@zwnne

CIP-CONFERENTIE PUTTEN | 2 JUNI 2022
DIGITALE OVERHEID IN EEN DESTABILISERENDE WERELD

gegevensbeschermingsrecht in een digitaliserende wereld

Prof. mr. G-J. (Gerrit-Jan) ZWENNE

eLaw Leiden

CIP centrum informatiebeveiliging en privacybescherming

Als ik op een avond naar een café ga…

toepassing van de AVG

…en tegenover vier vrienden aan tafel in die openbare gelegenheid waarbij ik dus waarschijnlijk niet voldoe aan de uitzondering van de persoonlijke of huishoudelijke activiteit […] een weinig vleiende opmerking over mijn buurman maak, waarbij ik ook zijn persoonsgegevens vermeld die ik zojuist per e-mail heb ontvangen (dus geautomatiseerd en/of opgenomen in mijn bestand), word ik dan de verwerkingsverantwoordelijke voor die gegevens en gelden voor mij dan ineens alle (nogal zware) verplichtingen van de AVG? Omdat mijn buurman nooit toestemming heeft gegeven voor die verwerking (verstrekken door middel van doorzending), en omdat roddel waarschijnlijk nooit een van de in artikel 6 AVG opgesomde legitieme gronden zal zijn, zal ik met die verstrekking onvermijdelijk een aantal bepalingen van de AVG schenden, waaronder de meeste rechten van de betrokkene.

?

Prins over 'de toezichtreflex' (d.w.z. over AP)

rol van de toezichthouder

Vooraf 233

Rutte IV: toezichtreflex en Autoriteit Persoonsgegevens

4 Deze week is – met 28 januari als de Dag van de Privacy – een mooi moment om iets over de 'privacy-ambities' van Rutte IV te zeggen. Ik beperk me tot het toezicht.

Laat ik beginnen met het plan om de Autoriteit Persoonsgegevens (AP) als algoritme-autoriteit aan te wijzen. Alhoewel de keuze op het eerste gezicht een logische lijkt, zijn er redenen om deze te heroverwegen. Allereerst vanuit het belang van ministeriële verantwoordelijkheid en parlementaire controle. Afgelopen juni heb ik op deze plaats, voortbouwend op een ongevraagd advies van de Raad van State, gewezen op de staatsrechtelijke implicaties van het groeiend aantal en de steeds grotere rol van (Europese) toezichthouders. Kort gezegd: met het uitdijend arsenaal aan toezichthouders en activiteiten die daar worden belegd, kalft de ruimte voor ministeriële verantwoordelijkheid af. Sowieso is het wat mij betreft problematisch dat de AP nagenoeg zonder enige serieuze controle of reflectie standpunten uitdraagt die zich soms maar moeizaam verhouden met wat rechters of wetgever daarover hebben gezegd. Slechts spaarzaam kunnen deze standpunten door de rechter worden gecorrigeerd. Kortom, voor een adequate (parlementaire) controle op – en daarmee vooral ook maatschappelijk debat over – het gebruik van algoritmen is de AP niet de aangewezen keuze.

Een tweede overweging heeft te maken met de ambitie zelf: meer transparantie van en controle op algoritmen. Los van wat we precies onder algoritmen verstaan: ze hebben vaak niets met privacy van doen en zitten vrijwel overal (in). Dus hoe willen we de geformuleerde ambitie überhaupt realistisch bij deze specifieke toezichthouder beleggen? Bovendien: moet het kabinet wel direct met een toezichthouder willen schermen? *Inzicht* in, *begeleiding* van en *controle* op de werking en effecten van algoritmen veronderstelt niet per se toezicht. Initiatieven zoals het algoritmeregister van de gemeente Amsterdam laten zien dat het ook anders kan.

Dat brengt mij op mijn derde, wat bredere, punt. Moeten de AP en vooral de hardwerkende medewerkers niet eerst de ruimte krijgen de bestaande taakopdracht beter ter hand te nemen, in plaats van weer een nieuwe klus erbij? Het kabinet wil de AP versterken en geeft structureel extra geld. Weliswaar niet het budget van 100 miljoen euro waar de AP voor had gepleit, maar wel meer dan de nul op het rekest die de toezichthouder bij de recente miljoenennota kreeg. Toch, voor het versterken van de AP is meer nodig dan extra financiële armslag. Onlangs nog bleek de toezichthouder niet te hebben voorzien in essentieel instrumentarium als een systeem voor kwaliteitszorg en audits op het primaire proces. Ook ontbreken volgens het evaluatierapport een volwaardige controlfunctie en een geautomatiseerd zaakvolgsysteem. Daarbij komt dat de AP in de discussie over extra middelen steevast de nadruk legt op activiteiten, aantallen en budgetten. Nauwelijks op (maatschappelijke) doelen en resultaten. Andere toezichthouders en inspecties lijken daarin verder te zijn. Zo wordt uit de recente doorlichting van het Agentschap Telecom duidelijk dat men actief stuurt op kwaliteit van dienstverlening aan de hand van indicatoren voor klantwaarde en maatschappelijke waarde. En voor de ACM geldt dat er weliswaar kritiek op 'de afschrikwekkende werking' van het toezicht was, maar het veld zegt deze autoriteit wel te ervaren als een toegankelijke, deskundige en navolgbare toezichthouder. Min of meer vergelijkbaar is de conclusie in de evaluatie van de AFM. Een doorlichting aan de hand van soortgelijke indicatoren komt voor de AP al jaren niet beschikbaar. Waarom is mij niet duidelijk. Iedere lerende organisatie, ook als deze een onafhankelijke positie heeft, laat zich af en toe een spiegel voorhouden. En afgaand op signalen uit het veld vallen juist bij de AP nog wel stappen te zetten. Illustratief zijn de berichten over het meldloket voor datalekken dat daar is ondergebracht. Afgelopen november verscheen een open brief aan de AP die leest als een noodkreet, maar ook talloze waardevolle suggesties ter verbetering van dit meldloket bevat. Twee maanden zijn verstreken, maar de afzenders – de Vereniging voor Privacyrecht Advocaten en de Vereniging Privacyrecht – hebben tot op heden geen reactie mogen ontvangen. Ook is, voor zover de opstellers van de brief konden nagaan, niets met de suggesties gedaan. Op antwoord wachten ook de juristen die een WOB-verzoek bij de AP hebben ingediend om vast te kunnen stellen of sprake is van een beveiligingslek bij de AP zelf. Het vermoeden bestaat dat via het digitale formulier bedoeld om datalekken te melden, sprake is van onrechtmatige (namelijk bovenmatige) gegevensoverwerking door de AP zelf. Eerder al kwamen via dit meldformulier persoonsgegevens beschikbaar voor daartoe onbevoegde derden. Momenteel loopt de evaluatie van de uitvoeringswet AVG. Ondanks dat de AP een cruciale rol speelt bij de uitvoering van deze wet, vormt het functioneren van deze toezichthouder geen onderdeel van deze evaluatie. Wellicht komt dit aspect zijdelings wel aan de orde bij de doorlichting van de regeling voor de meldplicht datalekken (deze is onderdeel van de evaluatie).

In talloze TV-praatprogramma's is momenteel steevast de vraag: waar gaan de miljoenen die Rutte IV op diverse beleidsdossiers uittrekt nu precies naartoe? Wat betreft het privacytoezicht is dat hopelijk niet alleen: *meer* toezicht. Maar vooral ook toezicht dat voldoet aan meetbare indicatoren als responsiviteit, transparantie, consistentie, voorspelbaarheid en zorgvuldigheid. En: toezicht waarin de samenleving zich gerepresenteerd kan voelen.

Corien Prins

Het Vooraf staat ook op njb.nl/blogs

255

Sowieso is het [..] problematisch dat de AP nagenoeg zonder enige serieuze controle of reflectie standpunten uitdraagt die zich soms maar moeizaam verhouden met wat rechters of wetgever daarover hebben gezegd. Slechts spaarzaam kunnen deze standpunten door de rechter worden gecorrigeerd.

rode draad

toepassing van de AVG

rol van het toezicht

Vandaag twee praktijkvoorbeelden

waarover we het niet gaan hebben:
- *VoetbalTV*
- *cookiemuurverbod*
- *coronamelder*
- *enz.*

De boete die AP aan Enschede oplegde

De DSAR-guidelines van de EDPB

Enschede: passantentelling of wifitracking?

AUTORITEIT
PERSOONSGEGEVENS

Boete gemeente Enschede om wifitracking

Persbericht / 29 april 2021 Categorie:

De Autoriteit Persoonsgegevens (AP) geeft de gemeente Enschede een boete van 600.000 euro, omdat de gemeente wifitracking gebruikte in de binnenstad op een manier die niet mag. Daardoor was het mogelijk winkelend publiek en mensen die in de binnenstad wonen of werken te volgen.

Wifitracking in Enschede

De gemeente Enschede besloot in 2017 om via sensoren de drukte in de binnenstad te gaan meten. De gemeente huurde daarvoor een bedrijf in dat is gespecialiseerd in het tellen van passanten.

Meetkastjes in de winkelstraten vingen de wifisignalen op van de mobiele telefoons van passerende mensen. Ieders telefoon werd apart geregistreerd, met een unieke code.

wat is een «persoonsgegeven»..?

alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon

kost het al dan niet een onevenredige inspanning om de betrokkene te identificeren?

(26) [...] Om te bepalen of een natuurlijke persoon identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren, bijvoorbeeld selectietechnieken.

wat is «identificeerbaar»..?

Art. 4(1) AVG

als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator

bijvoorbeeld een naam, identificatienummer, locatiegegevens, online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon

IP-address, MAC-address

(30) Natuurlijke personen kunnen worden gekoppeld aan online-identificatoren via hun apparatuur, applicaties, instrumenten en protocollen, zoals internetprotocol (IP)-adressen, identificatiecookies of andere identificatoren zoals radiofrequentie-identificatietags. Dit kan sporen achterlaten die, met name wanneer zij met unieke identificatoren en andere door de servers ontvangen informatie worden gecombineerd, kunnen worden gebruikt om profielen op te stellen van natuurlijke personen en natuurlijke personen te herkennen.

HvJEU: Bodil Lindqvist

EHvJ 6 november 2003, C-101/01, ECLI:EU:C:2003:596

24. Het in [...] begrip persoonsgegevens omvat volgens de definitie in artikel 2, sub a, daarvan iedere informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Hieronder valt vanzelfsprekend iemands naam tezamen met zijn telefoonnummer of gegevens over zijn werksituatie en zijn liefhebberijen.
[..]
27. Derhalve moet op de eerste vraag worden geantwoord, dat het vermelden van verschillende personen op een internetpagina
naam of anderszins, bijvoorbeeld met hun telefoonnummer
informatie over hun werksituatie en hun liefhebberijen, als e
gedeeltelijk geautomatiseerde verwerking van persoonsgege
aan te merken.

HvJEU: Scarlet SABAM

51 Het staat namelijk vast dat het rechterlijk bevel tot invoering van het litigieuze filtersysteem een systematische analyse van alle inhoud veronderstelt en de verzameling en identificatie van de IP-adressen van de gebruikers die illegale inhoud via het netwerk versturen. Aangezien die IP-adressen de precieze identificatie van die gebruikers mogelijk maken, vormen zij beschermde persoonsgegevens..

Rb. MNL: Brein/Ziggo

Rechtbank Midden NLD 2 februari 2022 ECLI:NL:RBMNE:2022:297

Een IP-adres is dus een persoonsgeven voor degene die wettelijke mogelijkheden heeft om dat IP-adres met behulp van informatie van een isp aan een persoon te koppelen. Uit het [Breyer-]arrest lijkt te volgen dat het begrip "wettelijke mogelijkheden" door het Europese Hof ruim wordt opgevat. In het Breyer-arrest is immers overwogen dat van die wettelijke mogelijheden geen sprake is indien de identificatie van de betrokkene bij de wet verboden wordt of in de praktijk ondoenlijk is, bijvoorbeeld omdat zij – gelet op de vereiste tijd, kosten en mankracht – een excessieve inspanning vergt, bestaat het gevaar voor identificatie in werkelijkheid onbeduidend lijkt. De voorzieningenrechter concludeert daarom dat de mogelijkheid om (al dan niet via de rechter) NAW-gegevens van de gebruiker van een IP-adres bij de isp op te vragen, wel onder de in het Breyer-arrest bedoelde wettelijke middelen valt.
Dat Brein in het kader van de waarschuwingscampagne (nog
gegevens bij Ziggo op te vragen (en, wanneer dat zonder suc
vorderen) en dat het niet zeker is dat – als zij dat wel doet –
doet er niet aan af dat zij wel over dat wettelijke middel besc
gemoeide tijd, kosten en mankracht niet excessief zijn in de
adressen die Brein verzamelt dus ook ten aanzien van haar g

HvJEU: Breyer

Zie ook: HvJEU 17 juni 2021, C
ECLI:EU:C:2021:492, nr. 102

[E]en dynamisch IP-adres dat door een aanbieder va
onlinemediadiensten wordt geregistreerd telkens als
een website bezoekt die door deze aanbieder toegan
gemaakt voor het publiek, ten aanzien van die aanbieder [vormt] een persoonsgegeven [..], wanneer hij beschikt over wettige middelen waarmee hij de betrokken persoon kan identificeren aan de hand van extra informatie die bij de internetprovider van deze persoon berust.

Rb DHG: fietsendepot

Rechtbank Den Haag 20 oktober 2020, ECLI:NL:RBDHA:2020:9590

7. [V]erweerder [heeft] aannemelijk gemaakt dat binnen de gemeente Den Haag géén IP-adressen worden vastgelegd, opgeslagen en gekoppeld aan personen. Er is dan ook geen sprake van directe of indirecte herleidbaarheid naar personen. Daartoe is van belang dat verweerder heeft toegelicht dat IP-adressen indirect herleidbaar kunnen zijn tot een persoon, maar dat daarvoor middelen moeten worden ingezet om dit te kunnen vaststellen. Verweerder heeft daarbij aangegeven dat het ondoenlijk qua tijd en mankracht is om van alle burgers met wie gecommuniceerd wordt, de identificatie via een IP-adres te achterhalen. Daarbij is van belang dat de gemeente niet zelf over de gegevens om een koppeling te kunnen maken tussen een IP-adres en een burger beschikt, maar zijn er gegevens nodig van een Internet Service Provider. Nu de verwerking een excessieve inspanning van verweerder vergt, waardoor het gevaar voor identificatie in de praktijk onbeduidend is, kan het IP adres niet beschouwd worden als persoonsgegeven.

Enschede: geen onevenredige inspanning, zegt AP

AUTORITEIT PERSOONSGEGEVENS

Boete gemeente Enschede om wifitracking

Persbericht / 29 april 2021 Categorie

De Autoriteit Persoonsgegevens (AP) geeft de gemeente Enschede een boete van 600.000 euro, omdat de gemeente wifitracking gebruikte in de binnenstad op een manier die niet mag. Daardoor was het mogelijk winkelend publiek en mensen die in de binnenstad wonen of werken te volgen.

Wifitracking in Enschede

De gemeente Enschede besloot in 2017 om via sensoren de drukte in de binnenstad te gaan meten. De gemeente huurde daarvoor een bedrijf in dat is gespecialiseerd in het tellen van passanten.

Meetkastjes in de winkelstraten vingen de wifisignalen op van de mobiele telefoons van passerende mensen. Ieders telefoon werd apart geregistreerd, met een unieke code.

Bij [VERWERKER] is [..] de exacte locatie van de sensoren bekend en heeft men toegang tot het werkgeheugen en de software die draait op elke sensor. Tegelijk met een nieuwe detectie van een mobiel apparaat door een sensor is het bijvoorbeeld voor iemand van [VERWERKER] mogelijk om ter plaatse of via een camera waar te nemen welke persoon binnen het bereik van de sensor komt lopen. Vooral op stille momenten in de binnenstad leidt dit direct tot identificatie van de natuurlijke persoon. Ter controle kan de persoon worden gevraagd naar zijn/haar MAC-adres. Dezelfde manier van identificeren is mogelijk in geval van gepseudonimiseerde MAC-adressen en de bijbehorende locatiegegevens, omdat ook dan op het moment van detectie ter plaatse of via een camera de persoon in kwestie waargenomen kan worden

?

alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt…?

toepassing van de AVG

rol van de toezichthouder

EDPB DSAR Guidelines

Universiteit Leiden

COMMENTS

prof dr. G-J. (Gerrit-Jan) ZWENNE[*]

EDPB Guidelines 01/2022 on Data Subject Access, version 1.0, adopted on 18 January 2022

INTRODUCTION

Without a doubt, data subject access rights are among the most useful rights the GDPR provides data subjects to enhance transparency and to facilitate control over the processing of their personal data. At the same time, the exercise of access rights by data subjects gives rise to many complaints and disputes.[1] As a result, there is a lot of detailed and nuanced case law on the scope of access rights and the applicable exemptions. In addition to the judgments of Court of Justice of the European Union, notably *Rijkeboer*,[2] *IND*[3] and *Nowak*,[4] there is also a large volume of court decisions by member states' courts, including judgments of the highest national civil and administrative courts.

Surprisingly, the EDPB Guidelines 01/2022 on Data Subject Access Rights seem to ignore, and in some instances even contradict, member state national courts' decisions on data subject access rights. In that respect, the guidelines raise some interesting questions on the legitimacy and validity of the Guidelines. Indeed, pursuant to Article 70(1)(e) GDPR the European Data Protection Board (hereinafter "EDPB" and also "the Board") can issue guidelines, recommendations and best practices in order to encourage consistent application of the Regulation. But does that imply that the Board can overrule or set aside judgments of national courts? Probably not.

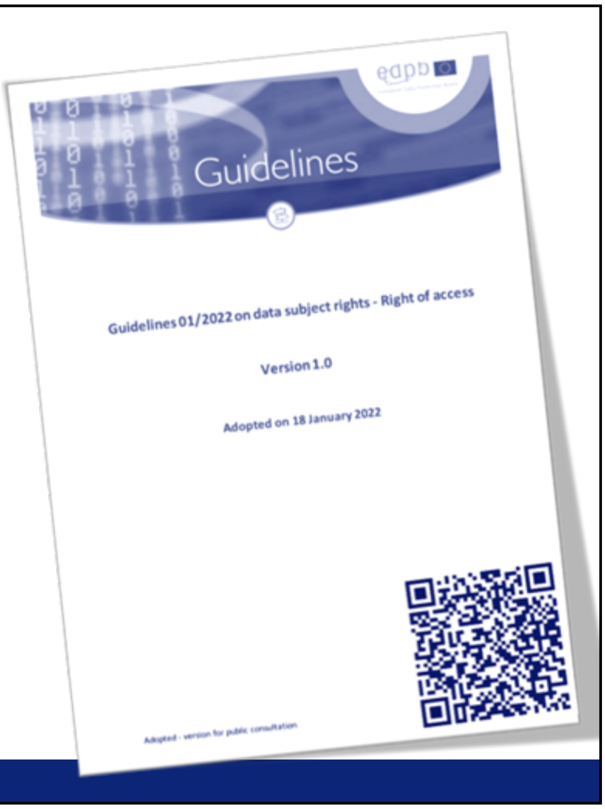
This short note will provide some of the most noticeable examples of statements made in the guidelines that are, to say the least, at odds with well-established case law in the Netherlands. In view of the timeframes set by the Board for this consultation, this analysis cannot be exhaustive. However, it is to be expected that further legal analysis of relevant case law in the Netherlands and other member states will reveal many more cases in which the guidelines deviate from national courts' case law. In any case, such legal analysis is needed and assuming the results of that analysis will be incorporated in version 2.0 of the Guidelines, it is likely to result in less unbalanced and controversial guidelines than that found in the current version 1.0. Most likely, this will do

---

[*] G-J. (Gerrit-Jan) ZWENNE is a full professor law and digital technologies, Leiden University in the Netherlands and partner at the law firm Pels Rijcken in The Hague, also in the Netherlands.

eLaw Leiden

1



edpb

Guidelines

Guidelines 01/2022 on data subject rights - Right of access

Version 1.0

Adopted on 18 January 2022

Adopted - version for public consultation

35. If the data subject, who has been asked to specify the scope of its request, confirms to seek all personal data concerning him or her, the controller of course has to provide it in full.

73. […] It should be emphasised that using a copy of an identity document as a part of the authentication process creates a risk for the security of personal data and may lead to unauthorised or unlawful processing, and as such it should be considered inappropriate

165. However, data subjects are not obliged to give reasons or to justify their request. As long as the requirements of Art. 15 GDPR are met the purposes behind the request should be regarded as irrelevant.

35. If the data subject, who has been asked to specify the scope of its request, confirms to seek all personal data concerning him or her, the controller of course has to provide it in full.

Hof Den Bosch 11 december 2014, ECLI:NL:GHSHE:2014:5221

7.12.8 [H]et hof [is] van oordeel dat het kennisnemingsverzoek van [appellanten] zo weinig concreet is dat gesproken moet worden van een ontoelaatbare 'fishing expedition'.

7.12.9. Het voorgaande betekent dat, voor zover daar door de Rabobank nog niet aan was voldaan, de verzoeken" van [appellanten] vanwege de onbepaaldheid daarvan moeten worden afgewezen.

Rb A'dam 20 juni 2019, ECLI:NL:RBAMS:2019:4404

4.11.Integrale honorering van het verzoek van [verzoeker] om alle verwerkte persoonsgegevens zou onder deze omstandigheden niet alleen welhaast praktisch ondoenlijk zijn maar ook een veel te omvangrijke en daarmee kostbare zoektocht van [verweerster] meebrengen.

Rechtbank NHLD 23 mei 2019, ECLI:NL:RBNHO:2019:4283

4.17.Gelet op de grote hoeveelheid gegevens die de rechtbank Amsterdam [verwerkingsverantwoordelijke] verwerkt mag van [verzoekers] worden verwacht dat zij preciseren op welke informatie of welke verwerkingsactiviteit het verzoek betrekking heeft.

73. [...] It should be emphasised that using a copy of an identity document as a part of the authentication process creates a risk for the security of personal data and may lead to unauthorised or unlawful processing, and as such it should be considered inappropriate [...]

ABRvS 9 december 2020, ECLI:NL:RVS:2020:2833

5.2 [..] Het uitgangspunt dat een kopie van een identiteitsbewijs wordt gevraagd bij een inzageverzoek, wordt niet onredelijk geacht. Dit waarborgt een deugdelijke identiteitsvaststelling zonder dat afbreuk wordt gedaan aan het recht van betrokkenen om zich vrijelijk tot het college te wenden.

Rb R'dam 21 januari 2020, ECLI:NL:RBROT:2020:515

4.8 [...] Het inzagerecht heeft tot doel de betrokkene in staat te stellen kennis te nemen van de persoonsgegevens die over hem zijn verzameld en te controleren of die gegevens juist zijn en rechtmatig zijn verwerkt. Ter gelegenheid van de mondelinge behandeling heeft [verzoeker] verklaard dat hij deze verzoeken uitsluitend heeft ingediend om zijn onschuld te bewijzen met stukken die betrekking hebben op procesdossiers waarin hij als procespartij betrokken was. [..] Het doel van [verzoeker] bij zijn inzagerecht ziet niet op de bescherming van persoonsgegevens zodat sprake is van misbruik van recht.

HR 16 maart 2018, ECLI:NL:HR:2018:365

3.3.3. [...] Richtlijn 95/46/EG [...] die door de Wbp is geïmplementeerd, [stelt] de betrokkene in staat te controleren of zijn persoonsgegevens juist zijn en rechtmatig zijn verwerkt, ter bescherming van het recht van betrokkene op eerbiediging van zijn persoonlijke levenssfeer. Die controle kan dan leiden tot rectificatie, uitwissing of afscherming van de gegevens. De onderhavige vordering van [eiseres] is gericht op verkrijging van informatie ten behoeve van de onderhavige procedure en niet op het doel waartoe Richtlijn 95/46/EG strekt. [...] Het gaat hier dus niet om persoonsgegevens in de zin van die richtlijn.

165. However, data subjects are not obliged to give reasons or to justify their request. As long as the requirements of Art. 15 GDPR are met the purposes behind the request should be regarded as irrelevant.

slotsom

Bobek

we doen er goed aan...

kan het misschien wat duidelijker?

we moeten ons bezinnen op toepassing van de Avg en het toezicht daarop

waarom?

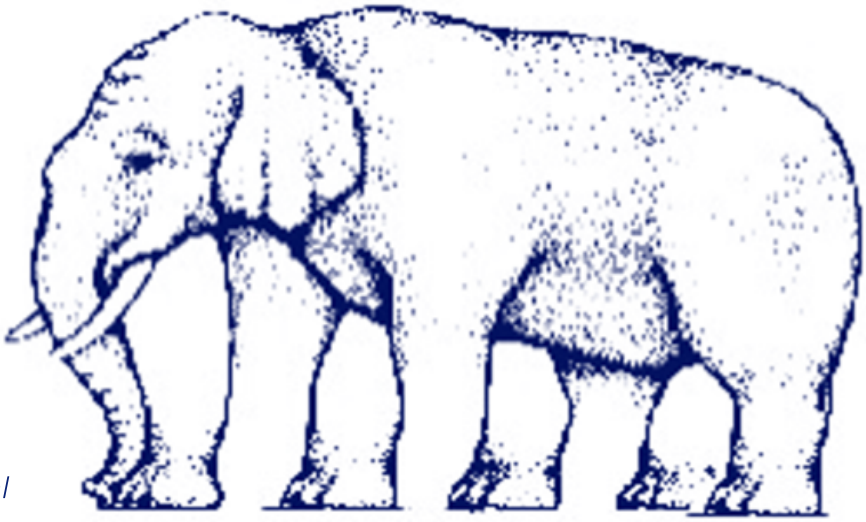
omdat de Avg anders geen betekenis meer heeft en het toezicht daarop ongeloofwaardig wordt

al was het maar omdat er nog veel meer aankomt:

- *Digital Market Act*
- *Digital Services Act*
- *AI-verordening*
- *ePrivacyverordening*
- *enz.*

Prins

toezichthouder is geen wetgever of rechter en is dus terughoudend met het introduceren van hele nieuwe regels



g.j.zwenne@law.leidenuniv.nl