Wijzig het digitale-eurovoorstel van een risico in een kans voor privacy

Eind juni diende de Europese Commissie een wetsvoorstel in voor de invoering van een digitale euro. Wat betekent dit digitale-eurovoorstel voor de betaalprivacy, en is dit wel wenselijk?

MAARTEN VAN OORDT
Universitair hoofddocent aan de Vrije Universiteit Amsterdam

IN HET KORT

- In twintig jaar is de privacy omtrent betalingen sluipenderwijs sterk afgenomen door veranderingen in het betalingsverkeer en regelgeving.
- De invoering van de digitale euro volgens de huidige plannen van de Europese Commissie dreigt de betaalprivacy verder te ondermijnen.
- Er is maatschappelijke behoefte aan betaalprivacy en technisch is dit ook mogelijk met digitaal geld. Tijd om het voorstel aan te passen!

De afgelopen twintig jaar heeft er een ingrijpende omwenteling plaatsgevonden in het gebruik van contant geld als betaalmiddel. In 2002 bedroeg het percentage betalingen bij verkooppunten met contant geld nog 85 procent; in 2022 was dit percentage teruggelopen tot slechts 20 procent (Brits en Winder, 2005; DNB en Betaalvereniging Nederland, 2022). Gelijktijdig is er sprake van een toenemend aandeel van betalingen-op-afstand waarbij het gebruik van contant geld niet praktisch uitvoerbaar is. Deze omwenteling in het gebruik van contant geld vond plaats tegen een achtergrond van zowel verbeteringen in de elektronische betaalmethoden (zoals contactloze betalingen) als een verminderde toegankelijkheid en acceptatie van contant geld.

Sluipenderwijs heeft de verschuiving in het betaallandschap ook een achteruitgang teweeggebracht in de privacy omtrent betalingen. Bij reguliere elektronische betalingen worden automatisch gedetailleerde gegevens vastgelegd door betaaldienstverleners, waaronder banken. Deze gegevens specificeren bijvoorbeeld de verzender, de begunstigde, het bedrag en het tijdstip van een betaling. Wanneer dezelfde betaling plaatsvindt met contant geld, dan zou slechts de consument, en in sommige gevallen de winkelier, over deze gegevens beschikken. Betaaldienstverleners kunnen de verzamelde betaalinformatie binnen bepaalde kaders voor commerciële doeleinden gebruiken. Tevens eist de wetgever in toenemende mate dat financiële instellingen een fijnmazige surveillance uitvoeren op de betaalrekeningen van consumenten en rechtspersonen.

Dit stuk is deels gebaseerd op Garratt en Van Oordt (2021) en Van Oordt (2022).

ROL VAN DE DIGITALE EURO

Het recente wetsvoorstel van de Europese Commissie (2023) voor de invoering van de digitale euro is een belangrijk moment om als samenleving stil te staan bij het gewenste niveau van privacy omtrent betalingen (EC, 2023). Ten eerste is het aannemelijk dat het gebruik van contant geld verder onder druk komt te staan als gevolg van de invoering van een concurrerend betaalmiddel als de digitale euro (Huynh et al., 2020; Li, 2023). Ten tweede bestaat er een scala aan technische mogelijkheden waardoor de privacy omtrent digitale-eurobetalingen beter gewaarborgd zou kunnen worden dan bij de bestaande elektronische betaalmiddelen. Deze variëren van cryptografische technieken, waarmee betalingen met online-tegoeden niet langer herleidbaar zijn tot technieken waarbij er sprake is van een asymmetrische privacy. Door de toepassing van dit soort technieken kan men bijvoorbeeld bereiken dat de verzender van gelden niet herleidbaar is maar de omvang van ontvangen gelden wel, dat kleinere betalingen niet herleidbaar zijn, of dat de betaler of ontvanger indien gewenst de anders onleesbare betaaldata kan delen (Chaum et al., 2021; Gross et al., 2021; Tinn en Dubach, 2021). Afhankelijk van het ontwerp kan de invoering van de digitale euro de privacy omtrent betalingen zowel ondermijnen als bevorderen.

Het belang van het privacy-aspect van het digitale-euro-ontwerp blijkt ook uit de breed gedragen vraag naar privacy omtrent betalingen vanuit de samenleving. Privacy omtrent betalingen kreeg veruit het grootste aantal stemmen als de meest gewenste functionaliteit in de publieke consultatie voor de digitale euro (ECB, 2021). Dichter bij huis ontving privacy voor digitale-eurorekeningen van Nederlandse respondenten maar liefst een gemiddelde score van 4,5 op een schaal van 1 tot 5 (van 'totaal onbelangrijk' tot 'erg belangrijk') in een onderzoek van De Nederlandsche Bank (Bijlsma et al., 2021). In buurland Duitsland gaf meer dan 90 procent van de respondenten aan het belangrijk te vinden dat gegevens over digitale-eurobetalingen een privézaak zullen zijn (Deutsche Bundesbank, 2021).

BETAALPRIVACY IN EEN RECHTSSTAAT

Een verregaande inperking van de privacy bij elektronische betalingen wordt veelal gepropageerd vanuit de doctrine dat surveillance van het betalingsverkeer bijdraagt aan de bestrijding van belastingontduiking en criminaliteit. Echter, hoewel de bestrijding van belastingontduiking en criminaliteit belangrijke overheidstaken zijn, betekent dit niet dat een verregaande surveillance van het betalingsverkeer zonder meer gerechtvaardigd is binnen een rechtsstaat. Zo is er ook sprake van een grotere effectiviteit van criminaliteitsbestrijding wanneer opsporingsinstanties onbeperkt woningen zouden kunnen doorzoeken of afluisterapparatuur zouden kunnen plaatsen – terwijl ook daar beperkingen aan worden gesteld. Een rechtsstaat onderscheidt zich daarin van een totalitaire staat dat er in de laatste rechtens geen grens is aan overheidsinterventie (Kortmann, 1997). Dit verschil uit zich onder meer door het waarborgen van klassieke grondrechten, waaronder de eerbiediging van de persoonlijke levenssfeer, correspondentie en het huis (Europees Verdrag voor de Rechten van de Mens, Art. 8). In dit kader is het vrijwel onbeperkte onderzoek naar de huishoudboekjes van Nederlandse burgers een opmerkelijke ontwikkeling te noemen. Of dit onderzoek direct plaatsvindt door de uitvoerende macht zelf, of door werknemers van derden met meldingsplicht (Wet ter voorkoming van witwassen en financieren van terrorisme, Art. 16-17), is daarbij vooral een optisch verschil.

Dat directe of indirecte beschikking over betaaldata samengaat met vérstrekkende mogelijkheden tot handhaving lijdt geen twijfel. Een voorbeeld is de recente reactie van de Canadese regering nadat er grotendeels vreedzame, maar ook langdurige demonstraties plaatsvonden tegen maatregelen waardoor ongevaccineerde vrachtwagenchauffeurs werkloos dreigden te raken. Na frustratie over het voortduren van de demonstraties riep de premier op 14 februari 2022 de noodtoestand uit. Een dag later gebruikte de regering de extra bevoegdheden om een noodbevel uit te vaardigen (Canada Gazette, 2022). Dit noodbevel gaf financiële instellingen de opdracht om zonder gerechtelijk bevel de bankrekeningen te bevriezen van een ieder die de demonstranten financieel ondersteunde. Voor de uitvoering van het noodbevel was een beperkte donatie van bijvoorbeeld twintig dollar in principe al voldoende om te kwalificeren als financiële steun, zoals een hoge ambtenaar voor parlementariërs verklaarde (Canadian

House of Commons, 2022). Ongeacht of men het eens of oneens is met de demonstranten laat deze episode weinig aan de fantasie over wat betreft het overheidsingrijpen dat mogelijk is wanneer de overheid direct of indirect kan beschikken over betaaldata, ook in een liberale democratie.

ECONOMISCHE LITERATUUR

Ook de economische literatuur draagt verscheidene argumenten aan voor een hoge mate van privacy omtrent betalingen, of de keuze daartoe voor consumenten. In de literatuur wordt er onderscheid gemaakt tussen de *intrinsieke* en de *instrumentele* waarde van privacy. Bij de intrinsieke waarde gaat het om de waarde die het individu er op zichzelf aan hecht om niet waargenomen te worden, onafhankelijk van potentiële andere voordelen of resultaten die door privacy bereikt kunnen worden. De instrumentele waarde slaat op de waarde van privacy voor het individu vanwege de potentiële gevolgen die het delen van informatie kan hebben (Acquisti et al., 2005). Hierbij kan men onder meer denken aan het vermijden van intimidatie, bijvoorbeeld op basis van giften aan maatschappelijke bewegingen of gênante betalingen voor medische behandelingen, aan het vermijden van spam of gerichte reclame, en aan het vermijden van misbruik van gegevens voor bijvoorbeeld identiteitsdiefstal (Kahn et al., 2005; Kahn, 2018).

Behalve regelgeving kan ook marktfalen leiden tot een gebrek aan privacy omtrent betalingen. Het model van Garratt en Van Oordt (2021) illustreert hoe het delen van betaaldata de norm kan worden, zelfs wanneer betaalprivacy een hoge waardering krijgt binnen de samenleving als geheel. De oorzaak is een negatieve externaliteit: marketeers kunnen betaaldata van de ene consument gebruiken om voorspellingen te doen over het koopgedrag van andere consumenten, zelfs wanneer die andere consumenten stappen hebben ondernomen om hun eigen gegevens te beschermen. Privacy is een publiek goed omdat het alle consumenten gezamenlijk beschermt, in dit specifieke model tegen schadelijke prijsdiscriminatie. Net als bij andere publieke goederen, zoals schone lucht, komt het maatschappelijke voordeel van de eigen bijdrage slechts voor een klein deel bij het individu terecht. Hierdoor zijn individuen geneigd om relatief weinig moeite te doen om de eigen betaalprivacy te beschermen. Een kosteneffectief digitaal betaalmiddel dat de privacy wel beschermt, kan dan een oplossing bieden.

Een privacybeschermend betaalmiddel kan zelfs positief bijdragen aan het welzijn van consumenten in modellen waar het delen van betaaldata op zichzelf genomen positieve effecten zou kunnen hebben. In het model van Garratt en Lee (2022) benutten bedrijven betaaldata om producten te ontwikkelen die beter bij de voorkeuren van consumenten passen. De voordelen daarvan komen echter niet bij de consument terecht. De data-gedreven verbeteringen leiden tot een marktstructuur met een dominant bedrijf dat een datamonopolie bezit. De monopolist is pas bereid om de voordelen van betaaldata te delen met consumenten wanneer zij de keuze zouden hebben om die data te veilig te stellen met een privacybeschermend betaalmiddel. Een vergelijkbaar principe keert terug in het model van Ahnert et al. (2022), waarin het monitoren van betaalrekeningen de bancaire kredietverlening bevordert. In dat model kan het datamonopolie van de huisbank worden doorbroken door de invoering van een privacybeschermend digitaal betaalmiddel.

Ook marktfalen kan leiden tot een gebrek aan privacy

LACUNE IN HET BETAALLANDSCHAP

Momenteel is de mate van betaalprivacy afhankelijk van de vraag of een betaling *in-persoon* of *op-afstand* plaatsvindt (figuur 1). Voor betalingen in-persoon biedt contant geld een hoge mate van privacy; relatief weinig privacy wordt geboden door betalingen in de vorm van tegoeden op betaalrekeningen met de daarbij behorende elektronische betaalmiddelen (bijvoorbeeld 'pinnen' of een 'tikkie'). Voor betalingen op-afstand bieden reguliere betaalmiddelen in de praktijk

Privacy voor reguliere betalingen zonder en met het digitale-eurovoorstel

TABEL 1

	Veel privacy	Weinig privacy
In-persoon	Contant geld (voorstel: offline digitale euro)	Betaalrekening (voorstel: online digitale euro)
Op-afstand	–	Betaalrekening (voorstel: online digitale euro)

Toelichting: Betalingen met contant geld vinden plaats door het overdragen van papiergeld en munten. Betalingen in de vorm van een tegoed op een betaalrekening kunnen bijvoorbeeld plaatsvinden in de vorm van pinbetalingen of bankoverschrijvingen. Reguliere elektronische betaalmiddelen, waarbij de betaling niet direct ten laste komt van het tegoed op een betaalrekening, zoals bij een creditcard, kunnen voor het doel van de figuur worden beschouwd als betaalmiddelen met weinig privacy.

weinig privacy. In figuur 1 blijkt deze lacune in het betaallandschap uit het lege vak linksonder.

De geschetste lacune wat betreft privacy voor betalingen op-afstand speelt een steeds grotere rol. Zo is er een gestage groei in het aandeel van betalingen op-afstand. Ook is er een sterke toename in de inzet van nieuwe technieken voor de verwerking en de analyse van grote hoeveelheden gegevens voor zowel *compliance* als commerciële doeleinden. Meer dan ooit wordt hierdoor gebruikgemaakt van opgeslagen betaalgegevens. Tenslotte betekent het voortbestaan van contant geld niet dat het individu dezelfde keuzevrijheid heeft voor privacy bij in-persoon-betalingen als voorheen: deze vrijheid staat onder druk door zowel een afname van de acceptatie van contant geld als een toename in de effectieve kosten bij het gebruik ervan.

HET DIGITALE-EUROVOORSTEL

In zijn huidige vorm beoogt het digitale-eurovoorstel (EC, 2023) om het betaallandschap aan te vullen met betaalmiddelen voor twee soorten digitale-eurotegoeden. Het gaat daarbij om *central bank digital currency* (CBDC) omdat de digitale tegoeden directe passiva zijn op de balans van de monetaire autoriteit. De twee soorten tegoeden moeten het mogelijk maken om digitale-eurobetalingen uit te voeren in respectievelijk een online- en een offline-context (EC, 2023, Art. 23). Betalingen met online- en offline-tegoeden zullen verschillende eigenschappen hebben vanuit een privacy-oogpunt.

Het doel is dat betalingen met online-tegoeden op een vergelijkbare manier zullen functioneren als betalingen met een betaalrekening bij een commerciële bank. Het digitale-eurovoorstel beoogt ook dat het beheer van online-tegoeden zal worden aangeboden via bestaande banken en mogelijk andere partijen (EC, 2023, Art. 14). De beoogde betaalfunctionaliteit voor online-tegoeden omvat zowel in-persoon-betalingen als betalingen op-afstand.

Vanuit een privacy-perspectief bieden betalingen met online digitale-eurotegoeden onder het huidige voorstel niet bepaald een verbetering ten opzichte van de bestaande situatie (zie ook figuur 1). Het voorstel beoogt dat het betaalverkeer met online digitale-eurotegoeden in essentie onder dezelfde surveillance-wetgeving zal vallen als betalingen met reguliere banktegoeden (EC, 2023, Art. 5). Ook worden alle betalingen verwerkt via het systeem van de Europese Centrale Bank, waar er een relatief zwakke techniek van pseudoniemen ('user identifiers') zal worden gebruikt om het individu te beschermen tegen de traceerbaarheid door de centrale bank (EC, 2023, Art. 2 en Annex IV). Ten slotte voorziet het voorstel ook in coördinatie tussen aanbieders van digitale-eurorekeningen en de centrale bank om te voorkomen dat het totale digitale-eurotegoed van een individu met meerdere digitale-eurorekeningen uitstijgt boven een voorgeschreven maximum per persoon (EC, 2023, Art. 16).

De beoogde betalingen met offline-tegoeden functioneren in bepaalde opzichten op vergelijkbare wijze als wat er in Nederland bekend stond als de Chipknip. Offline-tegoeden worden ter plaatse opgeslagen met behulp van een beveiligde chip in een betaalkaart of telefoon. Deze tegoeden kan men dan gebruiken voor betalingen tussen apparaten zonder een connectie te maken met een betaaldienstverlener of de centrale bank (EC, 2023, Art. 37). Het digitale-eurovoorstel beoogt ook dat betalingen met offline-tegoeden technisch beperkt zullen worden zodat deze slechts gebruikt kunnen worden voor betalingen in-persoon, waarbij de apparaten zich in elkaars nabijheid bevinden, en niet voor betalingen op-afstand (EC, 2023, Art. 2).

Vanuit het oogpunt van privacy beoogt het voorstel dat betalingen met offline-tegoeden worden gekenmerkt

door een relatief hoge mate van betaalprivacy ten opzichte van betalingen met online-tegoeden. Zo is het de intentie dat offline-betalingen tussen twee apparaten niet worden opgeslagen door betaaldienstverleners of de monetaire autoriteit. Wel beoogt het voorstel dat data worden opgeslagen wanneer een offline-tegoed wordt gestort op een online digitale-eurorekening, of juist wordt opgenomen. Deze data omvatten onder meer een unieke apparaat-code, als ook de gebruikte tegenrekening (EC, 2023, Art. 37).

Bij het beoogde privacy-ontwerp voor offline-betalingen zijn er verschillende kanttekeningen te plaatsen. Ten eerste is het niet onwaarschijnlijk dat de praktische bruikbaarheid voor dagelijkse betalingen ondermijnd zal worden door de lagere limieten die voor offline-tegoeden zullen gelden (EC, 2023, Art. 37). Een van de gestelde doelen van de lagere limieten is de bestrijding van de financiering van terrorisme. Helaas leert de praktijk dat terroristische aanslagen weinig financiële middelen vereisen (Oftedal, 2015). Betaallimieten bij offline-betalingen zouden dus zeer laag moeten zijn om effectief te zijn in het voorkomen van terroristische aanslagen. Ten tweede is er twijfel over de technische haalbaarheid van de beoogde privacy vanuit een beveiligingsperspectief. Een cruciale beveiligingskwestie bij offline-tegoeden is het voorkomen van situaties waarin kwaadwillenden de beveiliging doorbreken, zodat zij hetzelfde saldo meerdere keren kunnen uitgeven. Controle daarop vereist het nagaan of hetzelfde offline-geld niet meerdere keren wordt ingewisseld. Gericht ingrijpen wordt moeilijk wanneer het onmogelijk is om de oorsprong van offline-geld via de achterdeur te herleiden. Ten slotte is het vermeldenswaard dat, als mogelijke functionaliteit, het automatische herstel van offline-tegoeden op gesneuvelde of verloren apparaten vereist dat er betaaldata worden verwerkt om te verifiëren welke tegoeden al zijn uitgegeven (Kahn et al., 2021, 2022).

EINDOORDEEL

Het is waarschijnlijk dat de invoering van de digitale euro, zoals vormgegeven in het huidige voorstel van de Europese Commissie, de privacy omtrent betalingen verder zal ondermijnen. Met een ander ontwerp zou de digitale euro aanzienlijke vooruitgang kunnen boeken op het gebied van betaalprivacy, met name door betalingen op afstand met veel privacy mogelijk te maken. Dit is in het huidige digitale-eurovoorstel niet het geval. Ook betekenen digitale-eurobetalingen, in vergelijking tot het bestaande reguliere betaallandschap, veeleer een verslechtering dan een verbetering vanuit een privacy- perspectief. Gezien de ontwikkelingen op technisch gebied en de vraag om betaalprivacy vanuit de samenleving bestaat er nu een reëel risico dat de digitale euro daarmee een belangrijke kans zal laten liggen.

LITERATUUR

Acquisti, A., C. Taylor en L. Wagman (2016) The economics of privacy. *Journal of Economic Literature*, 54(2), 442–492.

Ahnert, T., P. Hoffmann en C. Monnet (2022) *The digital economy, privacy, and CBDC*. European Central Bank Working Paper, 2662.

Bijlsma, M., C. van der Cruijsen, N. Jonker en J. Reijerink (2021) *What triggers consumer adoption of CBDC?* De Nederlandsche Bank Working Paper, 709.

Brits, H. en C. Winder (2005) *Payments are no free lunch*. De Nederlandsche Bank Occasional Study 2005-2.

Canada Gazette (2022) Emergency Economic Measures Order: SOR/2022-22. *Canada Gazette*, Part II, 156 (Extra Number 1).

Canadian House of Commons (2022) *Standing Committee on Finance: Evidence (February 22). Volume 44-1 FINA-21*. Te vinden op tiny.cc/ykgavz.

Chaum, D., C. Grothoff en T. Moser (2021) *How to issue a central bank digital currency*. Swiss National Bank Working Paper, 2021-03.

Deutsche Bundesbank (2021) What do households in Germany think about the digital euro? *Deutsche Bundesbank Monthly Report*, oktober, 65–84.

DNB en Betaalvereniging Nederland (2022) *Point of sale payments in 2022*. DNB Rapport.

ECB (2021) *Eurosystem report on the public consultation on a digital euro*. ECB Rapport, april.

Europese Commissie (2023) *Proposal for a regulation of the European Parliament and of the Council on the establishment of the digital euro*, 2023/0212 (COD). Te vinden op eur-lex.europa.eu.

Garratt, R.J. en M.R.C. van Oordt (2021) Privacy as a public good: A case for electronic cash. *Journal of Political Economy*, 129(7), 2157–2180.

Garratt, R.J. en M.J. Lee (2021) *Monetizing privacy with central bank digital currencies*. Federal Reserve Bank of New York Staff Report, 958.

Gross, J., J. Sedlmeir, M. Babel et al. (2021) *Designing a central bank digital currency with support for cash-like privacy*. SSRN Working Paper.

Huynh, K., J. Molnar, O. Shcherbakov en Q. Yu (2020) *Demand for payment services and consumer welfare: The introduction of a central bank digital currency*. Bank of Canada Staff Working Paper, 2020-7.

Kahn, C.M. (2018) The threat of privacy. *Journal of Financial Market Infrastructures*, 6(2/3), 1–10.

Kahn, C.M., J. McAndrews en W. Roberds (2005) Money is privacy. *International Economic Review*, 46(2), 377–399.

Kahn, C.M., M.R.C. van Oordt en Y. Zhu (2021) *Best before? Expiring central bank digital currency and loss recovery*. Bank of Canada Staff Working Paper, 2021-67.

Kahn, C.M., M.R.C. van Oordt en Y. Zhu (2022) *Best before: Personal loss recovery for offline digital cash*. Voxeu Column, 18 februari. Te vinden op cepr.org.

Kortmann, C.A.J.M. (1997) *Constitutioneel recht*. Deventer: Kluwer.

Li, J. (2023) Predicting the demand for central bank digital currency: A structural analysis with survey data. *Journal of Monetary Economics*, 134, 73–85.

Oftedal, E. (2015) *The financing of jihadi terrorist cells in Europe*. Forsvarets Forskningsinstitutt (Norwegian Defence Research Establishment,) Rapport, 2014/02234.

Oordt, M.R.C. van (2022) Discussion of 'Central bank digital currency: Stability and information'. *Journal of Economic Dynamics and Control*, 104, 104503.

Tinn, K. en C. Dubach (2021) *Central bank digital currency with asymmetric privacy*. SSRN Working Paper.