Parlement en Wetenschap

FACTSHEET BESCHERMING PERSOONSGEGEVENS

Deze factsheet is tot stand gekomen in het kader van de samenwerking tussen de Tweede Kamer, de KNAW, NWO, VSNU en de Jonge Akademie.

22 november 2021

Auteurs: Dr. Tjerk Timan, TNO[1]

Bescherming persoonsgegevens

Inleiding

Dit factsheet is opgesteld op verzoek van de Vaste Tweede Kamercommissie voor Digitale Zaken. Voor de juridische inzichten zij verwezen naar het factsheet van prof. Gerrit-Jan Zwenne (d.d. 19-10-2021). Hieronder ga ik in op een aantal niet-juridische elementen die spelen rond de bescherming van persoonsgegevens.

Samenvatting

Er is een aantal conceptuele en een aantal praktische redenen voor het feit dat de AVG gezien kan worden als een succes, maar ook als een nog niet voltooide missie. Een eerste reden is dat de juridische opgestelde concepten en aannames op het gebied van controle en toestemming gebaseerd zijn op het idee van een contract (m.a.w. twee partijen spreken iets af en ondertekenen een soort 'gebruikersovereenkomst'). Dit afsluiten van een contract over het gebruik van persoonsgegevens tussen datasubject en datacontroller of -processor heeft weinig van doen met de sociale of technologische werkelijkheid van digitale diensten en ons digitale dagelijks leven. Het aantal databases waarin onze persoonsgegevens staan is niet te overzien[2] en is het niet per se duidelijk hoe juridische regels voor het bezitten van persoonsgegevens zijn te vertalen in technische methodieken of standaardmanieren voor werken met persoonsgegevens[3].

Daarnaast zijn persoonsgegevens - als afgeleide van een identiteit - per definitie interactief en sociaal: een identiteit, en dus ook persoonsgegevens, heb je in relatie tot iets of iemand anders (m.a.w. daar kan de facto nooit in alle soevereiniteit controle over uitgeoefend worden[4]). De kernvraag die hieraan voorafgaat is dan ook waar precies toestemming voor gegeven wordt: een proces, toegang tot een serie bits en bytes, een behandeling, of wijziging van de status van wat die bits of bytes al dan niet toelaten etc.

Ook zijn de notie van wat een persoonsgegeven precies is en de reikwijdte van die notie onderhevig aan veranderingen – zowel in technologie als in ons

[1] Tjerk Timan is werkzaam bij de afdeling Strategy, Analysis & Policy van TNO.

[2] https://www.wired.com/story/wired-guide-personal-data-collection/

[3] Kutyłowski, M., Lauks-Dutka, A., & Yung, M. (2020, September). GDPR–Challenges for Reconciling Legal Rules with Technical Reality. In European Symposium on Research in Computer Security (pp. 736-755). Springer, Cham.

[4] de notie van 'controle hebben' over gegevens, of over technologie in het algemeen wordt door juristen nauwelijks bevraagd; in kritische sociale wetenschappen wordt het gezien als een normatieve en masculiene kijk op de wereld en op technologie: de aanname je controle moet hebben als individu en dat controle iets positiefs is: iets nastrevenswaardigs. Zie Wajcman, J. (2010). Feminist theories of technology. *Cambridge journal of economics, 34*(1), 143-152.

gebruik daarvan (was voor de tijd van smartphones 'locatie' een persoonsgegeven?[5]). Hoewel de AVG ontworpen is als technologieneutrale wetgeving blijkt het toch lastig om de wet goed toe te passen in een snel veranderend sociaal-technologisch landschap[6].

De scheiding die de wetgever maakt tussen persoonsgegevens en niet-persoonsgegevens lijkt op papier logisch, maar is in de praktijk niet zo makkelijk[7]. Daarnaast levert de alomtegenwoordige digitale technologie evenals de datageneratie die daarmee gepaard gaat een groot risico op re-identificatie van geanonimiseerde persoonsgegevens[8], of het identificeren van personen op basis van indirecte indicatoren en metadata (de zogenaamde *mosaic-theory*[9]). Dit is een grote uitdaging voor privacywetgeving in het digitale domein, zoals de AVG. Uiteraard kan de AVG ingezet worden om de risico's te ondervangen van privacyschending die zich op deze indirecte wijze manifesteren, maar daarmee wordt het werkterrein van de AVG zo groot dat sommigen claimen dat zij onuitvoerbaar is geworden[10]. We zien dan ook dat ondanks de internationale impact van de AVG op de ontwikkeling van internationale normen en privacy-wetgevingsontwikkelingen buiten Europa, de verordening op kleinere schaal vooral leidt tot veel procedurele (en juridische) onduidelijkheid en onzekerheid[11], waarbij het datasubject (de burger, de consument) vaak maar marginaal onderdeel is van de discussie.

Over het vertrouwen in de AVG als instrument om privacy te beschermen zijn verschillende cijfers en studies te vinden: in het algemeen is dat vertrouwen bij burgers vrij laag[12]. Dit vertrouwen staat verder onder druk door een verminderd vertrouwen in de overheid alsook door een vrij recente 'techlash'[13] en meer wantrouwen jegens aanbieders van digitale diensten en de opkomst van AI[14].

---

[5] Georgiadou, Y., de By, R. A., & Kounadi, O. (2019). Location Privacy in the Wake of the GDPR. ISPRS international journal of geo-information, 8(3), 157.

[6] Zie de problemen rondom gegevensbescherming en Blockchain, bijvoorbeeld, waar de technologische principes in fundamentele tegenstelling staan tot de uitgangspunten van de AVG, beschreven in o.a. Tatar, U., Gokce, Y., & Nussbaum, B. (2020). Law versus technology: Blockchain, GDPR, and tough tradeoffs. *Computer Law & Security Review, 38*, 105454.

[7] Zie Graef, I., Gellert, R., & Husovec, M. (2018). Towards a holistic regulatory approach for the European data economy: Why the illusive notion of non-personal data is counterproductive to data innovation.

[8] Zie bijvoorbeeld Shabani, M., & Marelli, L. (2019). Re-identifiability of genomic data and the GDPR: Assessing the re-identifiability of genomic data in light of the EU General Data Protection Regulation. *EMBO reports, 20*(6), e48316.

[9] Zie bijvoorbeeld Kerr, O. S. (2012). The mosaic theory of the Fourth Amendment. *Mich. L. Rev., 111*, 311.

[10] Zie Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology, 10*(1), 40-81. [dit is een mooie bijdrage in een interessante en relevante discussie waarin door de auteur ook andere geluiden worden genoemd; die zouden hier ook mogen worden genoemd. En wellicht toch ook dat de auteur – niet onterecht – stelling neemt in dat debat]

[11] Sirur, S., Nurse, J. R., & Webb, H. (2018, January). Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security* (pp. 88-95).

[12] https://www.eureporter.co/business/data-protection/2021/06/09/online-privacy-the-gdpr-struggle. Zie ook Bauer, P. C., Gerdon, F., Keusch, F., Kreuter, F., & Vannette, D. (2021). Did the GDPR increase trust in data collectors? Evidence from observational and experimental data. *Information, Communication & Society*, 1-21.

[13] 'a strong negative feeling among a group of people in reaction to modern technology and the behaviour of big technology companies' (https://dictionary.cambridge.org/dictionary/english/techlash)

[14] van Dijck, J. (2020). Governing digital societies: Private platforms, public values. *Computer Law & Security Review, 36*, 105377.

Vanuit zowel juridisch als technisch oogpunt zijn er naast de AVG veel beleidsontwikkelingen vanuit Europa, erop gericht om digitale gegevensbescherming een stap verder te brengen. Vooral aan de technologische kant van regulering (naast andere modaliteiten van regulering zoals wetgeving, sociale normen en de markt), moet veel gedaan worden om ontwikkelaars van digitale diensten beter te ondersteunen bij het toepassen van *privacy-preserving technologies* en *privacy enhancing technologies*. Aan de kant van burgers en consumenten is er op privacybeschermingsgebied veel te halen in de vorm van educatie op het gebied van digitale geletterdheid[15] en digitale weerbaarheid.

1. Welke rechten en plichten hebben betrokkenen wanneer zij toestemming verlenen aan digitale dienstverleners voor het verzamelen, verwerken en delen van persoonsgegevens?

Voor de rechten van betrokkenen ('datasubjects') verwijs ik naar de factsheet van Gerrit-Jan Zwenne. De AVG bevat geen verplichtingen voor het datasubject maar verplichtingen voor dataprocessors en datacontrollers[16].

2. Hoe bewust en geïnformeerd zijn burgers over hun rechten en plichten wanneer ze toestemming verlenen aan digitale dienstverleners voor het verzamelen, verwerken en delen van hun persoonsgegevens?

Er is veel gezegd en geschreven over wat het geven van geïnformeerde toestemming (*informed consent*) in de context van digitale diensten kan betekenen (en wat niet[17]), veelal in juridische[18] en ethische literatuur[19]. Het gaat daarbij vooral over de problematiek van de reikwijdte en duur van geldigheid van toestemming; over de wijze van vragen van die toestemming (leidt aanvinken wel echt tot geïnformeerde toestemming?), en in hoeverre er sprake is van '*opt out*'-mogelijkheden[20].

Vanuit methodologisch perspectief is er op de toestemmingsvraag in relatie tot de AVG wel het een en ander op te merken. De AVG probeert een socio-technisch systeem, inclusief een nieuw soort gedrag dat voortkomt uit de interactie tussen mens en digitaal apparaat[21], te vangen in bestaande toestemmingsvormen zoals we die kennen uit sociaalwetenschappelijk of

---

[15] Alhoewel we het in NL aardig goed doen: Nederlanders in Europese kopgroep digitale vaardigheden (cbs.nl)
[16] Hintze, M. (2018). Data controllers, data processors, and the growing use of connected products in the enterprise: Managing risks, understanding benefits, and complying with the GDPR. *Journal of Internet Law (Wolters Kluwer), August*.
[17] Leenes, R., & Kosta, E. (2015). Taming the cookie monster with dutch law–a tale of regulatory failure. *Computer Law & Security Review, 31*(3), 317-335.
[18] Van Alsenoy, B., Kosta, E., & Dumortier, J. (2014). Privacy notices versus informational self-determination: Minding the gap. *International Review of Law, Computers & Technology, 28*(2), 185-203.
[19] Flick, C. (2016). Informed consent and the Facebook emotional manipulation study. *Research Ethics, 12*(1), 14-28.
[20] Sanchez-Rola, I., Dell'Amico, M., Kotzias, P., Balzarotti, D., Bilge, L., Vervier, P. A., & Santos, I. (2019, July). Can i opt out yet? gdpr and the global illusion of cookie control. In *Proceedings of the 2019 ACM Asia conference on computer and communications security* (pp. 340-351).
[21] Privacy Literacy and the Everyday Use of Social Technologies. In *European Conference on Information Literacy* (pp. 33-49). Springer, Cham.

medisch onderzoek. Via een soort contract-wetgevingstaal'[22] heeft dit heeft geresulteerd in een 'theater[23]' van online vinkjes aan- of uitzetten en de bekende 'whatever-button'[24]. Ook bij veel mobiele diensten ('*apps*'), klikken we vaak op voorwaarden die vervolgens toegang vragen tot functionaliteiten die weinig met de dienst van doen hebben, maar wel meer data vergaren[25]. Deze datahonger en het aanbod van (vaak gratis) diensten van in de regel private (en niet-Europese) digitale dienstverleners wordt in verband gebracht met de uitspraak: 'als iets gratis is, bent u het product'[26]. Er wordt in dit soort online-interfaces ingespeeld op directe behoeftebevrediging via gladde en immersieve interfaces en 'click-bait'-content[27].

De vraag of er überhaupt zoiets bestaat als geïnformeerde toestemming op sociale media en soortgelijke digitale diensten wordt door zowel juridische als niet-juridische wetenschappers in twijfel getrokken[28], mede omdat geen sprake is van rationele of gelijkwaardige waarde-uitwisseling. Veeleer gaat het om manipulatieve tactieken om mensen zo lang mogelijk binnen een bepaald digitaal ecosysteem te houden met als doel constant de aandacht te vangen[29].

De rol van AI in het automatisch genereren van vorm en inhoud om zo de strijd om aandacht[30] - en dus reclametijd – te winnen, mag in deze context niet worden onderschat. De AVG lijkt, ondanks haar artikel 22 over profilering[31], niet toegerust voor deze realiteit, mede omdat het onderwerp kunstmatige intelligentie (AI) nog niet zo prominent op de agenda stond ten tijde van de ontwikkeling van de AVG. Er klinkt dan ook een roep om artikel 22 te herzien omdat het in de huidige vorm te mager zou zijn (bijna een soort '*after-thought*')[32]. Ook zou ervoor gekozen kunnen worden om de regulering van automatische profilering te laten werken via de recent voorstelde AI Act en de bijbehorende Acts[33], als onderdeel van een nieuw 'regulatory package' waarin ook onlinegegevensbescherming, onlinetracking

---

[22] Zie Monteleone, S. (2015). Addressing the Failure of Informed Consent in Online Data Protection: Learning the Lessons from Behaviour-Aware Regulation. *Syracuse J. Int'l L. & Com., 43*, 69.
[23] Fassl, M., Gröber, L. T., & Krombholz, K. (2021, May). Stop the Consent Theater. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-7).
[24] Stevenson, M. Interactivity, Government and Affect.
[25] Momen, N., Hatamian, M., & Fritsch, L. (2019). Did app privacy improve after the GDPR?. IEEE Security & Privacy, 17(6), 10-20.
[26] Papadopoulos, P., Kourtellis, N., Rodriguez, P. R., & Laoutaris, N. (2017, November). If you are not paying for it, you are the product: How much do advertisers pay to reach you?. In Proceedings of the 2017 Internet Measurement Conference (pp. 142-156).
[27] Morozov, E. (2013). *To save everything, click here: The folly of technological solutionism*. Public Affairs.
[28] Gray, C. M., Santos, C., Bielova, N., Toth, M., & Clifford, D. (2021, May). Dark patterns and the legal requirements of consent banners: an interaction criticism perspective. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-18).
[29] Susser, D., Roessler, B., & Nissenbaum, H. (2019). Online manipulation: Hidden influences in a digital world. *Geo. L. Tech. Rev., 4*, 1.
[30] Marwick, A. E. (2015). Instafame: Luxury selfies in the attention economy. *Public culture, 27*(1), 137-160.
[31] Zie González, E. G., & De Hert, P. (2019, April). Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles. In Era Forum (Vol. 19, No. 4, pp. 597-621). Springer Berlin Heidelberg en Bygrave, L. A. (2019). Minding the machine v2. 0: The EU General Data Protection Regulation and automated decision making. Algorithmic Regulation (Oxford University Press 2019, Forthcoming, University of Oslo Faculty of Law Research Paper No. 2019-01.
[32] Radical rewriting of Article 22 GDPR on machine decisions in the AI era – European Law Blog
[33] Post GDPR EU laws and their GDPR mimesis. DGA, DSA, DMA and the EU regulation of AI – European Law Blog

en de uitdaging van het verlenen van toestemming in een wereld van slimme apparaten en zelflerende algoritmes worden geadresseerd[34].

De AVG en andere privacywetgeving zal veel verder moeten gaan dan de huidige scope van geïnformeerde toestemming via cookies op websites[35], willen we persoonsgegevens kunnen beschermen in digitale contexten die steeds vaker op de achtergrond meekijken, meelezen, of ons op afstand 'interpreteren' en leren kennen, met steeds minder mogelijkheden om daar geïnformeerde toestemming voor te geven[36].

3. Wanneer dit bewustzijn en de kennis hierover laag is, welke risico's brengt dat met zich mee?

In hoeverre mensen zich bewust zijn van mogelijke schending van hun privacy is moeilijk in te schatten. Er zijn verschillende kwantitatieve studies die worden uitgevoerd door bijvoorbeeld PEW Research Center in de VS[37] of door sociologen, via bijvoorbeeld Online Privacy Literacy Scales[38]. Echter, er bestaat een groot verschil tussen '*self-reported data*' (wat mensen denken te doen, of van iets vinden) en '*trace data*' (wat mensen daadwerkelijk doen online[39]). Een aangrenzend concept dat vaak genoemd wordt in deze context is de privacy paradox[40]: het feit dat mensen zich wel bewust zijn van een bepaald risico, maar dat ze er bewust, of onbewust, niet naar handelen. Bewust omdat het simpelweg niet kan[41]: de dienst of functionaliteit wordt niet geboden zonder een mogelijke inbreuk op privacy en/of een gedwongen 'toestemming', of onbewust omdat mensen niet beseffen waar ze precies toestemming voor geven, en zo hun kennis van of kijk op privacy niet omzetten in actie. Daarnaast loopt de perceptie van privacy en van de rechten die daarbij horen in Europa zeer uiteen[42], wat tot ongelijke rechtsbescherming kan leiden.

Ook voor het mkb is een laag bewustzijn van privacyrechten en -plichten een groot risico: veel bedrijven in Europa willen wel AVG-compliant opereren,

---

[34] Zie https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package https://iapp.org/news/a/proposal-for-an-eu-data-governance-act-a-first-analysis/ https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

[35] Koops, B. J., Newell, B. C., Timan, T., Skorvanek, I., Chokrevski, T., & Galic, M. (2016). A typology of privacy. *U. Pa. J. Int'l L., 38*, 483.

[36] Zie Kudina, O. (2019). Alexa Does Not Care. Should You?: Media Literacy in the Age of Digital Voice Assistants. *Glimpse, 20*, 107-115.

[37] Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information | Pew Research Center

[38] Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale"(OPLIS). In *Reforming European data protection law* (pp. 333-365). Springer, Dordrecht. Zie ook Pingo, Z., & Narayan, B. (2018, September).

[39] Menchen-Trevino, E. (2013). Collecting vertical trace data: Big possibilities and big challenges for multi-method research. *Policy & Internet, 5*(3), 328-339.

[40] Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security, 64*, 122-134.

[41] Strycharz, J., Ausloos, J., & Helberger, N. (2020). Data Protection or Data Frustration? Individual Perceptions and Attitudes Towards the GDPR. *Eur. Data Prot. L. Rev.*, 6, 407.

[42] Rughiniș, Răzvan, Cosima Rughiniș, Simona Nicoleta Vulpe, and Daniel Rosner. "From social netizens to data citizens: variations of GDPR awareness in 28 European countries." *Computer Law & Security Review 42* (2021): 105585.

maar weten vaak niet waar ze moeten beginnen. Vaak hebben ze ook niet de middelen voor een juridische afdeling of om een *data protection officer* in dienst te nemen. De vele *guidelines* vanuit de EDPS[43], ENISA *nationale data protection authorities* (DPA) en onderzoeksprojecten[44] ten spijt, liggen daar nog grote praktische uitdagingen[45] en daarmee risico's van ongelijke behandeling en ontwikkeling in 'privacy maturity' bij ontwikkelaars en aanbieders van digitale diensten.

Daarnaast vindt een aanzienlijk deel van gegevensverzameling online 'onder water' plaats: er wordt, helaas ook door de grote onlineplatformen, veelvuldig gebruikgemaakt van zogenaamde 'dark patterns': een serie technieken (zoals verborgen pixels) waarbij zonder toestemming toch veel gegevens worden verzameld over bijvoorbeeld surf-, kijk- en klikgedrag: gegevens die zeker onder de AVG kunnen vallen en privacy online schenden. Meer nog dan de AVG biedt de *ePrivacy Directive*[46] perspectief op dit probleem, maar het totaal verbannen van dit soort praktijken zal een lastige en toch ook meer technische dan juridische aangelegenheid zijn[47]. Het grootste risico van een gebrek aan bewustzijn is naast ontmenselijking (de mens achter de datapunten wordt vergeten[48]), de verregaande mate van manipulatie en profilering zonder enige vorm van inspraak of 'opt out'. Anders gezegd: het risico dat privacy online een luxegoed wordt[49].

4. Welke mogelijkheden zijn er om het bewustzijn te verhogen en burgers beter geïnformeerd te maken?

Naast mogelijkheden zoals een privacykeurmerk en alle bezwaren daaromtrent (zie de factsheet van Gerrit-Jan Zwenne), zijn educatie op het gebied van digitale geletterdheid en digitale weerbaarheid van invloed. Dat geldt zowel voor kinderen (die extra bescherming nodig hebben omdat ze geen rationele actoren zijn die 'geïnformeerde toestemming' kunnen geven[50], maar wel ontzettend kwetsbaar en beïnvloedbaar zijn online – de AVG biedt daar niet altijd soelaas[51]), als voor jongeren en volwassenen.

Er is ook een rol weggegeld voor oude en nieuwe media om het publieke debat te voeren over privacy en gegevensbescherming, en over de rechten die burgers hebben (bijvoorbeeld onder de AVG). Vóór de COVID-19-crisis

---

[43] Guidelines | European Data Protection Supervisor (europa.eu)
[44] Zie h2020 SMEData
[45] Freitas, M. D. C., & Mira da Silva, M. (2018). GDPR Compliance in SMEs: There is much to be done. *Journal of Information Systems Engineering & Management, 3*(4), 30.
[46] Zuiderveen Borgesius, F. J., Kruikemeier, S., Boerman, S. C., & Helberger, N. (2017). Tracking walls, take-it-or-leave-it choices, the GDPR, and the ePrivacy regulation. *Eur. Data Prot. L. Rev., 3*, 353.
[47] Gray, C. M., Santos, C., Bielova, N., Toth, M., & Clifford, D. (2021, May). Dark patterns and the legal requirements of consent banners: an interaction criticism perspective. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-18).
[48] Zie ook 'Op zoek naar de mens in AI' TNO whitepaper 2021. https://publications.tno.nl/publication/34638226/j0PHlS/veenstra-2021-op.pdf
[49] Papacharissi, Z. (2010). Privacy as a luxury commodity. *First Monday*.
[50] Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). Children's data and privacy online: growing up in a digital age: an evidence review. Zie ook https://www.oecd.org/education/ceri/21st-Century-Children-Digital-Risks-and-Resilience.pdf
[51] Zie Macenaite, M. (2017). From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. *New Media & Society, 19*(5), 765-779.

was er al sprake van een '*techlash*[52]' en van meer media-aandacht voor privacy en persoonsgegevens (vooral na de onthullingen door Edward Snowden en de uitspattingen van Facebook): discussies over de inzet van corona-apps en andere digitale technologie in tijden van crisis hebben hoogstwaarschijnlijk wel een effect op het collectief bewustzijn van privacy en digitalisering[53]. Ook bedrijven spelen daarop in door zich als privacyvriendelijk te positioneren in de markt[54] en er zijn veel nieuwe spelers die privacy als uitgangspunt nemen bij het aanbieden van een digitale dienst (o.a. in de wereld van internetbrowsers en sociale media apps[55]).

5. Wanneer burgers toestemming verlenen aan digitale dienstverleners voor het verzamelen, verwerken en delen van persoonsgegevens; is de rechtspositie van de burger ten opzichte van de digitale dienstverlener even sterk als die in het consumentenrecht?

Voor een deel ligt dat aan de bekrachtiging van bestaande wettelijke kaders (zie ook de factsheet van Gerrit-Jan Zwenne). De AVG wordt niet in elk land met dezelfde rigueur toegepast en niet elke gegevensbeschermingsautoriteit (DPA) heeft gelijke middelen of bemensing[56]. Daarnaast is het de vraag of de manier waarop schade wordt behandeld wel altijd de bescherming van privacy als recht dient, en op welke wijze kan worden bepaald welke schade het gevolg is van een overtreding van de AVG[57]. Naast het probleem van bewijslast is een gerelateerd probleem de in de AVG gekozen aanpak van risicogebaseerde regulering[58]. Die dwingt partijen immers om alle vormen van privacyrisico's en geleden schade uit te drukken in economische termen of waarde. Recentelijk schreef de voorzitter van de Autoriteit Persoonsgegevens over de ontwikkelingen rond immateriële schade en smartengeld in relatie tot o,a. privacy[59].

Ook de vaak gebruikte '*reasonable expectation of privacy*'-test in relatie tot de rechtspositie zal steeds moeilijker toepasbaar zijn. Deze test gaat ervan uit dat een gemiddelde burger zich bewust kan en dus moet zijn van technologie in de openbare ruimte en de privacyrisico's die bij de technologie horen. Als zelfs een AI-ontwikkelaar al niet kan uitleggen hoe een algoritme tot bepaalde uitkomsten komt is dit wel heel erg veel gevraagd[60]. Mogen we van burgers verwachten dat ze weten hoe de algoritmes 'onder de motorkap' werken bij digitale diensteverlening in relatie tot mogelijke privacyschendingen? Mogen we verwachten dat mensen weten dat de CCTV-camera in het centrum automatisch gezichten kan herkennen, of dat ook hun stemgeluid en sociale mediaberichten tijdens een avond stappen opgevangen

---

[52] Véliz, C. (2021). Privacy and digital ethics after the pandemic. *Nature Electronics, 4*(1), 10-11.

[53] Utz, C., Becker, S., Schnitzler, T., Farke, F. M., Herbert, F., Schaewitz, L., ... & Dürmuth, M. (2021, May). Apps against the spread: Privacy implications and user acceptance of COVID-19-related smartphone apps on three continents. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1-22).

[54] https://blog.mozilla.org/en/mozilla/building-a-more-privacy-preserving-ads-based-ecosystem/

[55] The Battle for Digital Privacy Is Reshaping the Internet - The New York Times (nytimes.com)

[56] DPA-Budget-and-Staffing-Whitepaper.pdf (politico.eu)

[57] Malgieri, G., & Custers, B. (2018). Pricing privacy–the right to know the value of your personal data. *Computer Law & Security Review, 34*(2), 289-303.

[58] Gellert, R. (2018). Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review, 34*(2), 279-288.

[59] Privacyblog Aleid Wolfsen: Smartengeld | Autoriteit Persoonsgegevens

[60] Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society, 3*(1), 2053951715622512.

worden[61], en dat zij 'gelezen' en geïnterpreteerd worden door sensoren en algoritmes zonder tussenkomst van een dialoog of zelfs maar een consent-vinkje[62]? In dat opzicht is de rechtspositie zeker niet gelijk of even sterk (wel is het zo dat juist het consumentenrecht, zij het indirect, veel doet voor de bescherming van persoonsgegevens[63] - zie de factsheet van Gerrit-Jan Zwenne).

6. Welke mogelijkheden zijn er om de rechtspositie van de burgers als 'digitale consument' zo nodig te versterken?

Naast juridische maatregelen (zoals het voorstel tot 'personal data taxation' in Frankrijk[64]), bestaan er veel technologische oplossingen om ervoor te zorgen dat privacy beter beschermd wordt. Hierbij spelen onderwerpen als onlineveiligheid (cybersecurity) en digitale soevereniteit een belangrijke rol. Ook kan worden gedacht aan zelfregulering en coregulering, zoals standaardisatie en certificering, *codes of conduct* en marktwerking (privacy als *unique selling point*[65]). Ook bestaan er veel Europese onderzoeksprojecten op het gebied van *privacy enhancing technologies* en *privacy preserving technologies* die verder ontwikkeld en gestandaardiseerd kunnen worden[66]. Het gebruik van privacyvriendelijke technologie en alternatieve manieren om je op het internet te begeven zijn aan een opmars bezig; het aanbod van privacyvriendelijke digitale diensten is aan het groeien (denk aan *Brave, Signal, Deepl* etc.). Alhoewel de inzet van privacybeschermende technologie ook wordt afgedwongen door de AVG, valt hier nog veel winst te behalen en te ontwikkelen, vooral methodes om publieke waarden zoals privacy ook daadwerkelijk toe te passen in de praktijk[67] (zoals *value sensitive design, privacy-by-design*[68], *ethics-by-design, responsible research & innovation* etc). Ook gegevensbeschermingscertificering[69] en de ontwikkeling van technische standaarden zijn hierin van belang.

---

[61] Edwards, L., & Urquhart, L. (2016). Privacy in public spaces: what expectations of privacy do we have in social media intelligence?. *International Journal of Law and Information Technology, 24*(3), 279-310.

[62] Zie Nagenborg, M. (2017). Hidden in plain sight. In *Privacy in public space*. Edward Elgar Publishing.

[63] Kamara, I., & de Hert, P. (2018). Understanding the balancing act behind the legitimate interest of the controller ground: A pragmatic approach. In E. Selinger, J. Polonetsky, & O. Tene (Eds.), *Cambridge handbook of consumer privacy* (1 ed., pp. 321-352)

[64] Digital Services Tax in France (twobirds.com)

[65] Is privacy the new selling point? (cybernews.com)

[66] Zie Timan, T., & Mann, Z. (2021). Data Protection in the Era of Artificial Intelligence: Trends, Existing Solutions and Recommendations for Privacy-Preserving Technologies. In *The Elements of Big Data Value* (pp. 153-175). Springer, Cham.

[67] Perera, H., Hussain, W., Mougouei, D., Shams, R. A., Nurwidyantoro, A., & Whittle, J. (2019, September). Towards integrating human values into software: Mapping principles and rights of GDPR to values. In *2019 IEEE 27th International Requirements Engineering Conference (RE)* (pp. 404-409). IEEE.

[68] Hoepman, J. H. (2018). Privacy design strategies (the little blue book).

[69] Kamara, I., & De Hert, P. (2018). Data protection certification in the EU: Possibilities, actors and building blocks in a reformed landscape. In *Privacy and data protection seals* (pp. 7-34). TMC Asser Press, The Hague.

Disclaimer: De Jonge Akademie, KNAW, NFU, NWO, TNO en VSNU bemiddelen tussen parlementaire kennisvraag en wetenschappelijk kennisaanbod. De informatie in het kader van Parlement en Wetenschap is afkomstig van vooraanstaande wetenschappers, maar niet onderworpen aan peer review en niet door de wetenschapsorganisaties geverifieerd.

Tweede Kamer
DER STATEN-GENERAAL

KNAW

de jonge akademie

NWO

NFU

vsnu

TNO