company is also fictitious. People from the social margins, drug addicts, people from criminal environments, blackmailed people are chosen and agree to do this for the organizer for a relatively low compensation When they receive a loan, such funds are disbursed through the company's account in order to show that the account is active. From these funds, the persons who received the loan are paid in the previously agreed amount, and after one or two instalments are being paid, the remaining portion of funds are withdrawn and the company is closed.

„Anti Fraud aktivnosti Udruženja, biće pod jačim fokusom od dosadašnjih u cilju preventive takvih dešavanja

grupi povezanih lica mimo limita zakonskih; visoke kamatne stope i smanjena sposobnost dobijanja kreditne podrške, teškoće u naplati potraživanja, neodgovarajuće rezerve u pogledu mogućnosti naplate, time prikrivanja gubitaka.

Nekad se angažuje eksterni revizor, jer je prepoznat rizik vezan sa ulaganjem, gdje poslovanje nije u skladu sa očekivanjima stope povrata na ulaganja, ili se želi nadzor nad kapitalnim investicijama.

Ne treba zanemariti prevare u kartičarstvu, ili syber napade, koji mogu prouzrokovati milionsku štetu, ali to da se pokuša sakriti kroz izvještaje. Korisnici usluga elektronskog i mobilnog bankarstva širom svijeta mogu dobiti maliciozan e-mail sa instrukcijama za aktivaciju naloga, promjenu lozinke, ili ažuriranje korisničkih podataka.

U budućem radu Udruženja posvetiće se adekvatna pažnja i moralnom hazardu na nivou sistema, kao što je istaknuto na zadnjem sastanku sa predstavnicima CBCG.

Pored prikazanog, različitost tumačenja od strane Uprave prihoda od tumačenja u samim bankama, može uzrokovati promjene u računovodstvenim iskazima, a time i u Bilasnu uspjeha. Naime, Poreska uprava može dovesti u pitanje ispravnost tekućeg obračuna poreza na dobit, sa aspekta sredstava rezervi na kontu 3025 iz 2013. Možemo tumačiti da je obaveza zastarjela uz stav da je svrha ovih sredstava funkcionalnih rezervi koje su služile kao prudencioni filter. Poreska uprava smatra da su otpisi poreski priznati samo ako su svi postupci prinudne naplate završeni, uključujući i nemogućnost unovčavanja kolaterala i okončani stečajni postupci. PU se pri tom poziva na čl.17. stav 1 tačka 3 Zakona o porezu na dobit pravnih lica. Pored toga stoji komentar, stav bankarske struke da PU ne bi trebala da tumači kako je prezentovano. Međutim, imamo stavove i da neki drugi organ po drugoj osnovi može tražiti naplatu i odgovornost, tužilaštvo… Tumačenja računovodstvenih i finansijskih iskaza variraju od ugla gledanja.

„U budućem radu Udruženja posvetiće se adekvatna pažnja i moralnom hazardu na nivou sistema, kao što je istaknuto na zadnjem sastanku sa predstavnicima CBCG

„Anti-fraud activities of the Association will be under a stronger focus than before in order to prevent them from happening

credit support; difficulties in collecting receivables; inadequate provisions regarding the possibility of collection, thereby concealing losses.

Sometimes an external auditor is engaged, because the risk associated with the investment is recognized, where the business is not in accordance with the expectations of the rate of return on investments, or the control of capital investments is desired.

We should not ignore fraud in the payment cards sector, or cyber-attacks that can cause millions of dollars in damage, and the attempt to hide it through reports. Users of electronic and mobile banking services around the world may receive a malicious e-mail with instructions for activating an account, changing a password, or updating user data.

The Association will pay special attention in the future to moral hazard at the system level, as it was pointed out at the last meeting with the CBCG representatives.

In addition to above-mentioned, the difference that exists in interpretation between the Tax Administration and the banks, can result in changes in the accounting statements, and thus in the income statement. Namely, the Tax Administration may question the correctness of the current calculation of income tax from the aspect of reserves shown at the accounts account number 3025 from 2013. We can interpret that the obligation is outdated with the view that the purpose of these funds are functional reserves that served as a prudential filter. The Tax Administration considers that write-offs are tax-recognized only if all forced collection procedures have been completed, including the impossibility of cashing in the collateral and completed bankruptcy procedures. Tax Administration refers to Article 17 paragraph 1 point 3 of the Law on corporate income tax. In addition, the bans believe that the Tax Administration should not interpret as presented. However, there are opinions that some other authority can request collection and responsibility on other grounds, such as the prosecution. The interpretations of accounting and financial statements vary from point of view.

„The Association will pay special attention in the future to moral hazard at the system level, as it was pointed out at the last meeting with the CBCG representatives

Lažne telefonske pozive “iz banke” primilo 55% Letonaca

„Ukupno je 2021. godine u četiri najveće banke u Letoniji otkriveno 3.180 slučajeva telefonskih prevara, kojima je ukradeno 4.950.333 eura

Najnovije istraživanje* Mastercarda i Udruženja Finance Latvia pokazuje da je više od polovine stanovništva (55%) u prošloj godini primilo lažni telefonski poziv radi prevare. Ukupno je 2021. godine u četiri najveće banke u Letoniji otkriveno 3.180 slučajeva telefonskih prevara, kojima su izvršene prevare u iznosu od 4.950.333 eura. S druge strane, u prva tri mjeseca ove godine iznos sredstava za koji su prevareni klijenti banaka, kada sami odobravaju plaćanje, dosegao je već 1,6 milion eura, a već u prvim mjesecima godine otkrivena su 443 slučaja telefonske prevare, prevarivši ih za 323 204 eura.

Stoga su stručnjaci iz industrije prikupili ključne savjete o tome kako prepoznati i spriječiti potencijalni pokušaj prevare i što učiniti u slučaju kada se dogodi prevara.

Iako je prema anketi 87% stanovništva uvjereno da bi uspjelo prepoznati da je prevarant kontaktirao telefonom u cilju prevare, statistika pokazuje da broj slučajeva prevare i dalje raste.

Anrijs Šmits, šef Radne grupe za ograničavanje prevara u Udruženju Finance Latvia, ističe osnovne stvari koje su karakteristične za situacije telekomunikacionih prevara:

„Treba imati na umu da zaposleni u banci nikada neće koristiti kanale kao što su WhatsApp, Viber, itd. za komunikaciju sa klijentom. Takođe, zaposleni u banci nikada

55% of Latvians has received a fraudulent phone call

„In total, 3,180 cases of telephone fraud were detected in the four largest banks in Latvia in 2021, defrauding EUR 4 950 333

The latest research* by Mastercard and the Finance Latvia Association shows that more than half of the population (55%) have received a fraudulent phone call in the last year to defraud. In total, 3,180 cases of telephone fraud were detected in the four largest banks in Latvia in 2021, defrauding EUR 4 950 333. In turn, in the first three months of this year, the amount of funds defrauded by bank customers, when approving the payment themselves, has already reached EUR 1.6 million, and already in the first months of the year 443 cases of telephone fraud were detected, defrauding them of EUR 323 204.

Therefore, industry experts have gathered key tips on how to recognise and prevent a potential attempted fraud and what to do in case it happens.

Although according to the survey, 87% of the population are convinced that they would be able to recognise if a fraudster contacted by phone with the aim of defrauding, statistics show that the number of fraud cases continues to grow.

Anrijs Šmits, Head of the Fraud Limitation Task Force at the Finance Latvia Association, highlights the basic things that are characteristic of telecommunications fraud situations:

"It should be remembered that the bank's employees will never use channels such as WhatsApp, Viber, etc. to communicate with the

neće tražiti od klijenta da otkrije lične podatke, neće tražiti da unese Smart-ID šifre tokom razgovora, i definitivno neće odbiti komunikaciju na službenom jeziku. Ako se bilo koja od ovih tačaka pojavi u telefonskom pozivu, onda svakako postoji razlog za sumnju da se radi o prevarantu i razgovor se mora odmah prekinuti. Ako želite da budete sigurni da su vaši podaci i finansijski resursi u redu, preporučujemo da nazovete službeni telefon koji vam je dala banka i kažete vam kakva je situacija."

„Ako nešto izgleda nevjerovatno dobro, onda je to gotovo sigurno prevara

Stručnjak državne policije Dmitrij Homenko ističe:

„Važno je biti svjestan da prevara u telekomunikacijama nije samo telefonski razgovor. Prevaranti koriste audio snimanje govora u raznim telefonskim aplikacijama, šalju tekstualne poruke, a potencijalnim žrtvama se prilazi na društvenim mrežama, mejlovima. Takođe, na primjer, potrebna nam je naš telefon za ulazak u Smart-ID, tako da su mogućnosti ove zamke koje postavljaju telekom prevaranti zapravo veoma široke.

Na primjer, u Letoniji su trenutno najpopularnije prevare ulaganja, koje takođe često nanose najveću štetu žrtvama. Stanovnici primaju pozive od lažnih brokera koji traže novac za ulaganje. Tokom razgovora šalje se web stranica koja pogrešno pokazuje porast ulaganja, stvarajući iluziju rasta vrijednosti investicije. Međutim, ispostavilo se da tu ništa nije stvarno i da je zapravo crtani film, s ciljem da se osoba namami u ovaj kriminalni plan i dobije njegov novac. Osim toga, vrijeme prije nego što žrtva shvati da je prevarena, često u slučajevima prevare ulaganja može trajati nekoliko mjeseci ili više."

Vladislavs Gurmans, šef razvoja ICT proizvoda i usluga i partnerstva telekomunikacionog operatera Bite u Letoniji, dodaje:

„Mobilni operateri redovno sarađuju sa nadležnim tijelima u Letoniji, lokalnim i međunarodnim mobilnim operaterima kako bi se ovi slučajevi telefonskih prevara što prije uklonili. Međutim, javnost mora biti na oprezu, jer u ovom trenutku prevaranti koriste sve složenije i rafiniranije metode i šeme, zadržavajući jednu zajedničku karakteristiku – poziv iz banke, razgovor na ruskom i potrebu dijeljenja osjetljivih podataka koje banke nikada ne bi tražile klijenata u telefonskom razgovoru. Nažalost, operateri ne mogu automatski da blokiraju brojeve koji se koriste za prevare, jer ih prevaranti često lažiraju koristeći telefonske brojeve pravih pretplatnika. Stoga je prilikom zajedničkog informisanja javnosti potrebno osigurati da građani primanjem takvog poziva isti dožive kao upozorenje da razgovor nije uobičajen i da mu je najvjerovatnija namjera prijevara. U svakom slučaju, ako se takav proziv primi, mora se odmah prekinuti."

Gints Mālkalnietis, stručnjak za sajber bezbjednost na CERT.LV, govori o tome kako se možemo zaštititi od telekomunikacionih prevara:

„Cilj prevaranata je da prevare korisnike na osjetljive informacije, kao što su podaci o platnim karticama, korisničko ime i lozinka ili informacije o pristupu bankovnom računu. Ovi napadi su popularni jer ne zahtijevaju veliko ulaganje resursa i znanja od strane prevaranta i relativno su jednostavan za implementaciju. Koliko god prevaranti bili kreativni i koje tehnologije koristili, vi imate najbolju moguću zaštitu u svojim rukama – sebe i svoje kritičko razmišljanje. Prvo što prevaranti obično pokušavaju da urade je da stvore stresnu situaciju i žure da obmanu žrtvu. Zato je tokom ovakvih pregovora važno pauzirati ili čak prekinuti razgovor kako bi se ušli u detalje i razmislili.Takođe procijenite kritične informacije u sms porukama, mejlovima i internet stranicama – nevjerovatan dobitak ili iznenadna ponuda za posao, iako se niste nigdje prijavili, neočekivano nasljeđe od rođaka o kojem ne znate ništa, ili iznenađujuće veliki popusti u online trgovini za brendove o kojima ste oduvijek sanjali – ako nešto izgleda nevjerovatno dobro, onda je to gotovo sigurno prevara."

customer. Also, the bank employee will never ask the customer to disclose personal information, will not ask to enter Smart-ID codes during the conversation, and will definitely not refuse communication in the official language. If any of these points appear in the phone call, then there is definitely reason to suspect that it is a fraudster and the conversation must be terminated immediately. If you want to make sure that your data and financial resources are fine, then we recommend that you call the official phone provided by the bank and tell you the situation."

State police expert Dmitry Homenko highlights:

"It's important to be aware that telecom fraud isn't just a phone conversation. Fraudsters use audio recording speeches in various phone applications, send text messages, and potential victims are approached on social networks, emails. Also, for example, we need our phone to enter Smart-ID. So the possibilities of this trap set by telecom fraudsters are actually very wide.

For example, investment fraud is the most popular in Latvia at the moment, which also often causes the most damage to victims. Residents receive calls from fake brokers who are calling for money to be invested. During the conversation, a website is sent, which mistakenly shows the rise in investment, creating the illusion of the growth of the value of the investment. However, it turns out that nothing is real about it and it is actually a cartoon, with the aim of luring a person into this criminal scheme and getting his money. In addition, the time before the victim realizes that he has been cheated, often in cases of investment fraud can be several months or more."

Vladislavs Gurmans Head of ICT Product and Service Development and Partnership of Telecommunications Operator Bite in Latvia adds:

"Mobile operators regularly cooperate with the responsible authorities in Latvia, local and international mobile operators in order to eliminate these cases of telephone fraud as quickly as possible. However, the public must be vigilant, because at the moment fraudsters are using increasingly complex and refined methods and schemes, maintaining one common feature – a call from the bank, a conversation in Russian and the need to share sensitive data that banks would never ask customers for in a phone conversation. Unfortunately, operators cannot automatically block the numbers used for fraud, as fraudsters often fake them using the phone numbers of real subscribers. Therefore, when informing the public together, it is necessary to ensure that, with the receipt of such a call, people perceive it as a warning that the conversation is not commonplace and its intention is most likely to defraud. In any case, upon receipt of such a call, it must be stopped immediately."

Gints Mālkalnietis, a cybersecurity expert at the CERT.LV, tells about how we can protect ourselves from telecommunications fraud:

"The purpose of fraudsters is to trick users into sensitive information, such as payment card data, username and password, or bank account access information. These attacks are popular because they do not require a large investment of resources and knowledge by fraudsters and are relatively easy to implement. However creative the fraudsters are and what technologies they use, you have the best possible protection in your hands – yourself and your critical thinking. The first thing fraudsters usually try to do is create a stressful situation and rush to get the victim wrong. Therefore, during such negotiations, it is important to pause or even stop the conversation in order to go into detail and think. Also evaluate critical information in text messages, emails and websites – an incredible winnings or a sudden job offer, even though you haven't applied anywhere, an unexpected inheritance from a relative you don't know anything about, or surprisingly large discounts in the online store for brands you've always dreamed of – if something looks incredibly good, then it's almost certainly a scam."

„If something looks incredibly good, then it's almost certainly a scam

Natasha Lomas-reporter
Tech Crunch-a

Vrhovni sud EU pooštrio smjernice o čuvanju podataka u borbi protiv kriminala

Presuda Vrhovnog suda Evropske unije (CJEU) je ponovo potvrdila da se nacionalni zakon ne može oslanjati na tužbu o borbi protiv teškog kriminala kako bi odstupila od zabrane u zakonu EU o opštem i neselektivnom prikupljanju podataka o elektronskim komunikacijama.

Iako je sud označio neke ciljane izuzetke, on ukazuje da bi moglo biti dopušteno prikupljanje digitalnih dokaza u velikom broju za borbu protiv teškog kriminala, kao što je ciljanje mjesta sa velikim brojem slučajeva kriminala ili velikim brojem posjetilaca (kao što su aerodromi) ili druge lokacije na kojima se nalazi kritična infrastruktura.

Upućivanje CJEU-u, koje je uslijedilo nakon žalbe u predmetu koji se odnosi na korišćenje podataka sa mobilnog telefona kako bi se osigurala osuda za ubistvo u Irskoj, dovela je do dugačkog spiska država članica EU koje se pridružuju Irskoj kako bi izvršile pritisak da sud uzme šire tumačenje o tome kako organi za sprovođenje zakona mogu zadržati i koristiti podatke, kao što je *Irish Times* ranije objavio. No, najviši sud bloka odbacio je bilo kakvo brisanje granice između nacionalne bezbjednosti i teškog kriminala - umjesto toga ponovivši da zakon EU onemogućava opšte i neselektivno zadržavanje podataka o prometu i lokaciji koji se odnose na elektronske komunikacije u svrhu borbe protiv teškog kriminala.

„Sud ponovio da zakon EU onemogućava opšte i neselektivno zadržavanje podataka o prometu i lokaciji koji se odnose na elektronske komunikacije u svrhu borbe protiv teškog kriminala

„Iako Direktiva o privatnosti i elektronskim komunikacijama dozvoljava državama članicama da ograniče ostvarivanje tih prava i obaveza u svrhu, između ostalog, borbe protiv kriminala, ta ograničenja moraju biti u skladu sa načelom proporcionalnosti“, stoji u saopštenju za javnost CJEU-a o presudi. „Taj princip zahtijeva usklađenost ne samo sa zahtjevima sposobnosti i nužnosti, već i sa zahtjevima srazmjerne prirode tih mjera u odnosu na cilj kojem se teži”.

„Dakle, Sud je već utvrdio da cilj borbe protiv teškog kriminala, koliko god da je fundamentalan, sam po sebi ne opravdava da mjera kojom se predviđa opšte i neselektivno zadržavanje svih podataka o prometu i lokaciji, kao što je ona utvrđena Direktivom [EU] 2006/24, treba smatrati neophodnim.

Europe's top court sharpens guidance on data retention for combating serious crime

Natasha Lomas-reporter Tech Crunch

A ruling by the European Union's top court has reaffirmed that national law cannot rely on a claim of combating serious crime to deviate from the prohibition in EU law on general and indiscriminate collection of electronic comms data.

Although the court has signposted some targeted exceptions it suggests may be permissible for gathering digital evidence in bulk to fight serious crime, such as by targeting places with a high instance of crime or a high volume of visitors (such as airports), or other locations which house critical infrastructure.

The referral to the CJEU, which followed an appeal in a case related to use of mobile phone data to secure a murder conviction in Ireland, saw a long list of EU Member States joining Ireland to press for the court to take a broader interpretation of how law enforcement authorities can retain and use data, as the Irish Times reported earlier. But the bloc's top court rejected any blurring of the line between national security and serious crime — instead reiterating that EU law precludes the general and indiscriminate retention of traffic and location data relating to electronic communications for the purposes of combating serious crime.

"While the privacy and electronic communications directive allows Member States to place limitations on the exercise of those rights and obligations for the purposes inter alia of combating crime, those limitations must comply with the principle of proportionality," runs a CJEU press release on the judgement. "That principle requires compliance not only with the requirements of aptitude and of necessity but also with that of the proportionate nature of those measures in relation to the objective pursued.

"Thus, the Court has already held that the objective of combating serious crime, as fundamental it may be, does not, in itself, justify that a measure providing for the general and indiscriminate retention of all traffic and location data, such as that established by [EU] Directive 2006/24, should be considered to be necessary.

„The Court reiterated that EU law precludes the general and indiscriminate retention of traffic and location data relating to electronic communications for the purposes of combating serious crime

„U slučaju hitnih prijetnji po nacionalnu bezbjednost, dopušteno privremeno masovno prikupljanje i zadržavanje podataka, ograničeno na 'ono što je strogo neophodno

„U istom smislu, čak ni pozitivne obaveze država članica koje se odnose na uspostavljanje pravila za olakšavanje efikasne akcije u borbi protiv krivičnih djela ne mogu imati učinak opravdavanja ometanja koje je tako ozbiljno kao ono koje podrazumijeva zakonodavstvo koje predviđa zadržavanje saobraćaja i podataka o lokaciji sa osnovnim pravima praktično cjelokupnog stanovništva, u okolnostima u kojima podaci dotičnih osoba ne mogu otkriti vezu, barem posrednu, između tih podataka i cilja kojem se teži."

Široki interes u ovom predmentu nagovještava koliko drugih nacionalnih zakona može djelovati na slično klimavim osnovama u odnosu na masovno zadržavanje podataka – bilo u vezi sa teškim kriminalom ili nacionalnom bezbjednošću.

U vezi sa nacionalnom bezbjednošću, CJEU je u više navrata jasno stavio do znanja da opšti i neselektivni režimi zadržavanja podataka nisu zakoniti - iako je sud dozvolio, u presudi iz oktobra 2020. godine, da kada se država članica suoči s hitnom prijetnjom po nacionalnu bezbjednost, tada može biti dopušteno privremeno masovno prikupljanje i zadržavanje podataka, ograničeno na 'ono što je strogo neophodno'.

Današnja presuda CJEU-a o irskom zahtjevu naglašava potrebu da javne vlasti uspostave ravnotežu između opšteg/javnog interesa u hvatanju kriminalca i osnovnih prava pojedinaca prema pravu EU, koja uključuju pravo na privatni život i poštovanje ličnih podataka.

Sud je odbacio podneske država članica za zaobilazno rješenje koje bi značilo da bi se posebno ozbiljan zločin mogao tretirati na isti način kao prijetnja nacionalnoj bezbjednosti „koja je istinska i trenutna ili predvidiva" - i na taj način omogućava vremenski ograničeno opšte i neselektivno čuvanje podataka o saobraćaju i lokaciji u svrhu suzbijanja kriminala.

„Takva prijetnja se po svojoj prirodi, ozbiljnosti i specifičnosti okolnosti od kojih se sastoji, razlikuje od opšteg i trajnog rizika od nastanka tenzija ili poremećaja, čak i ozbiljne prirode, koji utiču na javnu bezbjednost, odnosno od počinjenja teških krivičnih djela", navodi se u saopštenju.

Dakle, implikacija je da se države članice koje su pritiskale ovu liniju argumenata kako bi pokušale zaobići zakon EU – i „legalizovati" svoje ilegalne režime masovnog prikupljanja podataka – suočavaju sa nekom vrstom ćorsokaka.

U svojoj presudi, CJEU je nastojao da obezbijedi čvršće upravljanje za javne nadležne organe u alternativnim pravcima djelovanja koje bi mogli preduzeti za prikupljanje digitalnih dokaza - pri čemu sud kaže da potvrđuje raniju sudsku praksu smatrajući da pravo EU ne isključuje zakonodavne mjere u te svrhe borbe protiv teškog kriminala i sprečavanja ozbiljnih prijetnji javnoj sigurnosti koje predviđaju:

- ciljano zadržavanje podataka o saobraćaju i lokaciji koje je ograničeno, prema kategorijama dotičnih osoba ili korištenjem geografskog kriterija;
- opšte i neselektivno zadržavanje IP adresa dodijeljenih izvoru internetske veze;
- opšte i neselektivno zadržavanje podataka koji se odnose na građanski identitet korisnika elektronskih komunikacionih sistema;
- ubrzano zadržavanje (brzo zamrzavanje) podataka o prometu i lokaciji u posjedu tih pružaoca usluga.

Ipak, u presudi se takođe naglašava da sve takve mjere podliježu granicama onoga što je striktno neophodno.

Više o navedenim izuzecima od presude:

„ … ciljana mjera za zadržavanje podataka o prometu i lokaciji može se, po izboru nacionalnog zakonodavca i uz striktno poštovanje načela proporcionalnosti, postaviti i korišćenjem geografskog kriterijuma za koji nadležni nacionalni organi smatraju, na osnovu objektivnih i nediskriminatornih faktora, da na jednom ili više geografskih područja postoji situacija koju karakteriše visok rizik pripremanja ili izvršenja teških krivičnih dela. Ta područja mogu uključivati mjesta sa visokom učestalošću teškog kriminala, mjesta koja su posebno osjetljiva na teška krivična djela, kao što su mjesta ili infrastruktura koja redovno primaju vrlo veliki broj posjetilaca, ili strateške lokacije, kao što su aerodromi, stanice, pomorske luke ili područja naplatnih rampi (vidi, u tom smislu, presudu od 6. oktobra 2020. godine, *La Quadrature du Net and Others*, C 511/18,

ckbbanka
otp group

Nova generacija POSlovanja

CKB GO POS - Tvoj telefon je tvoj POS terminal

Dodatne informacije: www.ckb.me • CKB Contact Center 19894

„Presuda naglašava potrebu da javne vlasti uspostave ravnotežu između opšteg/javnog interesa u hvatanju kriminalca i osnovnih prava pojedinaca prema pravu EU

C 512/18 i C 520/18, EU:C:2020:791, st.150 i citirana sudska praksa).

„Treba imati na umu da, prema toj sudskoj praksi, nadležni nacionalni organi mogu usvojiti, za područja iz prethodnog stava, ciljanu mjeru zadržavanja koristeći geografski kriterijum, kao što je, između ostalog, prosjek stope kriminala na geografskom području, a da taj organ ne mora nužno imati posebne indikacije za pripremu ili izvršenje, u dotičnim područjima, djela teškog kriminala. Budući da će se ciljano zadržavanje po tom kriterijumu vjerovatno odnositi, u zavisnosti od teških krivičnih djela i situacije koja je specifična za dotične države članice, i područja obilježena velikom učestalošću teškog kriminala i područja koja su posebno osjetljiva na počinjenje tih djela, u principu nije vjerovatno da će dovesti do diskriminacije, budući da je kriterijum izvučen iz prosječne stope teškog kriminala potpuno nepovezan s bilo kojim potencijalno diskriminirajućim faktorima.

„Pored svega i iznad svega, ciljana mjera zadržavanja koja pokriva mjesta ili infrastrukturu koja redovno primaju vrlo veliki broj posjetilaca, ili strateška mjesta, kao što su aerodromi, stanice, pomorske luke ili područja naplatnih rampi, omogućava nadležnim vlastima da prikupljaju podatke o prometu, a posebno podatke o lokaciji svih osoba koje koriste, u određeno vrijeme, sredstvo elektronske komunikacije na jednom od tih mjesta. Dakle, takva ciljana mjera zadržavanja može omogućiti tim tijelima da, pristupom zadržanim podacima, dobiju informacije o prisutnosti tih osoba na mjestima ili geografskim područjima obuhvaćenim tom mjerom, kao i o njihovom kretanju između ili unutar tih područja i da izvuku zaključke, u svrhu borbe protiv teškog kriminala, o njihovom pristustvu i aktivnostima na tim mjestima ili geografskim područijime u određeo vrijeme tokom perioda zadržavanja.

Sud je odbacio još jedan argument za zaobilazno rešenje - koji je tvrdio da nadležnim organima za borbu protiv teškog kriminala treba dozvoliti da urone u mobilne podatke koji su prikupljeni na veliko, na opšti i neselektivni način, kako bi odgovorili na ozbiljnu pretnju nacionalnoj bezbjednosti koja je prava i aktuelna ili predvidiva.

„Taj argument čini da pristup zavisi od faktora koji nisu povezani sa ciljem borbe protiv teškog kriminala“, navodi se u saopštenju CJEU. „Osim toga, prema toj liniji argumenata, pristup bi se mogao opravdati ciljem manjeg značaja od onog koji je opravdavao njegovo zadržavanje, odnosno očuvanjem nacionalne bezbjednosti, što bi bilo u suprotnosti s tom hijerarhijom ciljeva javnog interesa u čijem kontekstu proporcionalnost mjere zadržavanja mora biti procijenjena. Nadalje, odobravanje takvog pristupa lišilo bi bilo kakve djelotvornosti zabranu sprovođenja opšteg i neselektivnog zadržavanja u svrhu borbe protiv teškog kriminala.”

Sud je dalje smatrao da pristup ličnim podacima kao što su podaci o prometu i lokaciji od strane nadležnih državnih organa mora biti podložan prethodnoj reviziji - koju obavlja sud ili nezavisno administrativno tijelo - i da odluci o preispitivanju mora prethoditi pravilan postupak podnošenja zahtjeva (tzv. „obrazloženi zahtjev tih organa podnijet, između ostalog, u okviru postupaka za sprečavanje, otkrivanje ili krivično gonjenje zločina”).

Sud EU takođe izričito jasno stavlja do znanja da policijski službenik u ovom scenariju ne može zamijeniti odgovarajući sud ili nezavisno tijelo. Dakle, u osnovi, potpisivanje pristupa podacima od strane policajca ne kvalifikuje se kao valjano tijelo za preispitivanje odluka i neće dozvoliti državama članicama da izvrše još jedno brzo 'i' prljavo zaobilaženje zakona EU (ionako ne pravno).

Nacionalni sud takođe ne može izbjeći svoju odgovornost da ukine nacionalno zakonodavstvo koje nije u skladu s direktivom EU o privatnosti i elektronskim komunikacijama, smatra CJEU - što se čini relevantnim za Francusku gdje vlada posljednjih godina pokušava da upotrijebi nacionalne sudove da učine upravo to.

Što se tiče specifične tačke uputnice na predmet - u vezi s tim da li bi zadržani podaci o mobilnom prometu i lokaciji trebali biti dopušteni da stoje kao dokaz u slučaju ubistva - CJEU je vratio stvar na irske sudove, naglašavajući da odluka mora biti u skladu sa principima jednakosti i efektivnosti. Dakle, da li će ti dokazi biti izbačeni ili ne, ostaje da se vidi.

"In the same vein, even the positive obligations of the Member States relating to the establishment of rules to facilitate effective action to combat criminal offences cannot have the effect of justifying interference that is as serious as that entailed by legislation providing for the retention of traffic and location data with the fundamental rights of practically the entire population, in circumstances where the data of the persons concerned are not liable to disclose a link, at least an indirect one, between those data and the objective pursued."

The broad interest in the case hints at how many other national laws may be operating on similarly shaky ground vis-a-vis bulk data retention — whether in relation to serious crime, or national security.

On the latter, the CJEU has repeatedly made it clear that general and indiscriminate data retention regimes are not legal — although the court did allow, in a ruling back in October 2020, that where a Member State faces a pressing national security threat then temporary bulk data collection and retention, limited to 'what is strictly necessary', may be allowed.

The CJEU's ruling on the Irish referral today emphasizes the need for public authorities to strike a balance between the general/public interest in catching a criminal and individuals' fundamental rights under EU law, which include a right to private life and respect for personal data.

The court rejected submissions by Member States for a workaround that would have meant particularly serious crime could be treated in the same way as a threat to national security "which is genuine and current or foreseeable" — and thereby allow for time-limited general and indiscriminate retention of traffic and location data for the purpose of combating crime.

"Such a threat is distinguishable, by its nature, its seriousness, and the specific nature of the circumstances of which it is constituted, from the general and permanent risk of the occurrence of tensions or disturbances, even of a serious nature, that affect public security, or from that of serious criminal offences being committed," the press release says on that.

So the implication is Member States which have been pressing this line of argument to try to workaround the EU law — and 'legalize' their illegal bulk data collection regimes — are facing a bit of a dead-end.

In the ruling, the CJEU has sought to provide tighter steerage for public authorities on alternative courses of action they may take to gather digital evidence — with the court saying it's confirming earlier case law by holding that EU law does not preclude legislative measures for the purposes of combating serious crime and preventing serious threats to public security that provide for:

„In the case of a pressing national security threat, a temporary bulk data collection and retention, limited to 'what is strictly necessary', may be allowed

- the targeted retention of traffic and location data which is limited, according to the categories of persons concerned or using a geographical criterion;
- the general and indiscriminate retention of IP addresses assigned to the source of an internet connection;
- the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems;
- the expedited retention (quick freeze) of traffic and location data in the possession of those service providers.

Albeit, the ruling also stresses that any such measures are subject to the limits of what is strictly necessary.

More on the cited exceptions from the ruling:

" … a targeted measure for the retention of traffic and location data may, at the choice of the national legislature and in strict compliance with the principle of proportionality, also be set using a geographical criterion where the competent national authorities consider, on the basis of objective and non-discriminatory factors, that there exists, in one or more geographical areas, a situation characterised by a high risk of preparation for or commission of serious criminal offences. Those areas may include places with a high incidence of serious crime, places that are particularly vulnerable to serious crime, such as places or infrastructure which regularly receive a very high volume of visitors, or strategic locations, such as airports, stations, maritime ports or tollbooth areas (see, to that effect, judgment of 6 October 2020, La Quadrature du Net and Others, C 511/18, C 512/18 and C 520/18, EU:C:2020:791, paragraphs 150 and the case-law cited).

"It should be borne in mind that, according to that

moj POS

Vaš telefon postaje POS terminal.

HIPOTEKARNA BANKA
Vama posvećena

www.hb.co.me Kontakt centar 19905

case-law, the competent national authorities may adopt, for areas referred to in the preceding paragraph, a targeted measure of retention using a geographic criterion, such as, inter alia, the average crime rate in a geographical area, without that authority necessarily having specific indications as to the preparation or commission, in the areas concerned, of acts of serious crime. Since a targeted retention using that criterion is likely to concern, depending on the serious criminal offences in question and the situation specific to the respective Member States, both the areas marked by a high incidence of serious crime and areas particularly vulnerable to the commission of those acts, it is, in principle, not likely moreover to give rise to discrimination, as the criterion drawn from the average rate of serious crime is entirely unconnected with any potentially discriminatory factors.

"In addition and above all, a targeted measure of retention covering places or infrastructures which regularly receive a very high volume of visitors, or strategic places, such as airports, stations, maritime ports or tollbooth areas, allows the competent authorities to collect traffic data and, in particular, location data of all persons using, at a specific time, a means of electronic communication in one of those places. Thus, such a targeted retention measure may allow those authorities to obtain, through access to the retained data, information as to the presence of those persons in the places or geographical areas covered by that measure as well as their movements between or within those areas and to draw, for the purposes of combating serious crime, conclusions as to their presence and activity in those places or geographical areas at a specific time during the period of retention."

The court rejected another workaround type argument — which had posited that serious-crime-fighting authorities should be allowed to dip into mobile data which had been gathered in bulk, in a general and indiscriminate way, to address a serious threat to national security which is genuine and current or foreseeable.

"That argument makes that access depend on factors that are unrelated to the objective of combating serious crime," notes the CJEU's press release. "In addition, under that line of argument, access could be justified by an objective of lesser importance than that which justified its retention, namely safeguarding national security, which would be contrary to that hierarchy of public interest objectives in the context of which the proportionality of a retention measure must be assessed. Furthermore, to authorise such access would deprive of any effectiveness the prohibition on carrying out general and indiscriminate retention for the purpose of combating serious crime."

„The ruling emphasizes the need for public authorities to strike a balance between the general/public interest in catching a criminal and individuals' fundamental rights under EU law

The court further held that access to personal data such as traffic and location data by competent national authorities must be subject to a prior review — carried out either by a court or by an independent administrative body — and that a review decision must be preceded by the proper requesting procedure (aka "a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime").

The CJEU also makes it explicitly clear that a police officer cannot stand in for the requisite court or independent body in this scenario. So, basically, sign-off on data access by a police officer does not qualify as a valid decision review body and will not let Member States pull off another quick 'n' dirty bypass of EU law (not legally anyway).

A national court also cannot eschew its responsibility to strike down national legislation that's incompatible with the EU directive on privacy and electronic communications, the CJEU further held — which looks pertinent for France where the government has been seeking to use the national courts to do just that in recent years (via Politico).

On the specific point of case referral — as to whether the retained mobile traffic and location data should be allowed to stand as evidence in the murder case — the CJEU has bounced the matter back to the Irish courts, emphasizing that a ruling needs to comply with the principles of equivalence and effectiveness. So, whether that evidence gets thrown out or not remains to be seen.

Marcéta Fišerová,
direktorica Odjeljenja za komunikacije
Radek Šalša,
portparol Udruženja banaka Češke

Za slanje novca neće biti potreban broj računa

Udruženje banaka Češke, u saradnji sa Češkom narodnom bankom, sarađuje na projektu nove usluge pod nazivom Payments to contact, koja će pojednostaviti slanje novca između ljudi. Umjesto broja računa u internet ili mobilnom bankarstvu, dovoljno je unijeti broj mobilnog telefona primaoca uplate.

Plaćanje i bez poznavanja broja računa primaoca biće moguće zahvaljujući registru brojeva računa koji su upareni sa brojevima mobilnih telefona njihovih vlasnika. Nakon unosa uplate, banka pošiljaoca kontaktira registar i na osnovu broja telefona primaoca dobija broj njegovog bankovnog računa na koji on šalje uplatu. Do sada se prijavilo devet banaka za realizaciju projekta. Primanje uplata putem kontakta biće omogućeno klijentima banaka uključenih u ovu novu uslugu, koji će se prijaviti da je koriste preko svoje banke i povezati svoj broj telefona sa svojim brojem računa.

„Od iduće godine moći će se uplatiti novac na tuđi račun samo uz poznavanje broja telefona vlasnika.

„Slični servisi već rade u inostranstvu, gde smo bili inspirisani – na primer, u SAD, Letoniji ili Slovačkoj. Predviđamo da ćemo uslugu moći da pokrenemo od nove godine, ako testiranje ne otkrije neočekivane komplikacije, a pojedine banke koje su trenutno uključene u projekat su takođe spremne. Počinjemo sa brojevima mobilnih telefona, ali bi se u budućnosti sistem mogao proširiti i na druge moguće kontakte za uparivanje sa brojem računa, kao što su e-mail adrese",rekao je član Uprave CNB Oldřich Dědek, koji nadzire odjeljenje za upravljanje rizicima i poslovnu podršku, koji na strani CNB-a upravlja projektom.

Testiranje funkcija novog sistema biće pokrenuto u ljetnjim mjesecima ove godine. Sistem će raditi zahvaljujući Češkoj narodnoj banci, koja će voditi registar sa prijavljenim parovima telefonskih brojeva i brojeva računa. Sistem kojim upravlja centralna banka tako utvrđuje, na osnovu upita banke platioca, da li je telefonski broj naveden u registru i, u pozitivnom slučaju, saopštava odgovarajući broj računa primaoca banci upitniku.

„Kopiranje ili prepisivanje broja računa često dovodi do grešaka kod klijenata sa kojima banke naknadno moraju da se bave. U najboljem slučaju ne postoji pogrešno unijeti broj računa, što mogu da otkriju bankarski sistemi. Nažalost, dešava se da unošenjem pogrešne šifre banke npr. novac stiže na potpuno strani račun. Osim veće pogodnosti za klijente, očekujemo manje ovakvih grešaka i dalje ubrzanje platnog prometa od uplate do kontakta",rekao je Tomáš Hládek, stručnjak CNB za plaćanja.

Payments to contact je još jedna velika inovacija u platnom sistemu u posljednje vrijeme. Instant plaćanja, koja su se prvi put pojavila na tržištu 2018. godine i koje trenutno svojim klijentima nudi 12 banaka, postaju sve popularniji među klijentima. Novac se prenosi 24/7 između bilo kojeg računa za nekoliko sekundi. Time se eliminiše kašnjenje između unosa i uplate na račun. Zbog toga je sada svaka peta transakcija u načinu instant plaćanja.

Marcéta Fišerová, Director of the Communication Department
Radek Šalša, spokesman of the Czech Banking Association

No account number will be required to send money

The Czech Banking Association, in cooperation with the Czech National Bank, is cooperating on a project of a new service called payments to contact, which will simplify the sending of money between people. Instead of an account number in internet or mobile banking, it will be enough to enter the mobile number of the payee.

Making a payment even without knowing the payee's account number will be possible thanks to the register of account numbers paired with the mobile numbers of their owners. After entering the payment, the sender's bank contacts the registry and, based on the payee's phone number, obtains the number of his bank account, to which he then sends the payment. So far, nine banks have signed up for the implementation of the project. Receiving contact payments will be made possible for clients of banks involved in this new service, who will log in to use it through their bank and link their phone number to their account number.

"Similar services are already operating abroad, where we have been inspired – for example, in the USA, Latvia or Slovakia. We anticipate that we will be able to launch the service from the new year, if testing does not reveal unexpected complications and the individual banks currently involved in the project are also ready. We start with mobile numbers, but in the future the system could also be extended to other possible contacts for pairing with the account number, such as email addresses," said CNB Bank Board member Oldřich Dědek, who oversees the Risk Management and Business Support section, which manages the project on the CNB's side.

Testing of the functions of the new system will be launched in the summer months of this year. The system will work thanks to the Czech National Bank, which will keep a register with reported pairs of phone numbers and account numbers. The system operated by the central bank thus determines, on the basis of a query from the payer's bank, whether the telephone number is listed in the register and, in the positive case, communicates the corresponding payee account number to the inquiring bank.

"Copying or overwriting the account number often leads to mistakes on the part of clients that banks subsequently have to deal with. In the best case, the incorrectly entered account number does not exist, which can be detected by bank systems. Unfortunately, it happens that by entering the wrong bank code, for example, the money arrives at a completely foreign account. In addition to greater convenience for clients, we expect fewer such errors and further acceleration of payment transactions from payments to contact," said Tomáš Hládek, ČBA's expert for payments.

Payments to contact are another major innovation in the payment system of recent times. Instant payments, which first appeared on the market in 2018 and which are currently offered to their clients by 12 banks, are gaining increasing popularity among clients. Money is transferred 24/7 between any accounts in a few seconds. This eliminates the delay between entering and crediting the payment to the account. That is why every fifth transaction is now in the instant payment mode.

„From next year, it will be possible to send a payment to someone else's account only with knowledge of the phone number of its owner

Kalyeena Makortoff,
Guardianov bankarski
dopisnik

Zviždači i novinari moći će da otkrivaju bankarske tajne

„Zakonom o bankarskoj tajni se objelodanjivanje informacija o klijentima banke smatra krivičnim djelom, čak i ako je to u javnom interesu

Odbor u švajcarskom parlamentu mogao bi iznijeti prijedloge kojima bi se izmijenio zakon o bankarskoj tajni.

Švajcarski političari će raspravljati o budućnosti kontroverznog zakona o bankarskoj tajni u zemlji, jer se suočava sa pritiskom zvaničnika UN-a da ukinu pravila prema kojima lica koja ukazuju na nepravilnosti (zviždači) i novinari koji izvještavaju o potencijalnim prekršajima mogu biti krivično gonjeni.

Odbor u švajcarskom parlamentu mogao bi iznijeti prijedloge kojima bi se izmijenio zakon o bankarskoj tajni – poznat kao član 47 – kojim se objelodanjivanje informacija o klijentima banke smatra krivičnim djelom, čak i ako je to u javnom interesu.

To dolazi usred sve većeg međunarodnog pritiska da se zakon ukine, uključujući i specijalnu izvjestiteljicu Ujedinjenih nacija za slobodu mišljenja i izražavanja, Irene Khan, koja je rekla da je član 47 prekršio međunarodno pravo i ljudska prava. „Ovo je inače problem u autoritarnim državama“, rekla je ona.

Khan, koja je pisala švajcarskoj vladi o tom pitanju, planira da iznese svoju zabrinutost u vezi sa članom 47 Savjetu UN-a za ljudska prava.

Njena intervencija uslijedila je nakon istrage konzorcijuma međunarodnih medija, uključujući i Guardian, u drugoj po veličini švajcarskoj banci Credit Suisse.Curenje podataka, koje je uključivalo podatke za 30.000 klijenata, otkrilo je da je banka decenijama držala račune za pojedince umiješane u torturu, trgovinu drogom, pranje novca, korupciju i druga teška krivična djela.

Međutim, švajcarski zakoni o ekstremnoj bankarskoj tajni značili su da novinari koji su učestvovali u istrazi, poznatiji kao projekat „Švajcarske tajne“, rizikovali potencijalne novčane ili čak zatvorske

Kalyeena Makortoff the Guardian's banking correspondent

Whistleblowers and journalists will be able to disclose banking secrets

A committee in Switzerland's parliament could put forward proposals that would amend the banking secrecy law.

Swiss politicians will debate the future of the country's controversial banking secrecy law this week, as it faces pressure from UN officials to scrap rules under which whistleblowers and journalists who report on potential wrongdoing can be prosecuted.

A committee in Switzerland's parliament could put forward proposals that would amend the banking secrecy law – known as article 47 – which makes it a criminal offence to disclose information about a bank's clients, even if it is in the public interest to do so.

It comes amid mounting international pressure to repeal the law, including from the United Nations special rapporteur for freedom of opinion and expression, Irene Khan, who said article 47 violated international law and human rights. "This is normally a problem in authoritarian states," she said.

Khan, who has written to the Swiss government on the matter, is planning to escalate her concerns regarding article 47 to the UN's human rights council next month.

Her intervention following an investigation by a consortium of international media outlets, including the Guardian, into Switzerland's second largest bank, Credit Suisse. The leak, which included data for 30,000 clients, revealed that the bank held accounts for individuals involved in torture, drug trafficking, money laundering, corruption, and other serious crimes, over decades.

However, Switzerland's extreme banking secrecy laws meant that journalists who took part in the investigation, known as the Suisse secrets project, risked potential fines or even imprisonment. Swiss media could not take part as a result.

„The banking secrecy law makes it a criminal offence to disclose information about a bank's clients, even if it is in the public interest to do so

„Konzorcijum međunarodnih medija otkrio da je banka Credit Suisse decenijama držala račune za pojedince umiješane u torturu, trgovinu drogom, pranje novca, korupciju i druga teška krivična djela

kazne. Kao rezultat toga, švajcarski mediji nisu mogli učestvovati.

To je navelo Khan da piše švajcarskoj vladi, zahtijevajući od njih da objasne kako su zakoni usklađeni sa opredijeljenošću zemlje za ljudska prava.

„Sveukupna zaštita bankarske tajne u Švajcarskoj krši međunarodno pravo", rekla je Khan novinarima iz Tamedia i Der Spiegel-a, koji su bili uključeni u projekat „Švajcarske tajne". Ona je rekla da su švajcarski zakoni o bankarskoj tajni nekompatibilni sa dvije međunarodne konvencije – članom 19 Međunarodnog pakta o građanskim i političkim pravima i članom 10 Evropske konvencije o ljudskim pravima – koje zajedno garantuju slobodu izražavanja i štampe.

„Švajcarska je potpisala oba i dužna je da ih podrži", rekla je ona.

Khan je dodala da je švajcarska vlada „u teškoj poziciji da objasni zašto bi objavljivanje informacija koje bi mogle otkriti finansijske zločine trebalo biti kažnjeno kaznom do tri godine zatvora. Pogotovo kada novinari i zviždači ukazuju na stvarne probleme u banci. Zakon to ne bi trebao da zabranjuje."

Član 47 postoji od početka 20. vijeka, ali je 2015. godine proširen na treće strane kao što su novinari i zviždači, nakon brojnih slučajeva u kojima su podaci o klijentima dijeljeni stranim poreskim vlastima. To je famozno uključivalo CD sa podacima HSBC Private Bank Suisse kojem su kasnije pristupili novinari.

Pristalice zakona su ranije citirale prava klijenata na privatnost. Međutim, Khan je rekla: „Osuđeni kriminalci i politički izložena lica imaju pravo na privatnost, ali ne kada postoji dobar osnov za vjerovanje da su možda umiješani u finansijska nedjela".

Credit Suisse je u februaru saopštio da ne može da komentariše određene klijente zbog istih zakona o bankarskoj tajni, ali „snažno odbacuje navode i zaključke o navodnim poslovnim praksama banke".

Specijalna izvjestiteljica je rekla da je švajcarska vlada od tada odgovorila na njeno pismo, koje je prvi put poslato u martu, tvrdeći da je u potpunosti posvećena slobodi izražavanja i da nijedan novinar nikada nije procesuiran po zakonu, za koji su rekli da je sada u fazi revizije.

U međuvremenu, švajcarski parlamentarni pododbor za ekonomiju i poreze treba da preispita član 47 i nalaze istrage iz projekta„Švajcarske tajne" od 5. maja. Podkomisija bi naknadno mogla podnijeti prijedlog kojim bi se zakon mogao izmijeniti.

Ali ako ne dođe do velike izmjene, Khan će izložiti ovo pitanje Savjetu UN-a za ljudska prava. Ona planira da predstavi zvaničnicima novi izvještaj o slobodama štampe koji će se „kritički pozabaviti" članom 47 i zabranjivanjem novinarstva za koji kaže da se obično opaža u autoritarnim režimima.

„Švajcarska je zagovornik ljudskih prava i slobode štampe, i aktivno učestvuje u Savjetu UN-a za ljudska prava. Više puta je osuđivala postupke drugih zemalja protiv novinara. Zato je važno da Švajcarska sada sama reaguje i promijeni ovako problematičan zakon. Švajcarska ne smije samo propovijedati. Mora i djelovati", rekla je Khan.

It prompted Khan to write to the Swiss government, demanding they explain how the laws aligned with the country's commitment to human rights.

"The blanket protection of banking secrecy in Switzerland violates international law," Khan told reporters from Tamedia and Der Spiegel, who were involved in the Suisse secrets project. She said Swiss banking secrecy laws were incompatible with two international conventions – article 19 of the international covenant on civil and political rights, and article 10 of the European convention on human rights – which together guarantee freedom of expression and the press.

"Switzerland has signed both and is obliged to uphold them," she said.

Khan added that the Swiss government was "in a difficult position to explain why publishing information that could reveal financial crimes should be punished with up to three years in prison. Especially when journalists and whistleblowers point out real problems in a bank. The law should not criminalise that."

Article 47 has existed since the early 20th century, but was expanded in 2015 to include third parties such as journalists and whistleblowers, after a number of cases where client data was shared with to foreign tax authorities. That famously included a CD of data from HSBC Private Bank Suisse that was subsequently accessed by journalists.

Supporters of the law have previously cited clients' rights to privacy. However, Khan said: "Convicted criminals and politically exposed persons have a right to privacy but not when there is good ground to believe they may be involved in financial wrongdoing."

Credit Suisse said in February that it could not comment on specific clients due to the same banking secrecy laws but "strongly rejects the allegations and inferences about the bank's purported business practices".

The special rapporteur said the Swiss government had since responded to her letter, first sent in March, claiming it was fully committed to freedom of expression and that no journalist had ever been prosecuted under the law, which they said was now under review.

A Swiss government spokesperson said they expected the full response to be published next week.

In the meantime, the Swiss parliamentary subcommittee on economy and taxes is to review article 47 and the findings from the Suisse secrets investigation from 5 May. The subcommittee could put forward a motion that could amend the law as early as Friday.

But barring a major overhaul, Khan will escalate the issue to the UN human rights council. She plans to present officials with a new report on press freedoms that will "critically address" article 47 and the criminalisation of journalism that she says is typically observed in authoritarian regimes.

"Switzerland is a champion of human rights and press freedom, and participates actively in the UN human rights council. It has repeatedly denounced the actions of other countries against journalists. That is why it is important that Switzerland now reacts itself and changes such a problematic law. Switzerland must not only preach. It must also act," she said.

„The consortium of international media outlets, revealed that Credit Suisse held accounts for individuals involved in torture, drug trafficking, money laundering, corruption, and other serious crimes

Kada i najbolje finansiranje nije dovoljno

José Luis Martínez Campuzano, portparol Udruženja banaka Španije

Glavni razlozi za zabrinutost španskih kompanija su problemi u snabdijevanju, povećanje cijene energije, neizvjesnost u pogledu ekonomske politike, ograničenja u snabdijevanju i teškoće u pronalaženju radne snage. Ovaj zaključak izvedenje iz najnovijeg istraživanja Banke Španije ošpanskim kompanijama u prvom kvartalu.

Važno je napomenuti da ispitane kompanije smatraju da je umjerenost u tempu rasta, umnogome posljedica svih ovih zabrinutosti, prolazna.

Banka Španije je prije nekoliko dana revidirala naniže svoje ekonomske prognoze za naredne dvije godine za jedan procentni poen, na 4,5% u 2023. i 2,9% u 2024. godini. Monetarne vlasti su takođe aludirale na „privremeno kašnjenje“ u procesu približavanja nivoima BDP-a prije pandemije, iako su takođe priznale da postoje poteškoće u ovom trenutku u pravljenju prognoza.

Rat u Ukrajini, pored strašne humanitarne krize koju je izazvao, predstavlja i ekonomski šok koji utiče na izglede za globalni rast, uključujući i špansku ekonomiju.

Egzogeni faktor kao što je rat ili kontinuirani rast cijena energije povlači za sobom kratkoročna ograničenja ponude i tražnje, sa većom neizvjesnošću za budućnost. Odgovor kompanija mora biti poboljšanje efikasnosti i produktivnosti reformama i većom fleksibilnošću u proizvodnji. Ukratko, reforme moraju biti ojačane suočavajući se sa neizvjesnošću. Nadležni organi, sa svoje strane, moraju stvoriti prave uslove da kompanije izvrše ova prilagođavanja.

Pod solidnim izgledima za rast kao što su oni koji su postojali prije rata, najrelevantnija stvar za nadležne organe je da sada stvore klimu sigurnosti za ekonomske subjekte. Promovisanje inovacija je uvijek bilo ključno za napredak u svakom scenariju. A to je upravo jedan od ciljeva evropskih fondova: postizanje solidnog, digitalnog i održivog rasta. Ali treba ih pravilno koristiti, za šta je potrebna veća javno-privatna koordinacija.

Nedavna studija koju je uradio KPMG pokazala je da samo 9% kompanija ima pristup planiranoj podršci iz EU fondova za oporavak. I prema zaključcima studije, 80% kompanija koje pristupaju uvijek je isto. Opštem nedostatku znanja o sredstvima i načinu pristupa njima pridružuje se i teškoća procedura za njihovo dobijanje i opravdavanje, kao pozadinski razlozi za njihovu oskudnu raspodjelu.

Saradnja svih ostaje od suštinskog značaja za vraćanje određene izvjesnosti koja je kompanijama potrebna u vremenima komplikovanim kao što su sadašnja. A adekvatno upravljanje evropskim fondovima, koji stižu efikasno iza projekte sa realnim budućim izgledima, ključno je da se to postigne.

„Dok banke garantuju povoljne uslove finansiranja za podsticanje oporavka, važno je da se radi o odgovornom finansiranju, kako se ne bi stvarali novi rizici

Dok banke garantuju povoljne uslove finansiranja za podsticanje oporavka, važno je da se radi o odgovornom finansiranju, kako se u budućnosti ne bi stvarali novi rizici koji ne postoje.

Jedan od zaključaka najnovijeg evropskog istraživanja o bankarskim kreditima koji je uradila ECB je da je došlo do pooštravanja kriterijuma za odobravanje kredita kompanijama, odnosno svih radnji koje institucije sprovode prije odobravanja kredita. Evropske banke stoga odražavaju svoju nižu toleranciju na rizik suočene sa povećanom neizvjesnošću o tome kako bi ukrajinski rat mogao uticati na kreditni rizik i očekivanja manje prilagodljive monetarne politike. Promjena diskursa ECB-a o svojoj strategiji monetarne politike takođe zahtijeva period prilagođavanja na finansijskim tržištima.

Ali veći oprez u novom finansiranju ne znači da će biti gore. Španske banke su, na primjer, zadržale nepromijenjene opšte uslove odobravanja novih kredita uprkos nestabilnosti na međunarodnim finansijskim tržištima. Finansiranje banaka ostaje ključno u vremenima neizvjesnosti, kao što su pokazali i tokom pandemije.

Glavne determinante poslovnih ulaganja su korišćeni proizvodni kapaciteti, buduća očekivanja i uslovi finansiranja. Prvi faktor je kratkoročno ograničenje koje je teško prevladati, a nije lako prevladati neizvjesnost, iako se mogu preduzeti mjere da se ona svede na minimum. Ovim preprekama, međutim, neće biti dodato finansiranje banaka. Uprkos padu tražnje za finansiranjem koji se očekuje u narednim mjesecima, bankarski sektor ima snagu i resurse da garantuje finansiranje koje je kompanijama potrebno da napreduju i ostvare svoje projekte.

When the best financing is not enough

José Luis Martínez Campuzano,
speaker of the Spanish Banking Association

The main reasons for concern of Spanish companies are supply problems, the increase in the cost of energy, uncertainty about economic policy, supply limitations and the difficulty in finding labour. This conclusion is drawn from the latest survey of Spanish companies in the first quarter of the Bank of Spain.

It is important to note that the companies surveyed consider that the moderation in the pace of growth, largely a consequence of all these concerns, is transitory.

The Bank of Spain revised downwards a few days ago its economic forecasts for the next two years by one percentage point, to 4.5% in 2023 and 2.9% in 2024%. The monetary authority also alluded to a "temporary delay" in the process of convergence towards pre-pandemic GDP levels, although it also acknowledged the difficulty at this time in making forecasts.

The war in Ukraine, in addition to the terrible humanitarian crisis it has caused, also represents an economic shock that affects the prospects for global growth, which includes the Spanish economy.

An exogenous factor such as war or the continued rise in energy prices entail short-term constraints on supply and demand, with greater uncertainty for the future. The response of companies must be to improve efficiency and productivity with reforms and more flexibility in production. In short, they must be strengthened in the face of uncertainty. The authorities, for their part, must create the right conditions for companies to carry out these adjustments.

Under solid growth prospects such as those existing before the war, the most relevant thing now for the authorities is to create a climate of certainty for economic agents. Promoting innovation has always been key to advancing in any scenario. And this is precisely one of the objectives of the European funds: to achieve solid, digital and sustainable growth. But they need to be used properly, for which greater public-private coordination is needed.

Only 9% of companies have access to the planned support from EU recovery funds, according to a recent KPMG study. And following the conclusions of the study, 80% of the companies that access are always the same. The general lack of knowledge about the funds and the way to access them is joined by the difficulty of the procedures to receive and justify them, as background reasons for their scarce distribution.

The cooperation of all remains essential to recover some of the certainty that companies need in times as complicated as the current ones. And an adequate management of European funds, which arrive efficiently and to projects with real future prospects, is key to achieving this.

„While banks guarantee favourable financing conditions to boost the recovery, it is important that this is responsible financing, so that no new risks are generated

While banks guarantee favourable financing conditions to boost the recovery, it is important that this is responsible financing, so that no new risks are generated in the future that do not exist.

One of the conclusions of the latest European survey of bank loans by the ECB is that there has been a tightening of the criteria for granting loans to companies, that is, of all the actions carried out by institutions before approving a loan. European banks thus reflect their lower risk tolerance in the face of increased uncertainty about how Ukraine's war may affect credit risk and expectations of a less accommodative monetary policy. The ECB's change of discourse on its monetary policy strategy also requires a period of adjustment in the financial markets.

But greater caution in new funding doesn't mean it gets worse. Spanish banks, for example, kept the general conditions of new loans unchanged despite the instability in international financial markets. Bank financing remains key in times of uncertainty as they have also shown during the pandemic.

The main determinants of business investment are the production capacity used, future expectations and financing conditions. The first factor is a short-term constraint that is difficult to overcome and it is not easy to overcome uncertainty, although measures can be taken to minimize it. To these obstacles, however, bank financing will not be added. Despite the decline in demand for financing expected in the coming months, the banking sector has the strength and resources to guarantee the financing that companies need to move forward and make their projects a reality.

Antonio Patuelli, Predsjednik Italijanskog udruženja banaka (ABI)

Italijanske banke su otporne

"Značajna otpornost" italijanskih banaka uprkos pandemiji i rusko-ukrajinskoj krizi, zahtjev da se ne pooštravaju pravila Bazelskog 3+ sporazuma osmišljenog pre dvije vanredne situacije, alarm za korišćenje kriptovaluta u odsustvu međunarodne regulative, očekivanja da će se prekogranična bankarska spajanja u Evropi suočiti sa sve većom konkurencijom američkih i azijskih finansijskih giganata, zahtjev da se banke ne opterećuju dodatnim kapitalnim zahtjevima uz kreiranje pravila za održivo finansiranje, važnost kompletiranja Bankarske unije i Unije tržišta kapitala na "pragmatičniji" način, a prije svega zahtjev za "produžene evropske i nacionalne mjere otpornosti za obnovljeni održivi razvoj i zapošljavanje – takođe neophodne za smanjenje javnog duga – u svjetlu eksplozije cijena energije, inflacije i neizvjesnog ekonomskog oporavka".

Ovo su samo neke od poruka koje je izrekao predsjednik ABI (Italijanskog udruženja banaka) Antonio Patuelli u svom uvodnom govoru na Godišnjem sastanku koji je održan 8. jula u Rimu. G. Patuelli, kojeg je novoizabrani Savjet takođe ponovo izabrao za predsjednika ABI-ja na obnovljeni dvogodišnji mandat, pozvao je Evropsku uniju (EU) da reformiše Pakt za stabilnost i rast tako što će „preokrenuti njegove faktore, čime se prvenstveno želi rast i, kao posljedica, stabilnost".

Takođe je pozvao na pravno obavezujući Ustav za Evropsku uniju, čak i na reviziju njenih ugovora, ako je potrebno. Konačno, naglasio je važnost stvaranja evropskog tijela za borbu protiv pranja novca - s nadležnostima i za kriptovalute - i da njegovo sjedište bude u Italiji.

U svom govoru, guverner Banke Italije Ignazio Visco potvrdio je "čvrstu volju Evropske centralne banke (ECB)" da se bori protiv inflacije, nazvavši je "nepravednim porezom za potrošače i građane". U zaključku, italijanski ministar finansija, Daniele Franco, fokusirao se na ekonomski podsticaj koji bi mogao proizaći iz pune implementacije Nacionalnog plana oporavka i otpornosti (PNRR).

"Uticaj bi mogao biti još veći ako se široki i artikulisani reformski program predviđen PNRR-om brzo i u cijelosti završi", komentarisao je Franco.

„Pautelli je naglasio važnost stvaranja evropskog tijela za borbu protiv pranja novca - s nadležnostima i za kriptovalute - i da njegovo sjedište bude u Italiji

Antonio Patuelli,
Chairman of the Italian Banking Association (ABI)

Italian banks are resilient

The "substantial resilience" of Italian banks despite the pandemic and the Russian-Ukrainian crisis, the request not to tighten the rules of the Basel 3+ Accord designed before the two emergencies, the alarm for the use of cryptocurrencies in the absence of international regulation, the hope for cross-border banking mergers in Europe to face the rising competition of US and Asian financial giants, the request not to burden banks with additional capital requirements while creating the rules for sustainable finance, the importance of the completing of the Banking Union and the Capital Markets Union in a more "pragmatic" way, and above all the request for "prolonged European and national resilience measures for renewed sustainable development and employment - also indispensable for reducing public debt - in light of the explosion of energy prices, inflation and the uncertain economic recovery ".

These are just some of the messages delivered by the Chairman of ABI (the Italian Banking Association), Antonio Patuelli, in his opening speech at the Annual Meeting which was held in Rome on 8 July. Mr. Patuelli, who has also been re-elected President of ABI for a renewed two-year term by the newly elected Council, invited the European Union (EU) to reform the Stability and Growth Pact by "reversing its factors, thus aiming firstly for growth and, as a consequence, for stability".

He also called for a legally binding Constitution for the European Union, even revising its Treaties, if necessary. Finally, he stressed the importance of creating a European anti-money laundering authority - with competences also on cryptocurrencies - and of having its headquarters in Italy.

In his speech, the Governor of the Bank of Italy, Ignazio Visco, confirmed the "firm will of the European Central Bank (ECB)" to fight inflation, calling it an "unfair tax on consumers and citizens". In conclusion, the Italian Minister of Finance, Daniele Franco, focused on the economic stimulus that could come from the full implementation of the National Recovery and Resilience Plan (PNRR).

"The impact may be even greater if the broad and articulated reform program envisaged by the PNRR is completed quickly and in its entirety", he commented.

„Patuelli stressed the importance of creating a European anti-money laundering authority - with competences also on cryptocurrencies - and of having its headquarters in Italy

Patrice Baubeau,
Viši predavač, Istorija,
Ekonomska istorija,
Université Paris
Nanterre – Université
Paris Lumières,
časopis „Razgovor“

Identifikacija, četvrta funkcija novca

Monetarna teorija uči da su tri funkcije novca čuvanje vrijednosti, obračunska jedinica i sredstvo razmjene. Ovaj članak otkriva četvrtu osnovnu funkciju - identifikaciju - i propituje političke i društvene implikacije na privatne i javne izdavaoce novca.

Kratko zaobilaženjekroz istoriju omogućava namda postavimo pitanje o tri funkcije novca koje su tradicionalno identifikovane: standard vrijednosti, posrednik razmjene i rezerva vrednosti, u širem okviru. Ova perspektiva otkriva četvrtu fundamentalnu funkciju, identifikaciju, koja označava zajedničko, političko i društveno porijeklo monetarne činjenice.

Nova monetarna sredstva, kao npr. bitcoin, državne kriptovalute ili virtuelne valute koje se koriste u video igrama, daju posebnu težinu ovoj funkciji identifikacije i njenim političkim i društvenim posljedicama.

„Danas nas nove monetarne inovacije podsjećaju na važnost ove četvrte funkcije novca - identifikacije

Pitanje identifikacije pojavljuje se uz Aristotelove analizenovcau njegovima djelima „Politika“ i „Nikomahova etika“, radovima koji se uglavnom fokusiraju napolis, njegove granice, njegovu organizaciju, njegovu pravdu. On tako razvija, slijedeći Platona, političku i građansku refleksiju koja povezuje granice polisa sa rađanjem novca, čija zloupotreba može biti u suprotnosti sa pravilima idealne države: 1) tako što će dobit od spoljnje trgovine imati prednost nad solidarnošću internih razmjena;

Patrice Baubeau Senior Lecturer, History, Economic History,
Université Paris Nanterre – Université Paris Lumières

Identification, the Fourth Function of Money

Monetary theory teaches that the three functions of money are a store of value, a unit of account, and a medium of exchange. This article reveals a fourth fundamental function - identification - and questions the political and social implications for private and public issuers of money

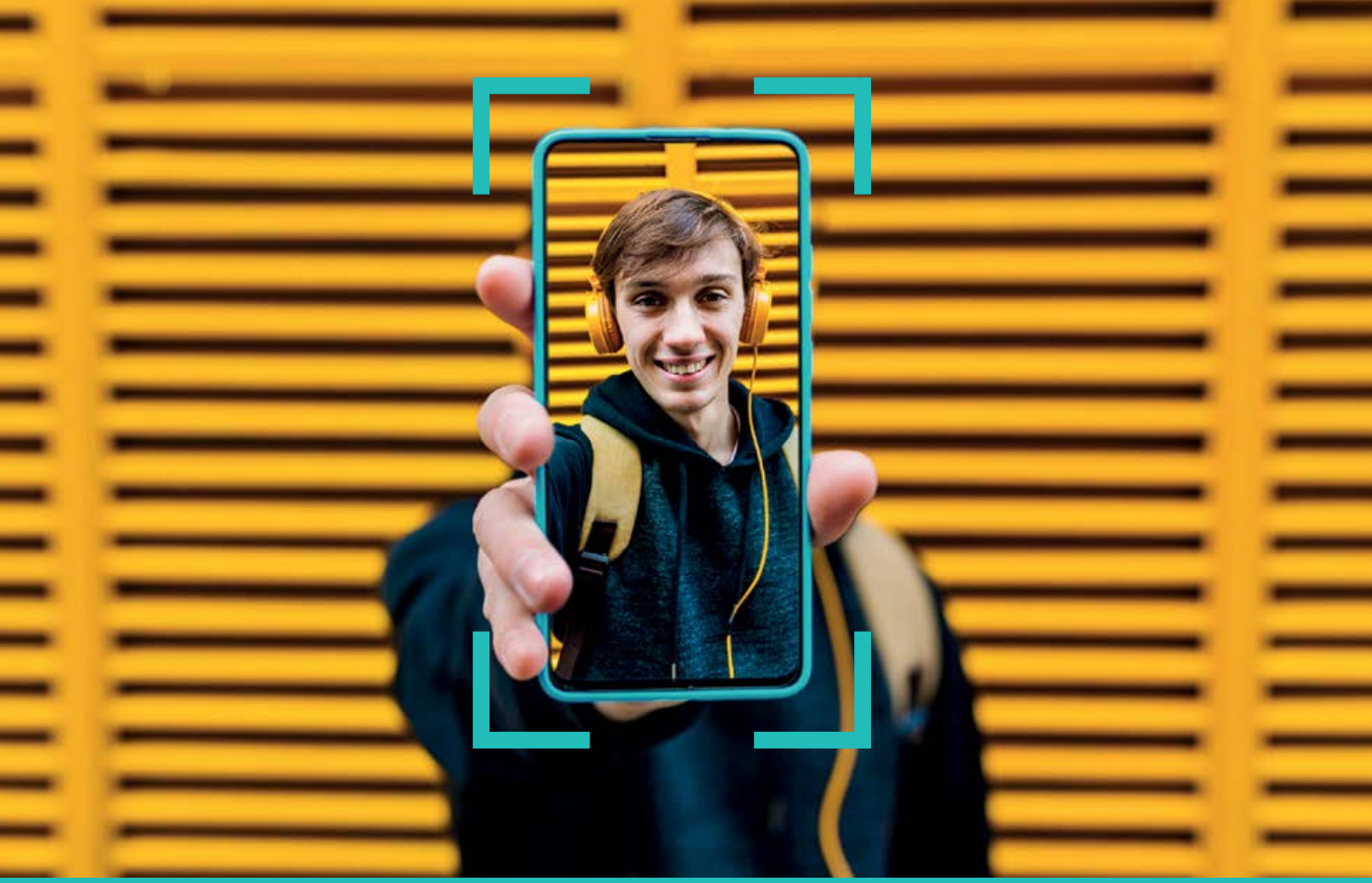
A short detour through history allows us to place the question of the three functions of money traditionally identified: standard of value, intermediary of exchanges, and reserve of value, in a broader framework. This perspective reveals a fourth fundamental function, identification, which denotes the monetary fact's common, political, and social origin.

Emerging monetary tools, such as bitcoin, state cryptocurrencies, or virtual currencies used in video games, give particular weight to this identification function and its political and social consequences.

The question of identification appears alongside Aristotle's analyses of money in Politics and Nicomachean Ethics, works that focus mainly on the polis, its limits, its organization, its justice. He thus develops, following Plato, a political and civic reflection that associates the limits of the polis with the birth of money, whose misuse can conflict with the rules of the ideal State: 1) by making the gain of foreign trade take precedence over the solidarity of internal exchanges; 2) by pricing the exchange value over the use-value; 3) by opening the infinite space of desires and speculations over the limited domain of needs.

„Today, new monetary innovations remind us of the importance of this fourth function of money - identification

In short, such a currency, freed from its civic dimensions, tends to become its own end, feeding inequalities and discord within the polis. This is why



Vaša šifra ste Vi

Evolucija sigurnosti sa biometrijom

Universal Capital Bank

Uvijek uz tebe!

call centar +382 20 67 33 11 | www.ucbank.me

„Leaving money in entirely private hands is not always a good idea, even if the management of money by States has also led to disasters

money, a political artifact, is also a marker of citizenship: its use inserts the user into a political, social, and ethical community and identifies them with it.

This function of identification through currency possession or use has not remained the prerogative of the Greek city-states: a constant feature of currencies is the concern of issuers – unless they are counterfeiters – to identify the origin of their currencies, usually territorial or political, by marks indicating the place of production, the issuer or the date.

The multiplication of social and complementary currencies since the 1970s corresponds, moreover, most often to a "territorial" project constituting a limited-size monetary space of solidarity. In this way, using money can become a militant act (sustainable, alternative, ecological economy…) and support or manifest an identity – this is notably the case with the Basque currency eusko.

CASH IS NOT SYNONYMOUS WITH ANONYMITY

This fourth function, this function of identification, is largely neglected in economics – historians and especially numismatists are, on the contrary, very attentive to it. However, taking it into account leads to two important contributions.

First, it reverses the usual perspective on anonymity. Anonymity no longer appears as a property of cash but becomes one of the modalities of identification by money, which allows a much more graduated approach.

Indeed, as we wrote in a research article in 2016, there is no "one" anonymity: anonymity is always, in fact, anonymity concerning a person or an institution. Consequently, it is susceptible to various configurations, which are part of a general identification function.

Thus, the usual payment in cash to a merchant that one knows does not, of course, entail any anonymity of the payer to the merchant. On the other hand, it does guarantee the anonymity of the merchant's customers to their banker or tax collector.

Similarly, using a contactless payment card results in almost complete anonymity of the customer towards the merchant. The payment receipt does not include any exploitable identity element but precisely identifies the customer to the bank issuing the payment card or the bank holding the merchant's accounts.

In general, a process of "nationalisation" of money has progressively made the limits of the modern state coincide with those of the monetary spaces of which these states have become the masters.

At the same time, the state assumes another function that is crucial for the proper functioning of civic and social life beyond payment systems alone: the identification of individuals. This function has grown considerably since the 19th century with the development of various forms of civil status and social security and the rise of enfranchisement and personal ballot.

Consequently, in a state governed by the rule of law, not only do individuals have a right to an identity that the State cannot deny them, but the methods of identification fall within the domain of the law, with the legal guarantees that surround it.

MONETARY INNOVATIONS CHANGE THE GAME

Today, new monetary innovations remind us of the importance of this fourth identification function. A first model, already old, consisted of delimiting virtual spaces within which specific monetary forms are employed: massively multiplayer "game" platforms

„Ostavljanje novca u potpuno privatnim rukama nije uvijek dobra ideja, čak i ako je upravljanje novcem od strane država takođe dovodilo do katastrofa

2) određivanjem cijene vrijednosti razmjeneiznad upotrebne vrijednosti; 3) otvaranjem beskonačnog prostora želja i spekulacija nad ograničenim domenom potreba.

Ukratko, takvavaluta, oslobođena svojih građanskih dimenzija, teži da postane svoj cilj, pothranjujući nejednakosti i razdor unutar polisa. Zbog toga je novac, politički artefakt, i oznaka građanstva: njegova upotreba ubacuje korisnika u političku, društvenu i etičku zajednicu i poistovjećuje ga s njom.

Ova funkcija identifikacije kroz posjedovanje ili korištenje valute nije ostala prerogativ grčkih gradova-država: stalna karakteristika valuta je briga emitenata – osim ako nisu falsifikatori – da identifikuju porijeklo svojih valuta, obično teritorijalno ili političko, oznakama koje označavaju mjesto proizvodnje, izdavaoca ilidatum.

Umnožavanje društvenih i komplementarnih valuta od 1970-ih godina odgovara, štaviše, najčešće „teritorijalnom“ projektu koji predstavlja ograničeni monetarni prostor solidarnosti. Na taj način korišćenje novca može postati militantni čin (održiva, alternativna, ekološka ekonomija...) i podržati ili ispoljiti identitet – to je posebno slučaj sabaskijskom valutomeusko.

GOTOVINA NIJE SINONIM ZA ANONIMNOST

Ova četvrta funkcija, ova funkcija identifikacije, u ekonomiji je u velikoj mjeri zanemarena – istoričari, a posebno numizmatičari, naprotiv, obraćaju pažnju na nju. Međutim, uzimanje u obzir vodi do dva važna doprinosa.

Prvo, preokreće uobičajenu perspektivu anonimnosti. Anonimnost se više ne pojavljuje kao svojstvogotovine ali postaje jedan od modaliteta identifikacije putem novca, što omogućava mnogo postupniji pristup.

Zaista, kao što smo pisali u jednom istraživačkom članku iz 2016. godine, ne postoji „ničija“anonimnost: anonimnost je uvijek, zapravo, anonimnost osobe ili institucije. Shodno tome, podložna je različitim konfiguracijama, koje su dio opšte funkcije identifikacije.

Dakle, uobičajenoplaćanjeu gotovini trgovcu za kojeg se zna, naravno, ne povlači za sobom nikakvu anonimnost platitioca prema trgovcu. S druge strane, garantuje anonimnost trgovčevih klijenata njihovom bankaru ili porezniku.

Slično, korišćenje beskontaktne platne kartice rezultira gotovo potpunom anonimnošću kupca prema trgovcu. Potvrda o uplati ne uključuje nijedan element identiteta koji se može iskoristiti, ali precizno identifikuje klijenta banci koja izdaje platnu karticu ili banci koja drži račune trgovca.

Uglavnom,proces “nacionalizacije” novcaje progresivno učinio da se granice moderne države poklapaju sa granicama monetarnih prostora kojima su ove države postale gospodari.

Istovremeno, država preuzima još jednu funkciju koja je ključna za pravilno funkcionisanje građanskog i društvenog života mimo samog platnog sistema: identifikaciju pojedinaca. Ova funkcija je značajno porasla od 19. vijeka sa razvojem različitih oblika građanskog statusa i socijalne sigurnosti i porastom biračkog prava i ličnog glasanja.

Shodno tome, u pravnoj državi, ne samo da pojedinci imaju pravo na identitet koji im država ne može uskratiti, već i metode identifikacije spadaju u domen zakona, sa pravnim garancijama koje ga okružuju.

generally provide techniques for accumulating symbols of wealth to attach objects, services, or skills avatars.

Already, in this case, the water-tightness between virtual and real is imperfect since player "farms" have emerged to acquire objects or abilities in the virtual universe that are then resold in real currency to players who wish to perform. In a way, this amounts to exchanging virtual currency for real currency via virtual goods and services.

In this context, identification takes place within the closed universe of the platform in question since the "identities" of the avatars are entirely controlled by the provider. The latter also determines the conditions of issue and use of "its" currency. We find again but are limited to a closed and virtual universe, the model of control of money and identities that territorial States carry out.

The second model, which is much more recent, stems from the innovation represented by the blockchain. The blockchain includes an identification device that validates the transaction between a seller and a buyer and makes the record of this validation available to other participants in the payment system.

On the one hand, identifying transactions makes it essential to identify the users who carry out exchanges. But on the other hand, this identity corresponds to the one declared within the virtual monetary space and not to an identity recognized by a State. Moreover, nothing prevents an economic agent from creating a different avatar for each of the existing cryptocurrencies or even associating different IP addresses (those that characterize the machines that access the Internet). It is no coincidence that Bitcoin has quickly become the preferred currency of cybercriminals.

This is where Facebook's Diem (ex-Libra) virtual currency project makes sense. Users have an identity guaranteed by the platform. More and more, rights and duties are attached concerning freedom of expression, the integrity of the "profile," and even the post-mortem destiny of accounts.

THE RISK OF A LUCRATIVE AND SELECTIVE FORM OF IDENTITY

Facebook is, therefore, able to identify its users very precisely. This is the core of its business model: selling the individual characteristics of these profiles. If a currency of its own, or almost, such as Diem, is associated with the Facebook ecosystem, the company or, more likely, the constellation of lucrative interests of which Facebook is the heart, will be able to simultaneously manage its own monetary assets and the proofs of identity-related to their use.

However, leaving money in entirely private hands is not always a good idea, even if the management of money by States has also led to disasters, such as the hyperinflationary episodes in Germany in 1923, Hungary in 1946, or Zimbabwe since 2000. Leaving the identification of human beings in private hands is even worse: what would happen to a human being whose only proof of existence is a private act, possibly transferable and of which third parties cannot become aware?

Thus, abandoning to the highest bidder these two key elements of the construction of the ancient polis or the modern State, which are money and identity, announces the worst of all worlds.

Solutions exist, old and new. Central bank digital currencies (CBDCs), being tested in Asia and Europe, bear witness to this. They limit the risk of substituting a lucrative form of identity for the civic form our rights depend on by subjecting payment to identification rather than the reverse.

In a world where the issuance of monetary assets, the creation of identities, and the management of the corresponding profiles are no longer the sole responsibility of nation-states, it is becoming urgent to reflect on the articulation of these different dimensions. Only then may we preserve the benefits of the innovations brought about by the rise of the Internet without losing our rights, our goods, and our beings. And therefore, we must take into account the fourth function of money: identification.

MONETARNE INOVACIJE MIJENJAJU IGRU

Danas nas nove monetarne inovacije podsjećaju na važnost ove četvrte funkcije identifikacije. Prvi model, već star, sastojao se od razgraničenja virtuelnih prostora unutar kojih se koriste specifični novčani oblici: platforme za masovne igre za više igrača generalno pružajutehnike za akumulisanje simbola bogatstvaza pričvršćivanje avatara objekata, usluga ili vještina.

Već, u ovom slučaju, vodonepropusnost između virtuelnog i stvarnog je nesavršena jer su se igračeve„farme"pojavile da bi kupili objekte ili sposobnosti u virtuelnom univerzumu koje se zatim preprodaju u stvarnoj valuti igračima koji žele da nastupaju. Na neki način, ovo se svodi na razmjenu virtuelne valute za stvarnu valutu putem virtuelne robe i usluga.

U ovom kontekstu, identifikacija se odvija unutar zatvorenog univerzuma dotične platforme budući da su „identiteti" avatara u potpunosti kontrolisani od strane provajdera. Provajderi takođe određuju uslove izdavanja i korišćenja „svoje" valute. Ponovo nalazimo, ali smo ograničeni na zatvoreni i virtuelni univerzum, model kontrole novca i identiteta koji sprovode teritorijalne države.

Drugi model, koji je mnogo noviji, proizlazi iz inovacije koju predstavlja blokčejn. Blokčejn uključuje identifikacioni uređaj koji potvrđuje transakciju između prodavca i kupca i čini evidenciju ove validacije dostupnom drugim učesnicima u platnom sistemu.

S jedne strane, identifikacija transakcija čini od suštinskog značaja za identifikaciju korisnika koji vrše razmjenu. Ali, s druge strane, ovaj identitet odgovara onom koji je deklarisan u virtuelnom monetarnom prostoru, a ne identitetu koji priznaje država. Štaviše, ništa ne sprečava ekonomskog agenta da kreira drugačiji avatar za svaku od postojećih kriptovaluta ili čak da poveže različite IP adrese (one koje karakterišu mašine koje pristupaju Internetu). Nije slučajno što je Bitcoin brzo postaopreferirana valuta sajber kriminalaca.

Evo gdjeFacebookov Diem(ex-Libra) projekat virtuelne valute ima smisla. Korisnici imaju identitet zagarantovan platformom. Sve više se pripisuju prava i dužnosti u vezi sa slobodom izražavanja, integritetom „profila", pa čak i posmrtnom sudbinom naloga.

RIZIK LUKRATIVNOG I SELEKTIVNOG OBLIKA IDENTITETA

Facebook je, dakle, u mogućnosti da vrlo precizno identifikuje svoje korisnike. To je srž njegovog poslovnog modela: prodaja individualnih karakteristika ovih profila. Ako je sopstvena valuta, ili skoro, kao što je Diem, povezana sa Facebook ekosistemom, kompanija ili, što je vjerovatnije, sazviježđe unosnih interesa čije je srce Facebook, moći će istovremeno da upravlja sopstvenim novčanim sredstvima i dokazima o identitetu koji se odnose na njihovu upotrebu.

Međutim, ostavljanje novca u potpuno privatnim rukama nije uvijek dobra ideja, čak i ako je upravljanje novcem od strane država takođe dovodilo do katastrofa, kao što su hiperinflacijske epizode uNemačkoj 1923. godine,Mađarskoj 1946. godine, iliZimbabveu od 2000. godine. Ostavljanje identifikacije ljudskih bića u privatnim rukama je još gore: šta bi se dogodilo sa ljudskim bićem čiji je jedini dokaz postojanja privatni čin, eventualno prenosiv i kojeg treće strane ne mogu saznati?

Dakle, prepuštanje onima koji najviše ponude ova dva ključna elementa izgradnje antičkog polisa ili moderne države, a to su novac i identitet, najavljuje najgori od svih svjetova.

Rešenja postoje, stara i nova.Digitalne valute centralnih banaka(CBDC), koje se testiraju u Aziji i Evropi, svjedoče o tome. One ograničavaju rizik zamjene unosnog oblika identiteta sa građanskim oblikom od kojeg zavise naša prava podvrgavanjem plaćanja identifikaciji, a neobrnuto.

U svijetu u kojem izdavanje novčanih sredstava, stvaranje identiteta i upravljanje odgovarajućim profilima više nisu isključiva odgovornost nacionalnih država, postaje hitno da se počne sa razmišljanjem o artikulaciji ovih različitih dimenzija. Samo tada možemo sačuvati prednosti inovacija koje je donio uspon interneta, a da pritom ne izgubimo svoja prava, svoja dobra i svoja bića. I stoga, moramo uzeti u obzir četvrtu funkciju novca: identifikaciju.

TRADICIJA DUGA PREKO 150 GODINA

020 442 200

www.ziraatbank.me

Ziraat Bank
Montenegro

Udruženje banaka
Crne Gore

Association of
Montenegrin Banks

Udruženi oko zajedničkog cilja

Addiko Bank AD Podgorica
Adriatic bank
Crnogorska komercijalna banka AD Podgorica
Erste Bank AD Podgorica
Hipotekarna Banka AD Podgorica
Lovćen banka AD
NLB Banka
Prva banka Crne Gore 1901.
Universal Capital Bank
Zapad Banka AD Podgorica
Ziraat Bank