Het opslaan van kopieën van legitimatiebewijzen, foto's en video's van cliënten: de grenzen van de Wwft-reconstructieplicht in het licht van fundamentele rechten

Mekić, D.

*D. Mekić**

Het opslaan van kopieën van legitimatiebewijzen, foto's en video's van cliënten: de grenzen van de Wwft-reconstructieplicht in het licht van fundamentele rechten

2

1 Inleiding

In 2022 werd 1 op de 100 Nederlandse ingezetenen van 15 jaar of ouder slachtoffer van identiteitsfraude.[1] Uit onderzoek naar meldingen van identiteitsfraude in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties blijkt dat de identiteitsfraude het vaakst voorkomt met kopieën van legitimatiebewijzen (38%).[2] Volgens datzelfde onderzoek vinden de meeste identificaties waarbij vaak kopieën van legitimatiebewijzen worden gemaakt, plaats bij instellingen die vallen onder de reikwijdte van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft).[3]

De Wwft geeft uitvoering aan de vierde anti-witwasrichtlijn (4AMLD), die gewijzigd is door de vijfde anti-witwasrichtlijn (5AMLD),[4] en heeft als doel om witwassen en terrorismefinanciering te bestrijden door 'poortwachters' in staat te stellen ongebruikelijke transacties te melden die relevant kunnen zijn voor het opsporen van strafbare feiten.[5] Daarom moet een breed scala aan instellingen die vallen onder de Wwft[6] de identiteit van hun cliënten verifiëren bij een incidentele transactie,[7] of wanneer zij hiermee een zakelijke relatie aangaan (de verificatieplicht).[8] Nadat is voldaan aan de verificatieplicht moet de instelling een aantal gegevens van de cliënt vastleggen (de reconstructieplicht).[9]

Om in een tijd zonder snelle computers en grootschalige beschikbaarheid van automatische tekstherkenning op een 'efficiënte wijze' te kunnen voldoen aan deze reconstructieplicht, biedt de Wwft sinds 2008 de mogelijkheid om een 'afschrift van het document dat een persoonidentificerend nummer bevat en aan de hand waarvan de verificatie van de identiteit heeft plaatsgevonden' (hierna: kopie legitimatiebewijs) vast te leggen, in plaats van de geslachtsnaam, de voornamen, de geboortedatum, het adres en de woonplaats van de cliënt, alsmede de aard, het nummer en de datum en plaats van uitgifte van het document waarmee

---

* Mr. drs. Danny Mekić is promovendus bij eLaw, Centrum voor Recht in de Informatiemaatschappij, van de Universiteit Leiden, onder gezamenlijke supervisie met de Eindhoven University of Technology, waar hij gastonderzoeker is bij de onderzoeksgroep Technologie, Innovatie en Samenleving. Hij doet onderzoek naar het fundamentele recht op menselijke waardigheid in relatie tot de aggregatieve impact van digitale technologieën op privacy en gegevensbescherming, en is daarnaast werkzaam als managementadviseur. De auteur bedankt prof. mr. Anna Berlee en prof. mr. Jac Rinkes voor hun waardevolle inzichten en begeleiding bij het schrijven van de masterscriptie waar dit artikel gedeeltelijk op is gebaseerd.

1 Centraal Bureau voor de Statistiek (CBS), *Veiligheidsmonitor 2022* 11 mei 2023.
2 Zie G. Bummelkamp e.a., *Monitor Identiteit 2021*, maart 2022, p. 57. Zie ook Ellen Timmer, 'Informatie over identificatie en identiteitsfraude | Monitor Identiteit 2021', ellentimmer.com, 20 juni 2022.
3 *Stb.* 2008, 303. Zie G. Bummelkamp e.a., *Monitor Identiteit 2021*, maart 2022, p. 21.
4 De vierde anti-witwasrichtlijn Richtlijn (EU) 2015/849 van het Europees Parlement en de Raad van 20 mei 2015 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, tot wijziging van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad en tot intrekking van Richtlijn 2005/60/EG van het Europees Parlement en de Raad en Richtlijn 2006/70/EG van de Commissie (*4AMLD*), zoals gewijzigd door de vijfde anti-witwasrichtlijn Richtlijn (EU) 2018/843 van het Europees Parlement en de Raad van 30 mei 2018 tot wijziging van Richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van de Richtlijnen 2009/138/EG en 2013/36/EU (*5AMLD*).
5 *Kamerstukken II* 1992/93, 23009 (*MvT bij Wet melding ongebruikelijke transacties*), p. 4 en *Kamerstukken II* 2007/08, 31238 (*MvT bij Wet ter voorkoming van witwassen en financieren van terrorisme – Samenvoeging van de Wet identificatie bij dienstverlening en de Wet melding ongebruikelijke transacties*), nr. 3, p. 35.
6 Het meest bekend zijn banken en financiële dienstverleners. Echter, na uitbreidingen van art. 4 Wwft vallen ook aanbieders van kansspelen op afstand, accountants, advocaten, belastingadviseurs, beleggingsinstellingen, beleggingsondernemingen, bemiddelaars bij koop en verkoop in zaken van grote waarde, bemiddelaars in levensverzekeringen, beroeps- of bedrijfsmatige aanbieders van bewaarportemonnees en diensten voor het wisselen tussen virtuele valuta en fiduciaire valuta, betaaldienstagenten, betaaldienstverleners, domicilieverleners, elektronischgeldinstellingen, instellingen niet zijnde een bank die bancaire activiteiten verrichten, instellingen voor collectieve belegging in effecten, juridische dienstverleners, kopers of verkopers van goederen en kunstvoorwerpen, levensverzekeraars, makelaars, notarissen, pandhuizen, speelcasino's, taxateurs, trustkantoren, verhuurders van safes en wisselinstellingen onder de reikwijdte van de Wwft.
7 In sommige gevallen gelden drempels, zie art. 3 Wwft.
8 Aanbeveling 10 van de *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation,* afkomstig van de Financial Action Task Force on Money Laundering (FATF), Parijs 2012-2023, p. 14-15. Deze aanbeveling is omgezet in art. 11 en art. 13 lid 1 onder a 4AMLD. In Nederland is deze omgezet in art. 11 lid 1 Wwft.
9 Aanbeveling 11 FATF 2012-2023, p. 15. Deze is omgezet in art. 40 lid 1 4AMLD. In Nederland is deze omgezet in art. 33 lid 2 Wwft.

de identiteit van die cliënt is geverifieerd (hierna: de identiteitsgegevens).[10] Iedereen die een bankrekening opent of gebruikmaakt van dienstverleners die vallen onder de reikwijdte van de Wwft komt in aanraking met deze verificatie- en reconstructieplicht. Daarom raken deze maatregelen vroeg of laat nagenoeg ieder lid van de bevolking.

Ondanks het risico dat het bewaren van kopieën van legitimatiebewijzen met zich meebrengt, geven de bij de Wwft betrokken toezichthouders in richtsnoeren verschillende interpretaties van de reconstructieplicht.[11] Deze variëren van dat het bewaren van een kopie van het legitimatiebewijs van cliënten 'niet verplicht' is,[12] 'kan',[13] 'mag',[14] 'verwacht wordt' (inclusief pasfoto),[15] 'van elke klant (…) verplicht' zou zijn,[16] tot de interpretatie dat de reconstructieplicht ook de verplichting behelst om audio- en video-opnamen van cliënten te maken en bewaren (bij geautomatiseerde identiteitsverificaties zonder menselijke tussenkomst).[17] Deze uiteenlopende interpretaties kunnen leiden tot inconsistenties in de naleving door de instellingen en tot onduidelijkheid bij de cliënten over wat nu exact van hen verwacht wordt in het kader van de Wwft. Deze onduidelijkheid is de aanleiding voor dit artikel.

Het bewaren van kopieën van legitimatiebewijzen, foto's en audio- en video-opnamen van cliënten vormt bovendien een inperking van het fundamentele recht op privacy en gegevensbescherming zoals vastgelegd in artikel 8 van het Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (hierna: EVRM),[18] en de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie (hierna: Handvest).[19] Daarom moet bij de uitvoering van de reconstructieplicht in het kader van de identiteitsverificatie van cliënten rekening worden gehouden met de vereisten van artikel 8, tweede lid, van het EVRM en artikel 52 van het Handvest, en moet de uitvoering in overeenstemming zijn met de jurisprudentie van het Europees Hof voor de Rechten van de Mens (hierna: EHRM) en het Hof van Justitie van de Europese Unie (hierna: HvJ EU).[20] De onduidelijkheid over de reikwijdte van de reconstructieplicht roept dan ook de vraag op in hoeverre het bewaren van kopieën van legitimatiebewijzen, foto's en audio- en video-opnamen van cliënten in overeenstemming is met de reconstructieplicht van de Wwft in het licht van het

10 *Kamerstukken II* 2007/08, 31238, p. 35; Rb. Noord-Holland 27 oktober 2021, ECLI:NL:RBNHO:2021:9542, r.o. 4.12.1; Autoriteit Financiële Markten, *Hoe moet u zich identificeren bij een financiële onderneming?*, perma.cc/HK3F-V5WK 30 december 2023; Rijksoverheid, 'Moet een bank een kopie van mijn paspoort maken en bewaren?', perma.cc/9C4P-PKCM 24 maart 2023.

11 Richtsnoeren geven de opvatting van de toezichthouder weer en zijn bedoeld om een gedragslijn te bevorderen. Ze hebben weliswaar geen kracht van wet, maar zijn wel van betekenis voor de instellingen, aangezien het niet volgen van de opvatting van de toezichthouder reden kan zijn voor de toezichthouder om handhavend op te treden. Het wel volgen van richtsnoeren kan een bevrijdend verweer vormen. Zie Concl. A-G T. Hartlief 12 maart 2021, ECLI:NL:PHR:2021:239, par. 5.5.

12 Rijksoverheid, 'Moet een bank een kopie van mijn paspoort maken en bewaren?', perma.cc/9C4P-PKCM 24 maart 2023 en Autoriteit Financiële Markten, *Hoe moet u zich identificeren bij een financiële onderneming?*, perma.cc/HK3F-V5WK 30 december 2023.

13 De Nederlandsche Bank, *Leidraad Wwft en Sw*, Amsterdam december 2020, p. 76 en *De Nederlandsche Bank, Consultatieversie DNB 'Q&As' en 'Good Practices' Wwft*, Amsterdam 18 oktober 2023, p. 53-54.

14 Ministerie van Financiën, *Algemene leidraad Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft)* 21 juli 2020, p. 48; Autoriteit persoonsgegevens, *Identificatie bij uw bank*, perma.cc/EM5C-MYBE 30 december 2023 en College bescherming persoonsgegevens (Cbp) 2012, *CBP Richtsnoeren Identificatie en verificatie van persoonsgegevens. Gebruik van 'kopietje paspoort' in de private sector*, p. 8. Het Cbp beperkt in deze richtsnoeren de bewaring van een kopie legitimatiebewijs tot 5 jaar, korter dan de bewaartermijn de Wwft, namelijk vijf jaar na het einde van de zakelijke relatie (of een incidentele transactie).

15 Commissie van Beroep, Klachteninstituut Financiële Dienstverlening (Kifid) 8 februari 2023, CB 2023-0004, r.o. 1.9.

16 Autoriteit persoonsgegevens, *Financiële ondernemingen*, perma.cc/LE5G-V7H8 30 december 2023. De tekst is halverwege 2023 vervangen toen de AP een nieuwe website lanceerde. De oude tekst was: 'Zij mogen daarvoor een kopie maken van het identiteitsbewijs van elke klant'. In de nieuwe tekst is 'mogen' weggelaten; nu staat er dat het een verplichting is. Er zijn meer teksten aangepast. Op de oude AP-website stond bijvoorbeeld: 'voor de identificatieplicht uit de Wwft mag uw bank, verzekeraar of creditcardmaatschappij uw BSN niet verwerken. Ook met een afgeschermde kopie van uw identiteitsbewijs kunnen financiële ondernemingen namelijk aantonen dat ze aan de identificatieplicht uit de Wwft voldoen.' Op de nieuwe website, gelanceerd halverwege 2023, staat onder 'Mag mijn bank een kopie ID maken of vragen?' het tegenovergestelde: 'Meestal mag u uw burgerservicenummer (BSN) niet afschermen op de kopie ID. Want de meeste financiële ondernemingen en dienstverleners zijn wettelijk verplicht om uw BSN te gebruiken.' Vgl. Autoriteit persoonsgegevens, *Financiële ondernemingen*, perma.cc/998Z-NJBX 23 mei 2023. Een uitgebreide bespreking voert te ver, maar de nieuwe teksten lijken niet in overeenstemming met de wet.

17 European Banking Authority (EBA) 2022, *Richtsnoeren voor het gebruik van oplossingen voor de acceptatie van cliënten op afstand overeenkomstig artikel 13, lid 1, van Richtlijn (EU) 2015/849*, p. 16. Omdat DNB niet binnen twee maanden bezwaar heeft gemaakt tegen het richtsnoer van de EBA, wordt zij nu geacht zich in Nederland 'tot het uiterste' in te spannen om te voldoen aan dit richtsnoer, bijvoorbeeld door deze te integreren in de toezichtsprocessen, zie art. 16 lid 3 Verordening (EU) nr. 1093/2010. Desondanks is het richtsnoer voor een 'filmplicht' van de EBA niet opgenomen in de consultatieversie van de nieuwe DNB-richtsnoeren.

18 Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden 4 november 1950, *Trb.* 1951, p. 154. Art. 8 lid 1 EVRM luidt: 'Een ieder heeft recht op respect voor zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.'

19 Handvest van de grondrechten van de Europese Unie 7 december 2000, *PbEG* 2000, C 364. Art. 7 Handvest luidt: 'Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn communicatie.' Art. 8 Handvest luidt: 'Eenieder heeft recht op bescherming van zijn persoonsgegevens' (lid 1); 'Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht van inzage in de over hem verzamelde gegevens en op rectificatie daarvan' (lid 2). Art. 8 Handvest is nader uitgewerkt in secundaire wetgeving, waaronder de Algemene verordening gegevensbescherming (AVG), zie overweging 1 van de AVG.

20 De Uniewetgever heeft in overweging 43 4AMLD en in overwegingen 5 en 51 5AMLD uitdrukkelijk bepaald dat de anti-witwasrichtlijnen moeten worden uitgevoerd in overeenstemming met de in het Handvest erkende rechten en beginselen.

fundamentele recht op privacy en gegevensbescherming zoals vastgelegd in artikel 8 van het EVRM en de artikelen 7 en 8 van het Handvest.

Om deze onderzoeksvraag te beantwoorden, bespreekt paragraaf 2 eerst de reikwijdte van de verificatie- en reconstructieplicht van de Wwft. Vervolgens gaat paragraaf 3 in op de eisen die het EHRM en HvJ EU stellen aan de voorzienbaarheid en subsidiariteit van inperkingen van het recht op privacy en gegevensbescherming. In paragraaf 4 wordt de onderzoeksvraag beantwoord. Om de beschikbare ruimte in dit artikel zo goed mogelijk te benutten, is ervoor gekozen om de bespreking te beperken tot de vereisten die worden gesteld aan de voorzienbaarheid en subsidiariteit (onderdeel van het Unierechtelijke evenredigheidsbeginsel).[21] Ook beperkt deze bespreking zich, in het kader van de verificatieplicht van de identiteit van natuurlijke personen die geen uiteindelijke belanghebbenden (UBO's) zijn, tot de reconstructieplicht van de Wwft, waarin 4AMLD is geïmplementeerd.[22]

2 Reikwijdte verificatieplicht en reconstructieplicht

2.1 *Verificatieplicht*

Artikel 11, eerste lid, van de Wwft bepaalt dat instellingen bij een incidentele transactie of het aangaan van een zakelijke relatie de identiteit van de cliënt moeten verifiëren aan de hand van documenten, gegevens of inlichtingen uit een betrouwbare en onafhankelijke bron.[23] Volgens artikel 4 van de Uitvoeringsregeling Wwft zijn identiteitsdocumenten zoals een paspoort, rijbewijs en identiteitskaart dergelijke documenten.[24] De identiteit van de cliënt wordt in beginsel eenmalig geverifieerd. Er is dus geen sprake van een heridentificatieplicht bij het verlopen van een legitimatiebewijs of bij opvolgende transacties,[25] behalve wanneer een instelling twijfelt aan de juistheid of volledigheid van eerder verkregen identiteitsgegevens,[26] of wanneer de initiële identiteitsverificatie heeft plaatsvonden vóór de inwerkingtreding van de Implementatiewet vierde anti-witwasrichtlijn op 25 juli 2018.[27]

2.1.1 *Risico's bepalend voor geschikte identificatiemethoden*

De Wwft schrijft niet gedetailleerd voor hoe instellingen de identiteitsverificatie moeten uitvoeren. Instellingen moeten dit zelf bepalen, op basis van een beoordeling van het risico op witwassen en terrorismefinanciering per product, dienst, markt en land waarin zij actief zijn, en per cliënt.[28] De door de Wwft-instelling gebruikte verificatiemethode moet geschikt zijn in het licht van het aanwezig geachte risico op witwassen en financiering van terrorisme.[29] Hoe hoger het risico is beoordeeld, hoe grondiger het cliëntenonderzoek moet zijn.[30] Daarom is als onderdeel van een laagrisico identiteitsverificatie het toesturen van een kopie van het legitimatiebewijs per post denkbaar,[31] maar is dit bij een verhoogd risico een ongeschikte methode.[32]

De identiteitsverificatie kan elektronisch plaatsvinden op grond van artikel 13 van de 4AMLD en artikel 4, eerste lid, onderdeel h, van de Uitvoeringsregeling Wwft. De Minister van Financiën heeft bepaald dat elektronische identificatiemethoden die voldoen aan het betrouwbaarheidsniveau 'substantieel' of 'hoog', zoals bedoeld in artikel 8 van de

---

21 Evenredigheid is een algemeen beginsel van het EU-recht en vereist dat de inhoud en vorm van het optreden van de Unie niet verder reiken dan noodzakelijk is voor de verwezenlijking van de doelstellingen van de Verdragen, zie art. 5 lid 4 VEU jo. art. 52 lid 1 Handvest en art. 8 lid 2 EVRM. Het evenredigheidsbeginsel schrijft ook voor dat maatregelen geschikt en proportioneel moeten zijn, maar die beoordeling valt buiten de scope van dit artikel. Zie ook *De Nederlandsche Bank, Consultatieversie DNB 'Q&As' en 'Good Practices' Wwft*, Amsterdam 18 oktober 2023, p. 21. Zie verder Concl. A-G J. Cruz Villalón 12 december 2013, ECLI:EU:C:2013:845, par. 46 (*Digital Rights Ireland* en *Seitlinger e.a.*).

22 Hoewel dit artikel relevant kan zijn voor andere, bijvoorbeeld sectorspecifieke, verificatie- en reconstructieverplichtingen, is het onmogelijk om deze volledig te bestuderen en te beschrijven in dit artikel. In het algemeen wordt opgemerkt dat andere inbreuken op het fundamentele recht op privacy en gegevensbescherming ook bij wet moeten zijn voorzien, voldoende voorzienbaar (voldoende nauwkeurig geformuleerd) moeten zijn en moeten voldoen aan het evenredigheidsbeginsel, wat betekent dat zij geschikt en subsidiair zijn en niet verdergaan dan strikt noodzakelijk, oftewel dat zij proportioneel zijn.

23 Art. 11 lid 1 Wwft.

24 Uitvoeringsregeling Wet ter voorkoming van witwassen en financieren van terrorisme 21 mei 2020. Zie ook: *Kamerstukken II* 2007/08, 31238, nr. 3, p. 23.

25 *Kamerstukken II* 2011/12, 33238, nr. 3, p. 14 (*MvT bij Wijziging van de Wet ter voorkoming van witwassen en financieren van terrorisme en de Wet ter voorkoming van witwassen en financieren van terrorisme BES in verband met de implementatie van aanbevelingen van de Financial Action Task Force*). Zie tevens: FATF 2012-2023, p. 67 en Ellen Timmer, 'De Wwft verplicht niet tot heridentificatie en ook niet tot kopietje paspoort', ellentimmer.com, 5 juli 2022.

26 Art. 3 lid 5 onder d Wwft. Zie tevens: FATF 2012-2023, p. 67.

27 Art. 38 lid 1 Wwft. Zie ook: Kifid 1 juli 2021, GC 2021-0606, r.o. 3.2-3.3.

28 *Kamerstukken II* 2007/08, 31238, nr. 3, p. 10 en 23 en *Kamerstukken II* 2017/18, 34808, nr. 3 (*MvT bij Implementatiewet vierde anti-witwasrichtlijn*), p. 8. Bijlage III 4AMLD bevat een enumeratieve lijst met 'potentiële' risicoverlagende en risicoverhogende factoren die instellingen in overweging moeten nemen.

29 Art. 8 lid 2 Wwft.

30 Art. 13 lid 2 jo. lid 1 onder a 4AMLD jo. art. 3 lid 2 onder a jo. art. 11 lid 1 jo. art. 3 lid 8 en art. 8 Wwft.

31 Deze methode is volgens Gohres toegestaan, maar wordt 'steeds minder populair door de identiteitsfraude', zie W.J.D. Gohres, 'Belastingadviseurs', in: B. Snijder-Kuipers & A.T.A. Tilleman (red.), *Handboek WWFT*, Deventer: Wolters Kluwer 2019, p. 175-176.

32 Art. 18 lid 3 4AMLD jo. bijlage III, no. 2, lid c 4AMLD. Aan de hand van een opgestuurde kopie van een legitimatiebewijs kan immers niet afdoende worden vastgesteld of het gekopieerde legitimatiebewijs echt is, en niet is gestolen, vervalst of toebehoort aan iemand anders.

eIDAS-verordening, voldoende betrouwbaar zijn om te worden gebruikt.[33] In Nederland is DigiD het enige Europees erkende inlogmiddel.[34] Er mogen ook andere, niet-goedgekeurde elektronische verificatiemethoden gebruikt worden. Het gebruik van deze verificatiemethoden wordt in zichzelf als potentieel risicoverhogend gezien, en is dus mogelijk minder geschikt voor een identiteitsverificatie waarbij volgens de instelling al sprake is van een verhoogd risico op witwassen en terrorismefinanciering.[35]

Als de risicobeoordeling dit vereist, kan een instelling de betrouwbaarheid van de identiteitsverificatie op afstand vergroten door de cliënt te vragen om, naast een foto of kopie van het identiteitsdocument, ook een selfie te sturen of een videogesprek te voeren met een medewerker, zodat de paspoortfoto kan worden vergeleken met het gezicht van de persoon die klant wordt. Het gebruik van *geautomatiseerde* apps voor videoverificatie is echter niet geschikt voor identiteitsverificaties met een verhoogd risico: de *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*, de Duitse privacytoezichthouder, heeft geconcludeerd dat apps voor videoverificaties 'onder geen enkele omstandigheid' kunnen worden gebruikt voor identiteitsverificaties met een verhoogd risico.[36] Uit een publicatie van de Chaos Computer Club, Europa's grootste hackersvereniging, blijkt bovendien hoe eenvoudig het is om de veelgebruikte videoverificatietechnologie voor elektronische identiteitsverificaties te kraken.[37] Daarom is het de vraag of geautomatiseerde verificatie-apps geschikt zijn voor identiteitsverificaties zonder verhoogd risico.[38] Het is dan ook raadzaam om, zeker wanneer sprake is van een verhoogd risico op witwassen en terrorismefinanciering, de voorkeur te geven aan persoonlijke en fysieke boven geautomatiseerde en elektronische identiteitsverificaties.[39]

2.1.2 *Contractuele afspraken tussen instelling en cliënt*

Wanneer uit de risicobeoordeling door de instelling volgt dat verschillende verificatiemethoden, zoals het fysiek tonen van een legitimatiebewijs en een voldoende betrouwbare elektronische identiteitsverificatie, voldoende betrouwbaarheid kunnen bieden over de identiteit van een cliënt, kan de instelling in beginsel kiezen tussen die verschillende methoden. Wanneer geen afspraken zijn gemaakt met de cliënt, dienen de partijen zich ten opzichte van elkaar te gedragen volgens de eisen van redelijkheid en billijkheid. Dit kan betekenen dat de instelling genoegen moet nemen met de voorkeur van de cliënt om zijn legitimatiebewijs te laten zien tijdens een FaceTime-gesprek[40] of fysiek aan een balie, en het opsturen van een kopie van zijn legitimatiebewijs of een andere (elektronische) methode om de identiteit te verifiëren niet mag eisen.[41]

---

33 Regeling van de Minister van Financiën van 6 mei 2020, nr. 2020-0000084921, directie Financiële Markten, tot wijziging van onder meer de Uitvoeringsregeling Wet ter voorkoming van witwassen en financieren van terrorisme ter implementatie van richtlijn (EU) 2018/843 van het Europees parlement en de Raad van 30 mei 2018 tot wijziging van richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van de Richtlijnen 2009/138/EG en 2013/36/EU, *PbEU* 2018, L 156 (*Implementatieregeling wijziging vierde anti-witwasrichtlijn*), p. 4. Zie ook: art. 8 lid 2 Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (*eIDAS-verordening*).

34 Stelsels voor elektronische identificatie aangemeld overeenkomstig art. 9 lid 1 van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt, 27.4.2022, 2022/C 173 I/01. Het gebruik van DigiD beperkt zich tot overheidsorganisaties en organisaties met een publieke taak, zoals ministeries, lokale overheden, organisaties actief in de zorg, onderwijs, pensioen en waterschappen, en kan daarom op dit moment niet (direct) worden gebruikt voor identiteitsverificaties bij instellingen, zie Logius, *Hoe werkt DigiD?*, perma.cc/PP52-RRZA 1 januari 2024.

35 Bijlage III, no. 2, lid c 4AMLD jo. art. 18 lid 3 4AMLD.

36 Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), *Tätigkeitsbericht für den Datenschutz und die Informationsfreiheit 2020*, Bonn 2021, p. 77-78. Nu zowel de Duitse als de Nederlandse anti-witwaswetgeving op dezelfde richtlijn is gebaseerd, en in beide landen dezelfde regels uit de Europese privacywetgeving van toepassing zijn, is dit ook relevant voor instellingen die aan de Wwft moeten voldoen.

37 Chaos Computer Club (CCC), 'Praktischer Angriff auf Video-Ident. Demonstration inhärenter Schwächen der videobasiert Echtheitsprüfung physischer ID-Dukomente', ccc.de, 8 augustus 2022, p. 13-18. In het persbericht wordt opgemerkt dat de aanval zo eenvoudig is dat geïnteresseerde hobbyisten en zeker gemotiveerde criminelen deze in korte tijd en met weinig inspanning kunnen uitvoeren. Het risico van verder misbruik moet daarom als hoog worden ingeschat, zie: CCC, 'Chaos Computer Club hackt Video-Ident', ccc.de, 10 augustus 2022.

38 Art. 13 lid 4 4AMLD. Zie ook: European Supervisory Authorities (ESA's), *Opinion on the use of innovative solutions by credit institutions and financial institutions in the customer due diligence process*, 23 januari 2018, p. 11.

39 Een onvoldoende betrouwbare identiteitsverificatie onder de verificatieplicht kan niet worden 'gecompenseerd' met het bewaren van meer gegevens en documenten onder de reconstructieplicht, zoals een audio- en video-opname van die onvoldoende betrouwbare identiteitsverificatie, zoals EBA lijkt te suggereren in zijn richtsnoeren, zie European Banking Authority (EBA) 2022, *Richtsnoeren voor het gebruik van oplossingen voor de acceptatie van cliënten op afstand overeenkomstig artikel 13, lid 1, van Richtlijn (EU) 2015/849*, p. 16. De identiteitsverificatie zelf dient voldoende betrouwbaar te zijn in het licht van de beoordeelde risico's.

40 A.E. van Almelo & M. Pheijffer, 'Accountants', in: B. Snijder-Kuipers & A.T.A. Tilleman (red.), *Handboek WWFT*, Deventer: Wolters Kluwer 2019, p. 215. Zie ook: Rb. Noord-Holland 27 oktober 2021, ECLI:NL:RBNHO:2021:9542, r.o. 4.14 (*Eiser/Srlev*).

41 Rb. Noord-Holland 27 oktober 2021, ECLI:NL:RBNHO:2021:9542, r.o. 4.14 (*Eiser/Srlev*). Zie anders: Rb. Amsterdam 11 januari 2023, ECLI:NL:RBAMS:2023:145, r.o. 4.13 (*SCK/ICS*), waarin de rechtbank ten onrechte overweegt dat art. 2.3 onder k van de algemene voorwaarden van ICS een bepaling zou bevatten over de *wijze* waarop de identiteitsverificatie moet plaatsvinden – *quod non*. Art. 2.3 onder k ziet (slechts) op de *blokkering* (niet opzegging) van een creditcard wanneer een cliënt in het geheel ('als u ons *geen* informatie (..) verstrekt', arcering DM) weigert persoonlijke of financiële informatie te verstrekken. Daar was in casu echter geen sprake van. Zie ook: Kifid 11 oktober 2012, GC 2012-294, r.o. 2.7 en 4.6-4.8.

2.2 *Reconstructieplicht*

Naast de hiervoor besproken verificatieplicht hebben instellingen op grond van artikel 33 van de Wwft ook een reconstructieplicht, die hen in het kader van de identiteitsverificatie verplicht om de geslachtsnaam, de voornamen, de geboortedatum, het adres en de woonplaats van de cliënt, alsmede de aard, het nummer en de datum en plaats van uitgifte van het document waarmee de identiteit van de cliënt is geverifieerd (de 'identiteitsgegevens'), te bewaren tot vijf jaar na het einde van de zakelijke relatie of de incidentele transactie. Onder de voorloper van de Wwft, de Wet Identificatie Dienstverlening (WID),[42] was het niet mogelijk om kopieën van legitimatiebewijzen van cliënten te bewaren.[43] Toch begonnen instellingen dit zonder grondslag te doen. Hierover schreef *Het Parool* destijds:

'Het College Bescherming Persoonsgegevens (CBP), dat toeziet op naleving van de privacyregels, bevestigt dat de WID helemaal niet vraagt om complete kopieën van het id-bewijs. Het eenmalig controleren en noteren van enkele wettelijk voorgeschreven gegevens is voldoende. (…) Het CPB [*sic*] heeft de banken in november 2005 vergeefs geadviseerd dat zij liever terughoudend moeten zijn met het digitaal scannen en centraal bewaren van identiteitsdocumenten. Het CBP heeft geen bevoegdheid dit te verbieden. "Het centraal opslaan van persoonsgegevens maakt ze gevoelig voor hackers," vindt het CBP. Omstreden hierbij is dat de banken ook het sofinummer en de pasfoto scannen en bewaren. "De WID vraagt niet om sofinummers of foto's," zegt de CBP-woordvoerder. Volgens de privacyregels mogen niet méér persoonsgegevens bewaard worden dan "strikt noodzakelijk is". De privacywet beschouwt foto's en sofinummers als "bijzondere gegevens", aldus het CBP. Die worden aangemerkt als privacygevoelig. "Daarom moet je terughoudend zijn met het bewaren er van [*sic*]. Op een pasfoto kan je zien of iemand zwart is, of blank. Dat is informatie die meer is dan strikt noodzakelijk," zegt de CBP-woordvoerder.'[44]

Ook bij de Nederlandse implementatie van de eerste anti-witwasrichtlijn (1AMLD) in de Wwft, die de WID heeft vervangen,[45] heeft de wetgever voor instellingen geen grondslag gecreëerd om kopieën van legitimatiebewijzen te bewaren.[46] Pas bij de implementatie van de derde anti-witwasrichtlijn,[47] in artikel 33, eerste lid, van de Wwft, heeft de wetgever de *mogelijkheid* gecreëerd voor instellingen om op een 'efficiënte wijze (…) [te kunnen] voldoen aan de verplichting tot het vastleggen van gegevens'. Die efficiënte wijze is dat zij 'een afschrift van het document dat een persoonidentificerend nummer bevat en aan de hand waarvan de verificatie van de identiteit heeft plaatsgevonden' (het 'kopie legitimatiebewijs') mogen bewaren *in plaats van* de identiteitsgegevens handmatig over te schrijven.[48]

Dat een keuze moet worden gemaakt tussen het bewaren van de losse identiteitsgegevens of een kopie van het legitimatiebewijs, en het feit dat dit geen cumulatieve verplichting of grondslag vormt, volgt uit het gebruik van het woord 'of' in de wettekst:

'Een instelling die op grond van deze wet een persoon heeft geïdentificeerd en zijn identiteit heeft geverifieerd (…) legt op opvraagbare wijze de volgende gegevens vast: (…) de geslachtsnaam, de voornamen, de geboortedatum, het adres en de woonplaats, (…) *of* een afschrift van het document dat een persoonidentificerend nummer bevat en aan de hand waarvan de identificatie heeft plaatsgevonden (…).'[49]

Zoals inmiddels ook de vaste lijn in de rechtspraak is geworden, is deze alternatieve mogelijkheid dus geen 'paspoortkopieplicht'.[50] Het Cbp heeft deze alternatieve mogelijkheid opgenomen in de richtsnoeren 'Identificatie en verificatie van persoonsgegevens', en heeft daarbij het woord 'kan' gearceerd:

'De financiële instelling *kan* – als bewijs van de identificatieverplichting (reconstructieplicht) – daarbij ook een afschrift (lees: kopie) van het gecontroleerde identiteitsdocument vastleggen en gedurende vijf jaar bewaren.'[51]

---

42 *Stb*. 1993, 704. De citeertitel is gewijzigd bij de Wet van 13 december 2001, Stb. 665 (*Wet identificatie bij dienstverlening*).
43 Art. 6 onder a jo b Wid luidde: 'De financiële instelling is verplicht de volgende gegevens vast te leggen op een zodanige wijze dat deze toegankelijk zijn: de naam, het adres en de woonplaats dan wel plaats van vestiging van de cliënt en van degene te wiens name het depot of de rekening wordt gesteld, van degene die toegang tot het safe-loket zal hebben of degene te wiens name een uitbetaling of transactie wordt verricht, alsmede van hun vertegenwoordigers; de aard, het nummer en de datum en plaats van uitgifte van het document met behulp waarvan de identiteitsvaststelling heeft plaatsgevonden, behoudens indien artikel 4 van toepassing is'.
44 M. Laan, 'Bank verzamelt ten onrechte foto van klant', *Het Parool* 9 augustus 2006 en Tweakers, 'Vraagtekens bij opslag id-bewijzen door banken', tweakers.net, 9 augustus 2006.
45 Wet van 15 juli 2008, houdende samenvoeging van de Wet identificatie bij dienstverlening en de Wet melding ongebruikelijke transacties (*Wet ter voorkoming van witwassen en financieren van terrorisme*), *Stb*. 2008, 303.
46 Art. 6 onder a en b Wet identificatie bij financiële dienstverlening, *Stb.* 1993, 704.
47 Richtlijn 2005/60/EG van het Europees Parlement en de Raad van 26 oktober 2005 tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme.
48 *Kamerstukken II* 2007/08, 31238, nr. 3, p. 35.
49 Art. 33 lid 1 aanhef jo. onder a Wwft (oud). Onderstreping en cursivering toegevoegd.
50 Rb. Noord-Holland 27 oktober 2021, ECLI:NL:RBNHO:2021:9542, r.o. 4.12.1. 'Zoals [eiseres] terecht heeft opgemerkt, bestaat geen wettelijke verplichting om bij een cliëntenonderzoek een kopie van het identiteitsbewijs van de klant te maken,' zie Rb. Rotterdam 20 april 2023, ECLI:NL:RBROT:2023:3301, r.o. 3.5. Zie naar analogie Concl. A-G G. Pitruzzella 12 mei 2022, ECLI:EU:C:2022:381, par. 110 (*Rodl & Partner*).
51 College bescherming persoonsgegevens (Cbp) 2012, *CBP Richtsnoeren Identificatie en verificatie van persoonsgegevens. Gebruik van 'kopietje paspoort' in de private sector*, p. 8.

Naast het los bewaren van identiteitsgegevens *of* (in plaats daarvan) een kopie van het legitimatiebewijs van de cliënt, stond de reconstructieplicht niet toe om ook andere documenten te bewaren (ook geen foto's of audio- of video-opnamen). Artikel 33, eerste lid, van de Wwft (oud) noemde specifiek één document dat kon worden bewaard, namelijk de kopie van het legitimatiebewijs.

Met de invoering van 4AMLD per 25 juli 2018 is de reconstructieplicht van artikel 33 van de Wwft echter gewijzigd van een limitatieve naar een enuntiatieve opsomming, door de toevoeging van de woorden 'ten minste'. Hierdoor benoemt dit wetsartikel nu welke documenten en gegevens *ten minste* onder de reconstructieplicht vallen:

'Onder de documenten en gegevens (…) zijn *ten minste* begrepen: (…) de geslachtsnaam, de voornamen, de geboortedatum, het adres en de woonplaats, (…) *of* een afschrift van het document dat een persoonidentificerend nummer bevat en aan de hand waarvan de verificatie van de identiteit heeft plaatsgevonden (…).'[52]

Uit de gewijzigde wettekst van de reconstructieplicht volgt echter nog steeds geen 'paspoortkopieplicht'. Het bewaren van een kopie van het legitimatiebewijs blijft een mogelijk alternatief ('of') voor het los noteren van de in het wetsartikel opgesomde identiteitsgegevens.

Daarnaast kan de wettekst door de woorden 'ten minste' zo gelezen worden dat de wetgever een grondslag heeft willen creëren voor het bewaren van *andere* gegevens en documenten dan de identiteitsgegevens of een kopie van het bij de identificatie gebruikte legitimatiebewijs, zoals foto's en audio- en video-opnamen van de cliënt. Uit de memorie van toelichting bij de Implementatiewet 4AMLD blijkt echter dat dat niet het geval is. De toevoeging van de woorden 'ten minste' was uitsluitend bedoeld om de reconstructieplicht te verruimen in verband met de complexere verificatie van *eigendomsstructuren* van UBO's[53] met een grondslag voor de bewaring van gegevens en documenten die *daarvoor* benodigd zijn (zoals een schema van een eigendomsstructuur).[54]

De minister benadrukte expliciet dat de nieuwe bepaling niet voorziet in een wijziging van de oude limitatieve reconstructieplicht bij cliënten die natuurlijke personen en geen UBO's zijn:

'Het voorgestelde artikel 33 *voorziet niet in een wijziging van de documenten* en *gegevens die* van [natuurlijke personen, niet zijnde een UBO] *moeten worden vastgelegd en bewaard*.'[55]

Hieruit volgt dat de reconstructieplicht van de Wwft in het kader van de identiteitsverificatie van natuurlijke personen die geen UBO zijn nog steeds uitsluitend een grondslag biedt voor de *mogelijkheid* – en niet de *verplichting* – om een kopie van het legitimatiebewijs te bewaren, *in plaats van* ('of') die identiteitsgegevens over te schrijven en los te bewaren.[56] Hieruit volgt tevens dat artikel 33 van de Wwft geen grondslag (laat staan een verplichting) biedt voor het bewaren van foto's en audio- en video-opnamen van cliënten. Het enige document dat mag worden bewaard in het kader van de reconstructieplicht van de identiteitsverificatie op grond van de Wwft is een kopie van het legitimatiebewijs.

3 Fundamenteel recht op privacy en gegevensbescherming

Het bewaren van kopieën van legitimatiebewijzen, foto's en audio- en video-opnamen van cliënten vormt ook een inperking van het fundamentele recht op privacy en gegevensbescherming dat is vastgelegd in artikel 8 van het EVRM en artikelen 7 en 8 van het Handvest. Artikel 52 van het Handvest en jurisprudentie van het EHRM en het HvJ EU schrijven voor dat inperkingen bij wet moeten zijn voorzien, voorzienbaar moeten zijn en in overeenstemming moeten zijn met het evenredigheidsbeginsel, dat onder meer vereist dat er geen minder ingrijpende alternatieven zijn om het legitieme doel te bereiken (het subsidiariteitsvereiste).

In de volgende subparagrafen wordt stilgestaan bij de subsidiariteit (paragraaf 3.1) en voorzienbaarheid (paragraaf 3.2) van een invulling van de reconstructieplicht waarbij door instellingen ook kopieën van legitimatiebewijzen, foto's en audio- en video-opnamen van cliënten worden bewaard.

3.1 *Subsidiariteit*

Het subsidiariteitsbeginsel vereist dat inperkingen op het fundamentele recht op privacy en gegevensbescherming, in dit geval de reconstructieplicht, op de minst ingrijpende geschikte wijze worden uitgevoerd.[57] Zoals in de inleiding van dit artikel reeds is toegelicht, blijkt uit de *Monitor Identiteit,* die tweejaarlijks wordt

52 Art. 33 lid 2 aanhef jo. onder a Wwft. Cursiveringen toegevoegd.
53 Art. 10a lid 1 Wwft.
54 *Kamerstukken II* 2017/18, 34808, nr. 3, p. 79-80.
55 *Kamerstukken II* 2017/18, 34808, nr. 3, p. 79-80. Cursiveringen toegevoegd.
56 Dit is ook de vaste lijn in de rechtspraak, zie Rb. Rotterdam 20 april 2023, ECLI:NL:RBROT:2023:3301, r.o. 3.5 en Rb. Noord-Holland 27 oktober 2021, ECLI:NL:RBNHO:2021:9542, r.o. 4.12.1.
57 HvJ EU 22 november 2022, C-37/20 en C-601/20, ECLI:EU:C:2022:912, r.o. 64 (*Sovim*); HvJ EU 17 oktober 2013, C-291/12, ECLI:EU:C:2013:670, r.o. 48-53 (*Schwarz*); HvJ EU 26 juli 2017, Advies 1/15, ECLI:EU:C:2017:592, par. 208 en 244 (*PNR-overeenkomst EU-Canada*); HvJ EU, gev. zaken C-465/00, C-138/01 en C-139/01, ECLI:EU:C:2003:294, r.o. 52 (*Rechnungshof/Österreichischer Rundfunk e.a.*).

uitgevoerd in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, dat identiteitsfraude het vaakst plaatsvindt op basis van een kopie van een legitimatiebewijs (38%).[58] Misbruik van een kopie van een legitimatiebewijs komt niet alleen vaker voor dan andere vormen van identiteitsfraude, maar kan, in het bijzonder in combinatie met een foto of audio- en video-opname, ook ernstigere gevolgen hebben dan wanneer enkel identiteitsgegevens worden misbruikt.[59] Met de snelle ontwikkeling van kunstmatige intelligentie, zoals *deep fake*-technologieën, wordt deze dreiging steeds groter en reëler. Daarom vergroot een invulling van de reconstructieplicht die het bewaren van kopieën van legitimatiebewijzen, foto's en audio- en video-opnamen van cliënten omvat, de kans, risico's en mogelijke gevolgen bij misbruik dan wanneer alleen de in artikel 33, tweede lid, onderdeel a, van de Wwft voorgeschreven 'losse' identiteitsgegevens worden bewaard, die volstaan om aan de reconstructieplicht te voldoen,[60] en vormt dit een grotere inbreuk op de fundamentele rechten van cliënten dan het los bewaren van hun identiteitsgegevens. Diezelfde snelle technologische ontwikkeling heeft ervoor gezorgd dat er, anders dan in 2008 bij de invoering van de 'efficiënte' mogelijkheid om een kopie van legitimatiebewijzen op te kunnen slaan in plaats van de losse identiteitsgegevens, weinig situaties denkbaar zijn waarin het bewaren van de losse identiteitsgegevens niet werkbaar is. Het subsidiariteitsbeginsel vereist daarom dat in beginsel gekozen wordt voor de losse bewaring van de identiteitsgegevens in plaats van een kopie van het legitimatiebewijs.

Omgekeerd volgt uit het subsidiariteitsvereiste dat de identiteitsgegevens niet ook los mogen worden bewaard als een instelling desondanks moet kiezen voor het bewaren van een kopie legitimatiebewijs (omdat het bewaren van de losse gegevens niet werkbaar is), en dat gegevens op het kopie legitimatiebewijs die niet zijn vereist op grond van artikel 33 van de Wwft zwart moeten worden gemaakt, zoals een foto, handtekening en het burgerservicenummer.[61] Een grondslag voor het in het kader van de identiteitsverificatie bewaren van foto's van cliënten, audio- en video-opnamen is niet voorzien in de Wwft.[62]

3.2 *Voorzienbaarheid*

Om de rechtszekerheid te waarborgen en de naleving van het legaliteitsbeginsel te bevorderen, moeten inbreuken op het fundamentele recht op privacy en gegevensbescherming die voortvloeien uit (de uitvoering van) de reconstructieplicht niet alleen worden uitgevoerd op de minst inbreukmakende geschikte manier, maar ook voldoende voorzienbaar zijn voor cliënten.[63] Voorzienbaarheid betekent dat het voor de cliënt duidelijk moet zijn onder welke omstandigheden zijn fundamentele rechten mogen worden ingeperkt. Dit beschermt cliënten tegen willekeurig overheidsingrijpen, in het geval van de Wwft gedelegeerd aan de instellingen, en stelt hen in staat de gevolgen van een inperking adequaat te voorzien en daar desgewenst hun gedrag op af te stemmen. Om aan dit vereiste te voldoen moet de reconstructieplicht voldoende precies

58 Zie G. Bummelkamp e.a., *Monitor Identiteit 2021*, maart 2022. Zie ook Ellen Timmer, 'Informatie over identificatie en identiteitsfraude | Monitor Identiteit 2021', ellentimmer.com, 20 juni 2022.

59 Vgl. HvJ EU 17 oktober 2013, C-291/12, ECLI:EU:C:2013:670, r.o. 48-53 (*Schwarz*) en HvJ EU 26 juli 2017, Advies 1/15, ECLI:EU:C:2017:592, par. 208 en 244 (*PNR-overeenkomst EU-Canada*). Zie ook M. Laan, 'Bank verzamelt ten onrechte foto van klant', *Het Parool* 9 augustus 2006.

60 Deze gegevens zijn voldoende om ongebruikelijke transactie te melden, en de Wwft biedt geen grondslag om documenten mee te sturen. Op grond van art. 16 lid 2 Wwft bevat een melding de identiteit van de cliënt en de aard en het nummer van het identiteitsbewijs van de cliënt, maar geen kopie van het legitimatiebewijs, foto's of andere documenten, zoals audio- of video-opnamen. Zie ook art. 17 lid 1 en 2 Wwft: 'gegevens' en 'inlichtingen' kunnen worden opgevraagd bij Wwft-instellingen, maar geen 'documenten'.

61 Dit volgt ook uit het beginsel van minimale gegevensverwerking van art. 5 lid 1 onder c AVG, gelezen in samenhang met overweging 4. Verwerkingsverantwoordelijken mogen enkel persoonsgegevens verwerken die toereikend en ter zake dienend zijn, en indien deze gegevens worden beperkt tot hetgeen noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Zie ook Cbp in M. Laan, 'Bank verzamelt ten onrechte foto van klant', *Het Parool* 9 augustus 2006. Het bewaren van een *integrale* kopie legitimatiebewijs, zonder gegevens zwart te lakken, is geboden bij een grondslag voor bewaring van de volledige, integrale kopie. Het subsidiariteitsbeginsel vereist bij grondslagen voor de bewaring van losse gegevens, zoals een pasfoto, handtekening of BSN-nummer, dat deze niet 'gemakshalve' als integrale kopie van het legitimatiebewijs bewaard worden, omdat dat een grotere inbreuk (en risico) vormt dan de bewaring van de losse gegevens. Zie ook Kifid 10 januari 2022, GC 2022-0013, r.o. 3.10.

62 De EBA, die in richtsnoeren heeft opgenomen dat een audio- en video-opname van cliënten moet worden bewaard, is er in de consultatiefase op gewezen dat dit op gespannen voet staat met de AVG, zie: European Banking Authority (EBA), *Response to consultation on draft Guidelines on the use of remote customer onboarding solutions* perma.cc/JA92-GJ97 30 december 2023. Het EHRM eerder heeft bepaald dat juist in de context van nieuwe technologische ontwikkelingen (zoals elektronische identiteitsverificaties) een bijzondere verantwoordelijkheid bestaat om fundamentele rechten te beschermen, zie EHRM 4 december 2008, nr. 30562/04 en 30566/04, r.o. 112 (*S. en Marper/het Verenigd Koninkrijk*) en Rb. Den Haag, 6 februari 2020, ECLI:NL:RBDHA:2020:865, r.o. 6.84 (*SyRI*).

63 Overweging 41 AVG stelt dat een verwerkingsgrondslag, overeenkomstig de vereisten van het EHRM en het HvJ EU, 'duidelijk en nauwkeurig [moet] zijn, en de toepassing daarvan moet voorspelbaar [moet] zijn voor degenen op wie deze van toepassing is'.

zijn beschreven. Een inperking die onvoldoende voorzienbaar is, is niet geldig.[64]

In paragraaf 2 is reeds opgemerkt dat de Wwft niet voorziet in een grondslag of verplichting voor het *bewaren* van foto's en audio- en video-opnamen van cliënten, net als het bewaren van kopieën van legitimatiebewijzen van cliënten *en* de identiteitsgegevens. Zelfs als de reconstructieplicht door de recente toevoeging van de woorden 'ten minste' (zie paragraaf 2) zo wordt uitgelegd dat instellingen ook kopieën van paspoorten, foto's en audio- en video-opnamen van elke cliënt mogen of moeten bewaren, in tegenstelling tot hetgeen de minister bij de invoering aangaf, moet worden vastgesteld dat de reconstructieplicht te onduidelijk en onnauwkeurig is geformuleerd[65] voor een dergelijke grootschalige inperking van het fundamentele recht op privacy en gegevensbescherming.[66]

Een bespreking van de proportionaliteit van de maatregelen valt buiten de reikwijdte van dit artikel, maar het is ook de vraag of het proportioneel is om in het kader van de identiteitsverificatie kopieën van legitimatiebewijzen, foto's en audio- en video-opnamen van grote delen van de bevolking op te slaan tot vijf jaar na het einde van de zakelijke relaties die zij vaak hebben met meerdere instellingen.[67]

5 Conclusie

Jaarlijks worden honderdduizenden Nederlandse ingezetenen slachtoffer van identiteitsfraude waarbij misbruik wordt gemaakt van een kopie van hun legitimatiebewijs. Instellingen die vallen onder de reikwijdte van de Wwft bewaren het vaakst op grote schaal kopieën van legitimatiebewijzen. De bij de Wwft betrokken toezichthouders stellen op hun websites en in richtsnoeren dat het bewaren van een kopie legitimatiebewijs van klanten 'niet verplicht' is, 'kan', 'mag', 'verwacht wordt' (inclusief pasfoto), 'van elke klant (…) verplicht' zou zijn, en dat de reconstructieplicht ook de verplichting zou behelzen audio- en video-opnamen van cliënten te maken en bewaren (bij geautomatiseerde identiteitsverificaties zonder menselijke tussenkomst).

Uit een rechtshistorische analyse van de Wwft blijkt, in lijn met de vaste rechtspraak, dat het bewaren van een kopie van het legitimatiebewijs van cliënten niet verplicht is, wel kan maar niet altijd mag, en dat de Wwft geen grondslag biedt, laat staan een verplichting bevat, om foto's en audio- en video-opnamen van cliënten te bewaren.

Het bewaren van een kopie van een legitimatiebewijs vormt een ernstigere inperking van het fundamentele recht op privacy en gegevensbescherming dan het enkel bewaren van losse identiteitsgegevens, omdat een kopie legitimatiebewijs een groter en ern-

64 B. van der Sloot, 'The Quality of Law', *Tijdschrift voor Intellectuele Eigendom, Informatietechnologie en E-Commerce Recht* (11) 2020/2, p. 161; A. Bertrand, W. Maxwell & X. Vamparys, 'Do AI-based anti-money laundering (AML) systems violate European fundamental rights?', *International Data Privacy Law* (11) 2021/3, p. 287-288; A.J. Nieuwenhuis & M. den Heijer, *Hoofdstukken grondrechten*, Nijmegen: Ars Aequi Libri 2021, p. 112-114; C. Kaiser, *Privacy and Identity Issues in Financial Transactions* (diss. Groningen), Rijksuniversiteit Groningen 2018, p. 214-215. Zowel het EHRM als het HvJ EU stelt vergelijkbare eisen aan de voorzienbaarheid van inperkingen van het recht op privacy en gegevensbescherming, zie: HvJ EU 21 december 2016, gevoegd: C-203/15 (*Tele2 Sverige AB/Post-och telestyrelsen*) en C-698/15 (*Secretary of State for the Home Department/Tom Watson, Peter Brice, Geoffrey Lewis*); Concl. A-G H. Saugmandsgaard ØE 19 juli 2016, ECLI:EU:C:2016:572, par. 140 (*Secretary of State for the Home Department/Tom Watson, Peter Brice, Geoffrey Lewis*); EHRM 26 april 1970, nr. 6538/74, r.o. 49 (*Sunday Times/Verenigd Koninkrijk*); EHRM 12 januari 2010, nr. 4158/05, r.o. 77 (*Gillan en Quinton/Verenigd Koninkrijk*). Zie verder: Concl. A-G Kokott 18 juli 2007, ECLI:EU:C:2007:454, par. 53 (*Promusicae*), HvJ EU 26 juli 2017, advies 1/15, EU:C:2017:592, r.o. 139-141 (*PNR-overeenkomst EU-Canada*); HvJ EU 16 juli 2020, C-311/18, EU:C:2020:559, r.o. 175 (*Facebook/Schrems*) en HvJ EU 6 oktober 2020, C-623/17, EU:C:2020:790, r.o. 65 (*Privacy International*); EHRM 25 maart 1998, nr. 23224/94, r.o. 72 (*Kopp/Zwitserland*); EHRM 6 september 1978, nr. 5029/71, r.o. 55 (*Klass e.a./Duitsland*); HvJ EU 17 december 2015, C-419/14, EU:C:2015:606, r.o. 81 (*WebMindLicenses*).

65 Vgl. Concl. A-G G. Pitruzzella 20 januari 2022, gev. zaken C-37/20 en C-601/20, ECLI:EU:C:2022:43, par. 114 (*Commissie/Luxembourg Business Registers*) en HvJ EU 26 juli 2017, advies 1/15, EU:C:2017:592, par. 160 (*PNR-overeenkomst EU-Canada*). In de zaak *Luxembourg Business Registers* werd een bepaling waarin ook de woorden 'ten minste' stonden ongeldig verklaard, zie HvJ EU 22 november 2022, ECLI:EU:C:2022:912 gev. zaken C-37/20 en C-601/20, ECLI:EU:C:2022:43, r.o. 82 (*Commissie/Luxembourg Business Registers*). Zie ook HvJ EU 26 juli 2017, ECLI:EU:C:2017:592, par. 156, 163 en 232, punt 3(a) (*PNR-overeenkomst EU-Canada*).

66 Door als Uniewetgever instellingen op te dragen kopieën van paspoorten, foto's en audio- en video-opnamen van nagenoeg de gehele bevolking te verzamelen en soms decennialang te bewaren, ontstaat op termijn een decentrale audiovisuele database van nagenoeg de gehele bevolking met grote risico's, zie Article 29 Working Party, *Opinion 3/2012 on developments in biometric technologies*, p. 30-31. In het licht van art. 8 EVRM en art. 7-8 Handvest moet dit vermoedelijk worden gezien als een 'ernstige' inbreuk die grote hoeveelheden burgers raakt en daarom aan hogere voorzienbaarheidsvereisten moet voldoen. De uitleg van de CvB Kifid 8 februari 2023, CB 2023-0004, r.o. 5.20, dat 'alle' documenten en gegevens moeten worden bewaard, is in strijd met wat de minister daar zelf over heeft gezegd (zie par. 2), de vaste lijn in de rechtspraak, vgl. Rb. Noord-Holland 27 oktober 2021, ECLI:NL:RBNHO:2021:9542, r.o. 4.12.1 en Rb. Rotterdam 20 april 2023, ECLI:NL:RBROT:2023:3301, r.o. 3.5, en leidt tot onbegrensde gegevensverwerkingen waar het voorzienbaarheidsvereiste tegen beschermt, zie HvJ EU 26 juli 2017, ECLI:EU:C:2017:592, r.o. 156 (*PNR-overeenkomst EU-Canada*). De GC Kifid kwam wel tot een uitspraak die daarmee in lijn is, zie Kifid 10 januari 2022, GC 2022-0013, r.o. 3.9.

67 Categorieën van te bewaren gegevens dienen immers beperkt te worden tot wat 'strikt noodzakelijk' is. Zie over het strike noodzakelijkheidsvereiste bijv. HvJ EU 6 oktober 2020, C-511/18, C-512/18 en C-520/18, EU:C:2020:791, r.o. 147 (*La Quadrature du Net e.a.*). Volgens Milaj en Kaiser voldoet de reconstructieplicht van 4AMLD niet aan het evenredigheidsbeginsel, omdat het instellingen opdraagt gegevens te verzamelen die handig, maar niet noodzakelijk zijn, en vanwege de bewaartermijn, zie J. Milaj & C. Kaiser, 'Retention of data in the new Anti-money Laundering Directive – 'need to know' versus 'nice to know', *International Data Privacy Law* (7) 2017/2, p. 125. Zie verder, in algemene zin, over de proportionaliteit van 4AMLD: A. Bertrand, W. Maxwell & X. Vamparys, 'Do AI-based anti-money laundering (AML) systems violate European fundamental rights?', *International Data Privacy Law* (11) 2021/3, p. 287-290 en C. Kaiser, *Privacy and Identity Issues in Financial Transactions* (diss. Groningen), Rijksuniversiteit Groningen 2018, p. 518.

stiger risico op misbruik met zich meebrengt dan de bewaring van losse identiteitsgegevens. Nu op grond van de Wwft blijkt dat het (enkel) bewaren van identiteitsgegevens volstaat, schrijft het subsidiariteitsvereiste voor dat instellingen daar indien mogelijk ook voor moeten kiezen, in plaats van voor het (ook) bewaren van een kopie van het legitimatiebewijs van de cliënt. Het subsidiariteitsvereiste staat er in de context van de reconstructieplicht van de Wwft om dezelfde reden aan in de weg om een kopie legitimatiebewijs te bewaren waar ook andere gegevens (foto, handtekening, burgerservicenummer) op zichtbaar zijn.

De situatie waarin richtsnoeren en websites van toezichthouders elkaar tegenspreken, en de reikwijdte van de reconstructieplicht soms onjuist weergeven, is mogelijk ontstaan omdat de wettekst zelf zonder rechtshistorische analyse onvoldoende duidelijkheid schept, mede door de recente toevoeging van de woorden 'ten minste'. Dat is dan ook de reden dat het bewaren van foto's en audio- en video-opnamen van cliënten op grond van deze onduidelijke reconstructieplicht niet voldoet aan het voorzienbaarheidsvereiste.

Instellingen die naast identiteitsgegevens ook (volledige) kopieën van legitimatiebewijzen, foto's en audio- en video-opnamen van hun cliënten willen bewaren, kunnen zich wat betreft de grondslag niet beroepen op de reconstructieplicht uit de Wwft. Dit sluit echter niet uit dat er andere grondslagen zijn om zulks alsnog te doen. Ook die zullen dan moeten voldoen aan het vereiste van voorzienbaarheid en evenredigheid (geschiktheid, subsidiariteit en proportionaliteit) om een rechtmatige inbreuk op het fundamentele recht op privacy en gegevensbescherming te vormen.

Dit artikel heeft geprobeerd enige verduidelijking te verschaffen over de reikwijdte van de reconstructieplicht van de Wwft en zo bij te dragen aan het ontstaan van consistentere richtlijnen en meer duidelijkheid voor instellingen en hun cliënten, die zo in staat worden gesteld om te voldoen aan de belangrijke verificatie- en reconstructieplicht en de privacy en gegevens van betrokkenen beter te beschermen. Als instellingen minder vaak kopieën van legitimatiebewijzen bewaren, neemt het algehele risico op identiteitsfraude af, terwijl zij hun verplichtingen nog steeds kunnen nakomen.