Consultatiereactie

Ministerie van Financiën
Postbus 20201
2500 EE Den Haag

Human Rights in Finance.EU
Postbus 15673
1001 ND AK Amsterdam
legal@hrif.eu

30 juni 2024

Beste lezer,

De stichting Human Rights in Finance.EU (HRIF.EU) reageert hierbij op de consultatie Wet Rapportage Hypotheekmarkt en de wet toezicht-ondersteunende rapportage AFM. Wij zullen hieronder eerst toelichten wat onze organisatie doet. Daarna bespreken we welke belangrijke vragen wij rond grondrechtinbreuken zien in de praktijk van het toezicht van DNB en het Ministerie van Financiën. Dat biedt de achtergrond waartegen u onze consultatiereactie kunt plaatsen.

De kern van onze reactie is dat in elk geval het Ministerie van Financiën, De Nederlandsche Bank op dit moment nog (steeds) te weinig kennis en expertise hebben van grondrechten, grondrechtenweging en de werking van de Algemene Verordening Gegevensverwerking om een inhoudsvol zinnig voorstel te doen c.q. als uitvoeringsorgaan op passende wijze de grondrechten te borgen. Dat het Ministerie bij dit wetsvoorstel niet in staat blijkt te identificeren dat organisaties als Bits of Freedom, Consumentenbond, PrivacyFirst en HRIF.EU betrokken moeten worden, is zowel veelzeggend als tekenend.

De twee wetsvoorstellen zijn in strijd met Europees recht. Wij adviseren zowel het Ministerie van Financiën als DNB en AFM een fundamentele professionaliseringsslag maken op het gebied van grondrechten en privacy. Onze hoofdconclusie, de wij hierna toelichten, luidt:

> **De voorstellen zijn strijdig met Europees recht nu er bulkinterceptie en sleepnetten worden geformaliseerd. Prioriteit 1 moet zijn dat de instituties die het financieel toezicht bepalen en uitvoeren, aantoonbaar een meer professionele invulling geven aan hun taakopdracht om de grondrechten te beschermen conform internationale verdragen. Tot dat moment moeten er in geen enkele wet nieuwe rollen of bevoegdheden worden toegekend die een inbreuk op grondrechten bij burgers (privacy) en bedrijven (vrijheid ondernemerschap) betekent.**

Over Human Rights in Finance.EU
Human Rights in Finance.EU is in augustus 2023 opgericht om de belangen te behartigen en schade te voorkomen voor alle consumenten en bedrijven die in hun grondrechten geraakt worden door financiële ondernemingen die in hun handelen veel verder gaan dan nodig is en in strijd met Europese grondrechten en regels rond marktwerking en consumentenbescherming opereren.

Wij bewaken, gezien onze doelstellingen, als rechtspersoon de grondrechten van alle (mogelijke) klanten van instellingen die economisch transactieverkeer faciliteren. Tegelijk houden wij ook oog voor de financiële instellingen zélf, waar die in de uitvoering van hun bedrijfsbeleid geconfronteerd worden met (een plicht tot) het schenden van grondrechten die hun ondernemersvrijheid belemmert. Voor een verdere schets van onze activiteiten en prioriteiten verwijzen wij naar ons eerste jaarverslag.

Overheidsplicht: geen onrechtmatige en disproportionele massa-surveillance
Speciale aandacht heeft voor onze stichting voor het thema massasurveillance en profilering. Wij bewaken alle vormen van toekomstige regelgeving die aan bedrijven/overheden een te vergaande plicht tot profilering en massa-surveillance oplegt. Dit vloeit rechtstreeks voort uit de resolutie A/HRC/34/7: Privacy in a Digital Age.

De genoemde resolutie is door Nederland erkend en roept Staten op om het recht op privacy te beschermen en te borgen dat de verplichtingen onder nationale regelgeving niet strijdig zijn met de verplichtingen onder internationaal recht (zoals het verdrag van Rome, het Europees Handvest) om het recht op privacy en privé-leven te beschermen. Als vervolg zegde de toenmalige regering toe voortaan bij wetsvoorstellen een goede grondrechten toetsing te doen. Maar die kennis is bij het Ministerie van Financiën, vermoedelijk door snelle functieroulaties, niet echt top of mind of top priority.

Wij wijzen in dit verband nadrukkelijk op de bepalingen 6c en 6j die de opdracht aan staten bevat om terughoudend te zijn met het maken van een inbreuk op privé-leven:

> *6c: To review, on a regular basis, their procedures, practices and legislation regarding the surveillance of communications, including mass surveillance and the interception and collection of personal data, as well as regarding the use of profiling, automated decision-making, machine learning and biometric technologies, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;*
>
> *6j: To refrain from requiring business enterprises to take steps that interfere with the right to privacy in an arbitrary or unlawful way, and to protect individuals from harm, including that caused by business enterprises through data collection, processing, storage and sharing and profiling, and the use of automated processes and machine learning;*
> *Bepaling*

Speerpunt HRIF.EU: vermijding van overmatige en onrechtmatige monitoring
Uit de door de Nederlandse staat in allerlei verdragen onderschreven grondrechten volgt dat we als samenleving voorzichtig moeten zijn met massamonitoring, big data en profilering. Dit is terug te zien in herhaalde visies van de European Data Protection Board, de Autoriteit Persoonsgegevens, de Raad van State. In Nederland zijn we evenzo met een serie aan grondrechtschendingen geconfronteerd die deels via de rechter (SyrI), deels via boete's (Belastingdienst, ICS etc) zijn geadresseerd.

HRIF.EU herkent deze zorg rond teveel monitoring en sleepnetten en het vormt een actief speerpunt van onze publicitaire en educatieve werk. Zo hebben we in februari namens bijna 15.000 bezorgde burgers en 9 belangenorganisaties aan de Tweede Kamer een petitie aangeboden opdat een einde komt aan overmatige monitoring door banken en aan onnodige sleepnetten met data van burgers.

Waar zitten vraagpunten rond privacy in de financiële sector en het financieel toezicht?
We beginnen onze consultatiereactie bij het basale begin. Die luidt dat de Nederlandse toezichthouders, in het bijzonder DNB, de gewoonte hebben om eerst door middel van onbepaalde, juridisch ongekwalificeerde informatieverzoeken aan de onder toezicht staande instellingen om allerlei informatie te vragen. Er wordt gehint of verwezen naar het artikel in de Algemene wet bestuursrecht (Awb) dat men mee moet werken aan het toezicht en uit angst levert menig bedrijf dan maar snel de informatie aan. In tal van situaties wordt dan ook door de instelling persoonsinformatie van klanten overhandigd.

Voor een passende overhandiging van persoonsinformatie aan een toezichthouder is echter nodig dat de toezichthouder een expliciet beroep doet op artikel 5:16 van de Awb. Met dat artikel vordert de toezichthouder formeel informatie aan de onder toezicht staande instelling. Het vormt de juridische basis die de onder toezicht staande instelling nodig heeft om rechtmatig persoonsgegevens aan de toezichthouder te verstrekken. De speciaal voor die vordering opgeleverde/gemaakte informatie kan vervolgens ook niet tegen de instelling gebruikt worden. Evident is ook dat genoemde informatie op passende manier door de toezichthouder beschermd moet worden. En evenzo evident is dat de toezichthouder een informatieverzoek dat proportioneel is voor het doel van het onderzoek naar het functioneren van een instelling. Die afweging is altijd concreet voor een specifieke situatie.

Vraag 1: zijn de informatieverzoeken (DNB) wel voldoende juridisch bepaald/expliciet?
De staande praktijk, zeker bij het toezicht door DNB, is dat makkelijk en soms nogal ruimhartig informatie opgevraagd wordt bij instellingen waaraan de toets op proportionaliteit en noodzaak ontbreekt. Daarbij wordt de juridische context niet altijd netjes geëxpliciteerd en worden instellingen in feite stilzwijgend geforceerd tot afgifte van informatie welke feitelijk gewoon als proportionele informatievordering had moeten worden gevraagd.

De instelling die antwoord met de mededeling: kunt u er een proportionele informatievordering van maken moet vervolgens heel helder opschrijven: 'we werken graag mee aan het onderzoek' en zich passend serviel opstellen. De individuele toezichthouders hebben namelijk de neiging om zo'n verzoek om een informatievordering eerder te zien als een obstructie van het toezicht dan als verzoek om een goede en proportionele juridische basis onder het informatieverzoek te leggen. Die individuele toezichthouders zijn zich namelijk, wellicht door gebrekkige kennis van de Awb en privacy-regelgeving, niet altijd bewust van de logica die onder het verzoek van de instelling schuilt. Hier ligt een knellend, bijna dagelijks probleem.

Een vraag die bij deze wetsvoorstellen gesteld kan worden is: als de toezichthouder in de feitelijke praktijk nu al in de praktijk moeite lijkt te hebben om enkelvoudige informatievorderingen op een proportionele en passende grondslag uit te vaardigen, zou dan het massa-informatievorderingskanon dat de beide wetten omvatten, wel passend zijn? Het komt in de kern neer op bestendiging van een toezichtpraktijk waarin de toezichthouder ten onrechte meer informatie opvraagt en verwerkt dan passend onder een grondrechtentoets voor de onderneming (geen onnodige toezichtlast) en de klanten van die onderneming (geen onnodige opname in de database van toezichthouders)?

Probleem 2: sluit de privacy policy van de toezichthouders aan op de feitelijke rol?
Zowel DNB en AFM hebben een privacy policy die ziet op het onder zich hebben van persoonsgegevens van direkt onder toezicht vallende instellingen alsmede hun klanten. Er is hier een duidelijk verschil te zien tussen DNB en AFM. De AFM heeft een nette policy en het jaarverslag van de AFM verduidelijkt dat deze geaudit wordt en er aan bewustwording gewerkt wordt bij medewerkers. Aan DNB kant is dat duidelijk minder: de term AVG komt in het jaarverslag DNB alleen voor in het stuk van de accountant.

Echter, de actualisering van die policy en het herijken en auditen ervan laat, zeker waar het DNB betreft, te wensen over. Zo heeft DNB pas in september 2021, daartoe aangespoord door één van de onder toezicht staande instellingen, haar privacy policy toezicht uitgebreid richting de cryptosector. DNB hield echter al sinds mei 2020 toezicht op die sector en had op dat moment uit dien hoofde al tal van informatie, inclusief klantgegevens, in haar verwerking opgenomen. Of de genoemde data uitsluitend op EU grondgebied beschikbaar is, of door gebruikmaking van internationale cloud-providers, ook voor Amerikaanse overheid opvorderbaar, is niet duidelijk.

Knelpunt is dat, bij een hantering van een te ruime, te weinig expliciete vorderings-cultuur en onvoldoende duidelijkheid over de feitelijke verwerkings-structuur, in de individuele toezichtdossiers van de toezichthouders, zeker waar het bulk bevragingen betreft van transactieinformatie, persoonsgegevens aanwezig kunnen zijn zonder passende juridische titel. De titel waaronder deze gegevens bewust overgedragen kan worden (aan structuren als FEC) blijft veel te vaag en algemeen. Ook is mogelijk dat onbewust (door inhuur van buitenlandse serviceproviders of adviseurs die in een andere jurisdictie werken c.q. een cloud die ingezien kan worden door Amerikaanse overheid) de gegevens toch in jurisdicties terecht komen die niet kwalificeren als een gelijkwaardig beschermingsniveau.

Al met al is een veel strakkere audit nodig op de feitelijkheid en rechtmatigheid van de persoonsverwerking door toezichthouders zelf, waaronder ook begrepen de vraag of voldoende bij elke toezichthandeling de noodzakelijkheid is bepaald en waar er dataminimalisatie mogelijk is.

Vraag 3: Hoe compliant is de toezichthouder bij informatievorderingen de AVG?
Alhoewel de toezichthouders claimen te voldoen aan de AVG bij hun informatieverzoeken en verwerking van persoonsgegevens is de vraag of dit bij de opvraging van datasets of informatie die veel klanten betreffen werkelijk zo is. In de privacy policies wordt met een ruime schets gezegd: we hebben het nodig voor ons toezicht en dus mag het onder de AVG.

De AVG stelt echter in overweging 31 ook heel expliciet:

> ***Door overheidsinstanties ingediende verzoeken om verstrekking moeten in ieder geval schriftelijk, gemotiveerd en incidenteel zijn, en mogen geen volledig bestand betreffen of resulteren in het onderling combineren van bestanden.***

HRIF.EU heeft sterk de indruk dat in de praktijk de Nederlandse toezichthouders en het Nederlandse Ministerie van Financiën zich deze randvoorwaarde die uit de AVG voortvloeit niet bewust zijn. Zelfs áls er een passende informatievordering wordt gemaakt door toezichthouders, dan nog is niet geborgd dat de feitelijke motivatie die vordering voldoende schraagt in termen van noodzakelijkheid en proportionaliteit. Er worden juist wél volledige datasets opgevraagd en als onderdeel van het werk bij toezichthouders worden die datasets mogelijk wél gecombineerd.

De staande praktijk lijkt veeleer te zijn dat er dus massieve datasets door toezichthouders worden opgeslagen, bewerkt en verwerkt, in strijd met de AVG. Genoemde werkwijze blijft echter verscholen achter de deuren van het geheime toezicht en dat is geen goede zaak. Een meer onafhankelijke controle op de werkwijze van toezichthouders is gewenst, mogelijk zelfs een expliciet onderzoek door de Autoriteit Persoonsgegevens.

Vraag 4: Hoe verhoudt zich met de grondrechten en de AVG dat DNB sinds tenminste 2017 DNB via een informatieverzoek (niet eens een vordering) de volledige transactiepool van alle geldtransactiekantoren in een eigen datapool opzuigt, bewerkt en analyseert?

In de sector geldtransactiekantoren is sinds jaar en dag gebruikelijk dat DNB alle transactiedata opvraagt via een informatieverzoek. Uit het position paper van DNB van 7 februari 2017 aan de Tweede Kamer blijkt dat een eigen datapool is opgezet. De vraag doet zich nadrukkelijk gelden of genoemde datapool nog wel binnen het bereik van het individueel toezicht op de geldtransactiekantoren passend is. Wint hier het enthousiasme rond big data, analytics en Artificial Intelligence het van de behoefte binnen de kaders van de AVG te blijven?

> ***DNB speelt op verschillende manieren als toezichthouder een rol bij het voorkomen van betrokkenheid van de financiële sector bij terrorismefinanciering.*** *Dit varieert van het verrichten van onderzoek bij instellingen en het (daar) agenderen van het onderwerp en guidance geven, tot het waar nodig handhaven van wet- en regelgeving. Daarnaast worden ook eigen analyses verricht van transacties die door Money Transfer-kantoren worden uitgevoerd. Met deze analyses toetst DNB of de sector voldoende alert is op ongebruikelijke transacties. DNB werkt constant aan het verbeteren van de eigen toezichtmethodiek, bijvoorbeeld door te werken aan data-analyse op het terrein van bancaire data.*

Een vergelijkbare vraag kan gesteld worden rond het onderzoek naar de Russian Laundromat waarover DNB in haar position paper uit najaar 2020 over publiek-private samenwerking refereert. Met de Nederlandse banken samen werd een transactieoverzicht gemaakt, gecombineerd en beoordeeld. Genoemde werkwijze ziet er niet op voorhand AVG-compliant uit.

Vraag 5: Moet de publiek private samenwerking toezichthouders en instellingen zich ook tot het individueel transactieniveau en klantniveau uitstrekken of niet?

De aanname die onder de geconsulteerde wetsvoorstellen zou kunnen liggen, zou kunnen zijn dat het een goed idee kan zijn als de toezichthouders in feite ook over dezelfde data beschikken als de onder toezicht staande instellingen. Dat controleert beter is dan het idee. Het is echter sterk de vraag of dat gewenst is en hoe ver publiek private samenwerkingen eigenlijk moeten gaan.

Wij wijzen erop dat de European Data Protection Board op 28 maart 2023 (letter to the European Parliament, the Council, and the European Commission on data sharing for AML/CFT purposes in light of the Council's mandate for negotiation) heel duidelijke kaders aangeeft die de mate van data pooling en verwerking juist beperken. De EDPB merkt op:

> *From a privacy and data protection perspective, limiting the flow of information from obliged entities to public authorities constitutes a safeguard for individuals.*

Het is in dat licht bezien ook volstrekt begrijpelijk om te constateren dat de Bankwet 1998 de expliciete bepaling omvatte dat voor de taken van DNB geen verwerking van persoonsgegevens nodig is. De genoemde bepaling dient als een waarborg voor de grondrechten van burgers onder het Europees Handvest van de Grondrechten voor de Europese Unie.

Daarbij strekt de norm van artikel 8 van het Handvest, alsmede de norm van proportionaliteit onder het Verdrag van de Werking van de Europese Unie, tot het uitsluitend maken van een inbreuk indien deze strikt noodzakelijk is en daarbij proportioneel en als last resort (alle andere mogelijk middelen om doel te bereiken zijn uitgeput).

Ten principale kan gesteld worden dat het niet in de opdracht van de prudentiële toezichthouders besloten ligt om een kopie van de transactiedatabase van onder toezichtstaande instellingen onder zich te hebben. Dit argument kan wél in enige mate voor de AFM standhouden, vanwege het markttoezicht, maar ook dan is zeer de vraag of de huidige datarecords en persoonsgegevens die worden verwerkt voor het markttoezicht, op die manier nuttig/noodzakelijk zijn.

Vraag 6: Kan het vertrouwen in het AVG-compliant handelen door het Ministerie van Financiën, DNB en NVB standhouden indien de afgelopen 3 jaar deze drie partijen buiten de regels van strafrecht en AVG om vorm hebben gegeven aan het bancair sleepnet dat Transactie Monitoring Nederland heet?

Zoals uit onze website en jaarverslag blijkt is onze hoofddoelstelling dat dit jaar een eind komt aan de onrechtmatige gezamenlijke transactiemonitoring door banken bij Transactie Monitoring Nederland. Follow the Money schreef hier onlangs een helder artikel over: Banken bespieden samen je betalingen – illegaal, maar niemand grijpt in (J.H. Strop).

Het is schrijnend hierbij om in de publieke stukken te constateren dat het Ministerie van Financiën op zeker moment tijdens het regelgevend traject ontdekt dat TMNL in de praktijk veel verder ging dan was toegestaan en het Ministerie verkeerd had geïnformeerd:

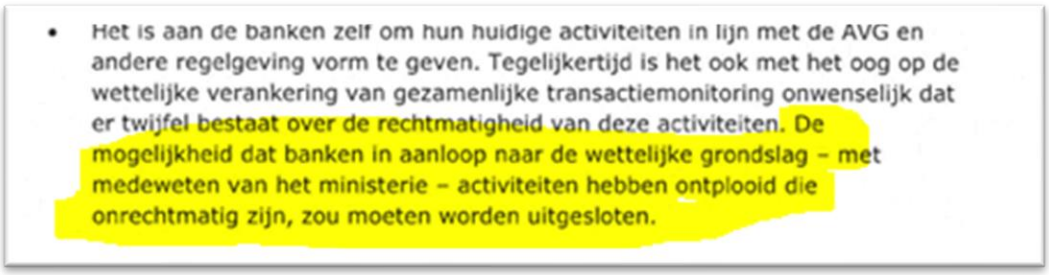
- Naar aanleiding van het kritische advies van de RvS hebben wij intensief met de banken gesproken over de mogelijkheden om de wettelijke grondslag voor gezamenlijke transactiemonitoring te beperken. Uit deze gesprekken kwam naar voren dat de huidige activiteiten van TMNL verder reiken dan eerder bekend was bij het ministerie.

De schoen wringt overigens niet alleen bij het uitbestedingsverbod transactiemonitoring artikel 10 onder de Wwft, maar ook bij het zonder geldige wetstitel verwerken van bijzondere persoonsgegevens. Het Ministerie schrijft hier zelf over ‘inbreuk op de privacy’ die gevoelig is.

Er worden bijzondere en strafrechtelijke gegevens verwerkt.	Dit is juist: transactiegegevens kunnen bijzondere en strafrechtelijke persoonsgegevens bevatten. We kunnen nog explicieter toelichten dat dit ook al gebeurt bij individuele monitoring van transacties en waarom dit nodig is. Dit blijf desondanks een inbreuk op de privacy en daarmee gevoelig.
Rechtsbescherming	

Het komt ons voor dat sprake is van méér dan gevoeligheid rond inbreuk op de privacy. In de kern ontbreekt een wettelijke grondslag onder Transactie Monitoring Nederland en zijn alle transactieverstrekkingen van banken aan TMNL (en vice versa) hierdoor onrechtmatig.

De stukken van het Ministerie laten zien dat het Ministerie van Financiën niet in een situatie wil komen dat ze feitelijk een wetsovertreding moet gedogen, vooruitlopend op de totstandkoming van de wet.



- Het is aan de banken zelf om hun huidige activiteiten in lijn met de AVG en andere regelgeving vorm te geven. Tegelijkertijd is het ook met het oog op de wettelijke verankering van gezamenlijke transactiemonitoring onwenselijk dat er twijfel bestaat over de rechtmatigheid van deze activiteiten. De mogelijkheid dat banken in aanloop naar de wettelijke grondslag – met medeweten van het ministerie – activiteiten hebben ontplooid die onrechtmatig zijn, zou moeten worden uitgesloten.

De realiteit is echter dat banken en TMNL door door te gaan met Transactie Monitoring Nederland, de AVG en de wet gewoon overtreden. HRIF.EU heeft zich daarbij afgevraagd of dan ook niet sprake zou zijn van strafrechtelijke overtreding en dat blijkt inderdaad het geval. Onderstaande conclusie van advocaat Zeegers van Prakken D’Oliveira beschrijft hoe banken en TMNL nu het cybercime artikel 138c van het Nederlands wetboek van strafrecht overtreden.

Concluderend: Er is geen wettelijke grond of bevoegdheid voor het doorgeven van de transactie gegevens door banken aan TMNL – de oprichting van TMNL is een zelfstandig initiatief van de deelnemende banken. Het doorgeven van deze gegevens lijkt dan ook te kwalificeren als wederrechtelijk. Te meer nu, zoals hiervoor is opgemerkt, de Wwft financiële instellingen verbiedt om hun verplichting tot transactiemonitoring uit te besteden aan derden. Althans, de bevoegdheid om onderdelen van het cliëntenonderzoek wél uit te besteden aan derden, sluit transactiemonitoring expliciet uit.

Het doorgeven van bancaire transactiegegevens van zakelijke klanten door ABN AMRO, ING, de Rabobank, Triodos Bank en De Volksbank aan TMNL (en, via TMNL, aan de andere deelnemende banken) vervult daarmee alle bestanddelen van de delictsomschrijving uit artikel 138c Sr en kan daarmee worden aangemerkt als strafbaar feit.[11] Ook de terugmeldingen van TMNL aan individuele banken kwalificeert als zodanig nu zij voor de banken (de ander) een bewerking van de eerder onrechtmatige informatie doorgeeft.

Tussenconclusie: de staat van respecteren van grondrechten in het financieel toezicht is onder de maat
Human Rights in Finance.EU constateert dat de generieke trend die zichtbaar is in de achtereenvolgende rapporten over kindertoeslag schandaal, fraudebestrijding etc. evenzo zichtbaar is in het beleidsdomein van financieel toezicht. Omwille van algemeen geformuleerde, onvoldoende gemotiveerde fraudebestrijdingsdoelen worden grondrechten van bedrijven en burgers geschonden, zonder dat daaraan een passende democratische en juridische afweging van grondrechten ten grondslag ligt.

De meer gedetailleerde vragen en observaties die wij hiervoor hebben genoemd laten zien dat er hier geen sprake is van een incidenteel foutje dat kan gebeuren. Er is sprake van een systematische miskenning van het belang van grondrechten in het financieel toezicht. Dat blijkt ook uit het achterwege blijven van het noemen van burgerrechten organisaties bij de belanghebbenden bij dit voorstel.

In concrete zin wordt dit belang ook door DNB niet toegekend aan een partij als HRIF.EU. Toen wij na tal van beleefde vragen aan banken, NVB, Financiën en TMNL zelf uiteindelijk aan DNB vroegen om TMNL te stoppen via een handhavingsprocedure stelde DNB simpelweg dat HRIF.EU en haar petitie-ondertekenaars geen belang zouden hebben om haar dit te vragen**. Maar als een misdrijf tegen de openbare orde, meervoudige schending van de Avg en schending van de Wwft geen grond meer zou zijn om belanghebbende te zijn, hoe ziet DNB dan de bescherming van de grondrechten voor zich?**

Het is hoogst zorgelijk, tekend en kenmerkend dat we serieus in een situatie zijn gekomen dat de banken en TMNL zélf kwalificeren als plegers van een massale datadiefstal in betalingsverkeer sinds 2021 (een cybercrime). Het is opmerkelijk dat NVB de medepleger hiervan is die ervoor gezorgd heeft dat TMNL operationeel werd en die beleidsmatig naar de buitenwereld bleef verkopen dat het allemaal wel prima was, terwijl op het Ministerie van Financiën met zorg werd geconstateerd dat TMNL bijzondere persoonsgegevens verwerkt in strijd met de wet. En tegen die zorgelijke achtergrond kunt u onze consultatiereactie lezen: als het fundament ontbreekt moet je dat eerst repareren.

Onze reactie op de geconsulteerde voorstellen: niet doen en eerst de fouten repareren
Graag verwijzen wij ook naar de consultatiereactie van Privacy First op de twee wetsvoorstellen, welke wij volledig onderschrijven. Te zien is dat er veel fundamentele gebreken aan de wetsvoorstellen kleven: er wordt een feitelijk onbepaald mandaat/blanco cheque voorgesteld voor verwerking van persoonsgegevens zonder dat de strikte noodzaak is onderbouwd en de reikwijdte is ingeperkt. Het mandaat zelf is volstrekt onbepaald nu alle toekomstige regels in een AmvB worden neergezet.

Belangrijk is ook dat in plaats van de informatieverzoeken (die een informatievordering horen te zijn) een periodieke rapportageplicht wordt ingesteld. Daarmee wordt per definitie aangenomen dat vanaf dat moment er altijd een legitieme en proportionele reden is om al die data te krijgen. Genoemde rapportages zijn in feite een permanente informatievordering van overheden welke zou moeten voldoen aan de eisen onder het Prokuratuur Arrest (C-746/18). Genoemd arrest is ook in Nederlandse rechtspraak toegepast (ECLI:NL:GHDHA:2021:1588).

Wij wijzen op het belang van dit arrest voor alle informatievorderingen onder de Nederlandse wet. Zie hiertoe ook de bijdrage van Prof. Mr P. Verrest (De invloed van het Handvest op het Nederlandse strafrecht, p 154) in het pre-advies: Waarde, werking en potentie van het EU-Grondrechtenhandvest in de Nederlandse rechtsorde van de Nederlandse Juristenvereniging. Het komt ons voor dat juist ook bij de inrichting van informatievorderingen van financiële toezichthouders de genoemde uitspraak van het Hof van Justitie evenzo relevant is.

Ook de jurisprudentie van het Europees Hof van de Rechten van de Mens rond bulk-interceptie noopt tot terughoudendheid. Het verwerken van individuele persoonsgegevens in financieel toezicht (of ze pseudoniem zijn doet er hierbij niet toe) dient beperkt te zijn, individueel, gemotiveerd en aan voldoende waarborgen onderhevig. Wij verwijzen naar de zaken Centrum för Rättvisa v. Sweden (application no. 35252/08) en de zaak Big Brother Watch v. het VK, (application nos. 58170/13, 62322/14 and 24960/15).

AFM en DNB als toezichthouders op Artifical Intelligence in de financiële sector?
U kunt zich wellicht voorstellen dat, in het licht van de relevante internationale verdragsregels rond grondrechten, in het licht van de Europese jurisprudentie en in het licht van het beperkte besef en respect voor die grondrechten in de huidige beleidsgemeenschap van het Nederlands financieel toezicht (Ministerie van Financiën, DNB, NVB en iets minder mate AFM) voor HRIF.EU onbespreekbaar is dat het toezicht op Artifical Intelligence thuis zou horen bij deze toezichthouders.

De gezamenlijke notitie van DNB en AFM van 9 april 2024 over AI in de financiële sector laat zien dat de toezichthouder zich in theorie bewust zijn van de relevantie van de grondrechten. Dat is te prijzen en dat juicht HRIF.EU ook toe. Echter, het gaat er niet om of de theorie van het toezicht klopt, het gaat erom of in de praktijk de toezichthouders die bescherming van grondrechten waarmaken. Elk orgaan van de staat heeft namelijk de taak om voorkomende mensenrechtenschendingen teniet te doen, zodat zij die herkent.

Wij wijzen in dit verband op Resolutie 53/144 over Mensenrecht Verdedigers die op 9 december 1998 door de Verenigde Naties is aangenomen. Het toont in artikel 9.5 en 10 hoe organen van de Staat, maar ook bedrijven, niet stil kunnen zitten maar een opdracht hebben om mensenrechten schendingen direkt te onderzoeken als er iets aan de hand is.

> 5. The State shall conduct a prompt and impartial investigation or ensure that an inquiry takes place whenever there is reasonable ground to believe that a violation of human rights and fundamental freedoms has occurred in any territory under its jurisdiction.
>
> *Article 10*
>
> No one shall participate, by act or by failure to act where required, in violating human rights and fundamental freedoms and no one shall be subjected to punishment or adverse action of any kind for refusing to do so.

De wetsvoorstellen verduidelijken dat de regelgever en toezichthouders AFM en DNB juist graag heel veel gedetailleerde informatie als een sleepnet op permanente basis beschikbaar hebben. Het verleden laat echter zien dat Ministerie, DNB én AFM vooral intern besluiten dat hun eigen visie op taakstelling en werkwijze tot inherent gevolg heeft dat de grondrechten van burgers en bedrijven ondergeschikt gemaakt worden aan die taakstelling. Dat is echter de omgekeerde wereld.

De grondrechten van burger en bedrijven vormen een randvoorwaarde waarbinnen toezichthouders de uitdaging hebben om rechtmatig te handelen en uitsluitend op grond van keiharde en democratisch vastgestelde en aangetoonde noodzaak een inbreuk te maken die beperkt blijft tot het hoogst noodzakelijke. Blanco cheques, periodieke rapportages en alle eufemismes die in de wetsvoorstellen genoemd zijn om bulk interceptie en sleepnetten te verhullen, horen daarvan echter geen onderdeel te zijn, omdat ze strijdig zijn met gangbaar Europees recht en jurisprudentie (zie hiervoor).

Dat brengt ons bij de conclusie en ons hoofdantwoord op de twee consultaties:

> **1. De voorstellen zijn strijdig met Europees recht nu er bulkinterceptie en sleepnetten worden geformaliseerd. Die strijdigheid is door ontbrekende grondrechtenweging en onvoldoende professionaliteit bij het regelgevend Ministerie (nog niet onderzocht) maar dat zou wel moeten gebeuren.**
>
> **2. Daarnaast toont het voorstel en de huidige toezichtpraktijk dat de instituties die het financieel toezicht bepalen en uitvoeren, aantoonbaar een meer professionele invulling geven aan hun taakopdracht om de grondrechten te beschermen conform internationale verdragen. Tot dat moment moeten er in geen enkele wet nieuwe rollen of bevoegdheden worden toegekend die een inbreuk op grondrechten bij burgers (privacy) en bedrijven (vrijheid ondernemerschap) betekent.**

Voor zover toelichting op bovenstaande nodig is zijn we daartoe graag bereid.

Tenslotte adviseren we het Ministerie van Financiën om in voorkomende gevallen wél de vertegenwoordigers van bedrijven/organisaties/burgers en grondrechtenverderdigers te raadplegen en attenderen als het de bedoeling is nieuwe sleepnetten en bulk-interceptie te organiseren omwille van de vermeend hogere effectiviteit van het toezicht.

Met vriendelijke groet

Simon Lelieveldt
Digitaal getuurd

Voorzitter
Human Rights in Finance.EU