Persoonlijke PIMS: privacyfort of luchtkasteel?

Janssen, H.L.

Publication date
2021
Document Version
Final published version
Published in
Privacy & Informatie

*Dr. mr. H.L. Janssen**

Persoonlijke PIMS: privacyfort of luchtkasteel?

234

Trefwoorden:
machtsongelijkheid, controle, persoonlijk informatiebeheersysteem (PIMS), gedecentraliseerde techniek, empowerment, AVG, verwerkingsgrondslagen, rechten van betrokkenen, overdraagbaarheid van gegevens, privacy zelf-management

Persoonsgegevens worden thans veelal op ondoorzichtige wijze, buiten de controle van de betrokkenen verwerkt. Persoonlijke informatiebeheersystemen (PIMS) willen betrokkenen technologische toepassingen aanreiken, die hun meer controle geven over de verwerking van hun persoonsgegevens. PIMS presenteren zich als alternatief voor de huidige, 'gecentraliseerde' wijze van gegevensverwerking, waarbij (grote) organisaties persoonsgegevens op meestal ondoorzichtige wijze verzamelen, analyseren en doorgeven aan derden. PIMS bieden betrokkenen technische instrumenten waarmee zij zelf kunnen controleren en bepalen wanneer en aan wie zijn hun gegevens overdragen, en/of analyses over hun gegevens kunnen laten uitvoeren. Hoewel argumenten voor deze 'decentralisatie' aantrekkelijk klinken, rijzen vragen over de mate waarin PIMS de problemen met de huidige gegevensverwerking effectief kunnen bestrijden. In dit artikel ligt de focus bij de vraag in hoeverre deze PIMS de machtsongelijkheid tussen betrokkenen en grote organisaties daadwerkelijk kunnen bestrijden, die als gevolg van de huidige gegevensverwerkingspraktijk zijn ontstaan. PIMS kunnen enig inzicht in en controle over gegevensverwerking bieden, maar desondanks zal de machtsongelijkheid grotendeels blijven voortbestaan.

1 Inleiding[1]

De wijze waarop en de omvang waarmee private organisaties data, inclusief persoonsgegevens, verzamelen, analyseren en (verder) overdragen geeft aanleiding tot groeiende zorgen.[2] Zo verzamelt Google persoonsgegevens teneinde adverteerders gerichte advertenties te kunnen laten aanbieden of om resultaten van diens zoekmachine met behulp van algoritmen te kunnen afstemmen op de zoeker, terwijl Facebook persoonsgegevens benut om online kijkgedrag te analyseren, en met behulp van algoritmen te bepalen wie welke berichtgeving ontvangt.[3] Met de huidige dataverwerking heerst bij veel betrokkenen ontevredenheid over het gebrek aan transparantie en controle, over de naleving van individuele rechten, en meer algemeen, over wie de vruchten van de gegevensverwerking plukt.[4] Veel organisaties leggen grote hoeveelheden gegevens van individuen vast die zij vervolgens voor verschillende publieke of private doeleinden gebruiken, op een manier die vaak ondoorzichtig is voor degenen op wie de gegevens betrekking hebben. Dit gebrek aan transparantie over de verwerking heeft ertoe geleid dat toestemming en andere wettelijke waarborgen in de AVG voor de veilige en verantwoorde verwerking van persoonsgegevens vaak als ondoeltreffend worden beschouwd.[5]

Privacy Enhancing Technologies (PET's) zijn technologieën die bedoeld zijn om privacyproblemen aan te

* Heleen Janssen is postdoctoraal onderzoeker bij de Blockchain Policy & Society onderzoeksgroep, Instituut voor Informatierecht, Universiteit van Amsterdam en de Compliant & Accountable Systems research group, Department of Computer Science & Technology, Universiteit van Cambridge (Verenigd Koninkrijk).

1 Deze bijdrage is deels gebaseerd op een eerder artikel van de auteur (H. Janssen, J. Cobbe & J. Singh, 'Personal Information Management Systems: a user-centric utopia?', *Internet Policy Review* (9) 2020, afl. 4, p. 1-25).

2 Een voorbeeld van een zorgwekkende omgang met een verzameling persoonsgegevens door Facebook kwam naar voren in de kwestie 'Cambridge Analytica', C. Cadwalladr & E. Graham-Harrison, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach', *The Guardian* 17 maart 2018, theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election, bezocht 9 september 2021.

3 Zie over Google, YouTube, Amazon en Facebook J. Cobbe & J. Singh, 'Regulating Recommending: Motivations, Considerations, and Principles', *European Journal of Law and Technology* (10) 2019, afl. 3.

4 *Gutachten der deutschen Datenethik Kommission,* Duitse Commissie voor gegevensethiek 2019; T. Hartman, H. Kennedy & R. Steedman, 'Public perceptions of good data management: Findings from a UK-based survey', *Big Data & Society* 2021 (januari-juni), p. 1-16.

5 P. Blume, 'The inherent contradictions in data protection law', *International Data Privacy Law* (2) 2012, afl. 1, p. 26-34; F.H. Cate & V. Mayer-Schönberger, 'Notice and consent in a world of Big data', *International Data Privacy Law* (3) 2013, afl. 2, p. 67-73; P. Tolmie e.a., 'This has to be the cats – personal data legibility in networked sensing systems', in: *Proceedings of the 19th ACM Conference on Computer Supported Cooperative Work* (februari 2016) San Francisco; Duitse Commissie voor gegevensethiek (noot 4).

pakken.[6] *Persoonlijke informatiebeheersystemen* (hierna PIMS) vertegenwoordigen een type PET, primair gericht op gegevensbeheer door betrokkenen. PIMS bieden de gebruiker (de betrokkene) een technisch systeem – veelal een virtueel of fysiek apparaat – voor het beheren van diens (persoons)gegevens.[7] PIMS verschaffen de gebruiker daarnaast technische middelen voor het nemen van besluiten over, en het bewaken en controleren van: (i) de gegevens die worden verzameld, vastgelegd, opgeslagen, doorgegeven, of die anderszins worden beheerd in hun PIMS; (ii) de analyses die over die gegevens plaatsvinden; en (iii) hoe en wanneer de gegevens, inclusief de resultaten van de analyses, worden overgedragen (bijv. buiten de PIMS, met derden).

Aanbieders van PIMS stellen dat ze gebruikers in staat stellen controle uit te oefenen over hun eigen persoonsgegevens.[8] Zij baseren dit op het feit dat PIMS gebruikers technische mechanismen bieden om te beslissen wat er met hun gegevens moet gebeuren; derden kunnen de PIMS niet openen, en dus geen gegevens ontvangen of analyseren, zonder dat daar enige gebruikersovereenkomst of interactie met de gebruiker aan is voorafgegaan. Andere voordelen die vaak worden genoemd zijn dat privacy beter wordt beschermd, en dat gebruikers hun gegevens kunnen inzetten voor financiële transacties, of het verwerven van inzichten uit hun eigen gegevens (zie nader par. 2.4).

Meer algemeen pogen PIMS een alternatief te bieden voor de huidige gegevensverwerkingspraktijk waarin organisaties gegevens van veel individuen verzamelen, opslaan en/of gebruiken. Omdat dit vaak gebeurt binnen de technische infrastructuur van één organisatie is de ruimte voor individuen beperkt om te controleren wat er met hun gegevens gebeurt. Hoewel de AVG de rechten van individuen heeft verstevigd, blijkt uit de praktijk nog niet dat deze rechten de transparantie en controle over de gegevensverwerking effectief vergroten.[9] De visie van veel aanbieders van PIMS (platforms, par. 2.2) is niet zozeer gericht op het verder versterken van deze rechten, maar om de gegevensverwerking zelf te 'decentraliseren', door deze weg te halen bij de organisaties, en de verwerking onder de controle van de gebruiker te brengen. Deze decentralisatie van de verwerking zou, volgens diverse platforms, als belangrijk voordeel hebben dat met de verschuiving van de beslissingsmacht over de data naar de gebruiker, de gebruikerscontrole wordt versterkt ten koste van de beslissingsmacht van de organisaties (par. 2.4).

De technologie achter PIMS staat nog in de kinderschoenen. Aanbieders van PIMS die zich momenteel in verschillende stadia van ontwikkeling en beschikbaarheid bevinden, zijn onder meer MyData,[10] Dataswift,[11] Mydex,[12] CitizenMe,[13] Databox[14] en Inrupt/Solid[15] (de Inrupt staat onder leiding van www-uitvinder Sir Tim Berners-Lee). Als ontluikende technologie trekken PIMS aandacht bij diverse onderzoeksgebieden, bij beleidsmakers en bij de industrie.[16] Wetenschappers denken bijvoorbeeld na over hoe PIMS kunnen bijdragen aan betere bescherming van persoonsgegevens, aan meer transparantie, of aan het versterken van de accountability over de dataverwerking[17], of aan rechtsonzekerheid binnen PIMS rondom de toewijzing van rollen en verantwoordelijkheden.[18]

In deze bijdrage wordt vanuit een bredere invalshoek naar PIMS gekeken, en wordt de vraag gesteld in hoeverre PIMS gebruikers daadwerkelijk meer controle kunnen geven, en zorgen over ondoorzichtige dataverwerking kunnen worden weggenomen die inherent zijn aan de huidige gegevensverwerkingspraktijk binnen veel (grote) organisaties. Daartoe wordt in paragraaf 2 een overzicht gegeven van de werking van de technologie, en worden vaak genoemde voordelen van PIMS belicht. In paragraaf 3 wordt onderzocht hoe de grote machtsongelijkheid tussen individuen en groepen enerzijds en grote organisaties anderzijds grotendeels onberoerd blijven door PIMS. Concluderende opmerkingen worden in paragraaf 4 gemaakt.

2 Hoe werkt een PIMS?

Persoonlijke PIMS werken met gegevensbeheertechnologieën die de controle over het verzamelen, het vastleggen, het analyseren en de doorgifte van gegevens letterlijk in handen van het individu willen leggen. Meer concreet krijgt een gebruiker een eigen PIMS om zijn

6 The Royal Society, *Protecting privacy in practice: The current use, development and limits of Privacy Enhancing Technologies in data analysis*, Londen: The Royal Society 2019.
7 Zie bijvoorbeeld de Persoonlijke gezondheidsomgeving (PGO), medmij.nl/wat-is-medmij/ of QiY, qiyfoundation.org/qiy-scheme/qiy-scheme-rulebook/, bezocht 9 september 2021.
8 A. Crabtree e.a., 'Building Accountability into the Internet of Things: The IoT Databox Model', *Journal of Reliable Intelligent Environments* 2018, afl. 4, p. 39-55.
9 L. Edwards, 'Data Protection: Enter the General Data Protection Regulation', in: L. Edwards (red.), *Law, Policy and the Internet,* Oxford: Hart Publishing 2018.
10 mydata.org.
11 dataswift.io.
12 mydex.org.
13 citizenme.com.
14 haddadi.github.io/papers/CAN2016Databox.pdf.
15 inrupt.com.
16 *A European strategy for Data*, Europese Commissie, Brussel 19 februari 2020, COM(2020)66 def.
17 Crabtree e.a. (noot 8); L. Urquhart, T. Lodge & A. Crabtree, 'Demonstrably doing accountability in the Internet of Things', *InternationalJournal of Law and Information Technology* (27) 2019, afl. 1, p. 1-27.
18 H. Janssen e.a., 'Decentralised Data Processing: Personal Data Stores and the GDPR', *International Data Privacy Law* (10) 2020, afl. 4, p. 356-384; J. Chen e.a., 'Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption', *International Data Privacy Law* (10) 2020, afl. 4, p. 1-15.

gegevens te beheren. In de PIMS worden persoonsgegevens verzameld, opgeslagen, en/of overgedragen aan derden. Binnen de PIMS vinden ook de analyses plaats (tenzij de gebruiker anders besluit). Sommige PIMS zijn volledig virtueel, dat wil zeggen gehost in een cloud,[19] terwijl andere PIMS erop gericht zijn specifieke fysieke apparatuur aan te bieden.[20]

2.1 *Technische aspecten*

De aanbieders van PIMS, ofwel platforms, stellen gebruikers in staat controle over de verwerking van persoonsgegevens uit te oefenen via hun PIMS. Hoewel het aanbod en de precieze details variëren, bieden PIMS over het algemeen technische functionaliteit voor:

1. Lokale vergaring, vastlegging en opslag, binnen de PIMS, van gebruikersgegevens. Vaak bieden ze ook mechanismen waarmee gebruikers hun PIMS kunnen vullen met gegevens uit verschillende bronnen, zoals van hun telefoons, wearables, onlinediensten, handmatige gegevensinvoer, camera's, sensoren, etc.
2. Uitvoering van lokale analyses met behulp van software in de PIMS. Het mogelijk maken van analyses binnen de PIMS brengt over het algemeen enige verwerking van persoonsgegevens met zich mee.
3. Gegevensoverdracht met behulp van de PIMS. Deze functionaliteit moet gebruikers controle bieden over de gegevens die moeten worden overgedragen naar externen. De over te dragen gegevens kunnen zowel 'ruwe' gebruikersgegevens, als resultaten van analyses, alsook andere externe interacties (bijv. gebruikersoproepen naar externe services zoals zoekmachines) betreffen.
4. Transparantie en maatregelen ter ondersteuning van de gebruikerscontrole, zoals technische middelen voor het monitoren, configureren en beheren van de bovenstaande functionaliteiten. Dit omvat beheersmaatregelen voor gebruikers om voorkeuren en beperkingen in de PIMS in te stellen met betrekking tot het vastleggen, overbrengen en verwerken van gegevens; het visualiseren en alerteren van specifieke gebeurtenissen binnen de PIMS, etc.

De technische omgeving (infrastructuur) van de PIMS omvat ook het beheer van de beveiligingsaspecten, zoals gegevensversleuteling, het beheren en controleren van gebruikerstoegang tot de PIMS en de gegevens daarin, en het verstrekken van middelen voor het separaat isoleren van de ruwe gebruikersgegevens en de analyses (gebaseerd op de ruwe gegevens). Verder wordt de PIMS zodanig ingesteld dat alle regels, voorkeuren en beperkingen die de gebruiker wenst, daadwerkelijk worden nageleefd (zie (4)). Als een gebruiker bijvoorbeeld specificeert dat bepaalde gegevens niet mogen worden overgedragen aan een partij, of niet mogen worden opgenomen in een analyse, zal de technische omgeving van de PIMS ervoor zorgen dat deze beperkingen worden gerespecteerd.

PIMS bevatten vaak technische mechanismen die belemmeren dat organisaties die gebruikersgegevens verwerken, rechtstreeks toegang krijgen tot de ruwe persoonsgegevens van de gebruiker die zich in een PIMS bevinden.[21] In plaats daarvan maken dergelijke mechanismen het mogelijk om de gewenste berekening, analyse of andere verwerking naar de gegevens van de gebruiker te brengen die zich in het PIMS apparaat bevinden, waarna dan enkel de resultaten van die verwerking worden naar de organisatie worden gestuurd.[22]
Dit wordt ook wel gedecentraliseerde gegevensverwerking genoemd: de analyses vinden niet plaats in het technisch systeem van de organisatie, maar in de PIMS van gebruikers. Dit gebeurt (net als bij andere vormen van verwerking) in overeenstemming met een gebruikersovereenkomst, en alleen voor bepaalde gegevens zoals aangewezen door de gebruiker. Op de (beweerdelijke) voordelen van deze benadering voor organisaties wordt nader ingegaan in par. 2.5.

Wanneer de gegevens zich eenmaal binnen de PIMS bevinden, worden analyses daarover verricht met behulp van een *app*. Een app bevat de software die de analyse uitvoert op de gebruikersgegevens. Apps worden doorgaans aangeboden door ontwikkelaars, bedrijven en andere organisaties, zoals we die ook kennen van onze mobiele apparaten. Het verschil met de huidige mobiele apparatuur is echter dat apps de analyses *in* de technische omgeving van de PIMS uitvoeren, terwijl de analyses die nu via apps op onze mobiele apparaten verlopen, worden uitgevoerd in de technische omgeving van het betreffende bedrijf of organisatie – op een locatie en met een procedure die vaak volledig zijn onttrokken aan het overzicht en de controle van de gebruiker.

Apps brengen vaak (enkele) persoonsgegevens die zich in de PIMS bevinden, buiten de PIMS. Dat is bijvoorbeeld het geval wanneer de resultaten van data-analyses worden overgedragen aan de app-ontwikkelaar. Platforms (ofwel aanbieders van PIMS) stellen dat een dergelijke functionaliteit van groot belang is voor organisaties, met het argument dat het ontvangen van enkel de *resultaten* van de analyses de risico's met het overdragen van persoonsgegevens tot een minimum worden beperkt, en dat gevoeligheden, overheadkosten en weerstand worden vermeden die vaak gepaard gaan met het beheren van gedetailleerde en specifieke persoonsgegevens van gebruikers (zie par. 2.5).

Gelet op het waarborgen van de controle door de gebruiker is het van groot belang dat apps, die de analyses

19 digi.me.
20 Databox (noot 14).
21 Crabtree e.a. (noot 8).
22 Janssen e.a. (noot 1).

binnen de PIMS in opdracht van de gebruiker uitvoeren, door het platform worden beperkt in wat zij mogen doen met gebruikersgegevens. Dat betekent dat niet willekeurig elke organisatie kan aansluiten op een PIMS. App-ontwikkelaars zullen veelal voorafgaand aan de toelating tot het PIMS-ecosysteem in zogenoemde app-notificaties expliciet moeten maken welke gegevensbronnen ze willen gebruiken voor de analyses, welke gegevens ze precies willen overdragen (enkel resultaten van analyses, of ook ruwe gebruikersdata), etc. Gebruikers kunnen zelf vaak ook andere beperkingen opleggen, bijvoorbeeld met betrekking tot de gegevens waartoe apps toegang kunnen verkrijgen, die apps kunnen verwerken, en/of mogen overdragen. De technische infrastructuur van de PIMS zorgt er vervolgens voor dat aan deze beperkingen daadwerkelijk wordt voldaan. Naast deze technische specificaties bestaan rondom de PIMS ook juridische mechanismen (dienstverleningsvoorwaarden) om het gedrag en de werking van apps te beheren (par. 2.3).

2.2 *Een ecosysteem met meerdere actoren*

Binnen het 'ecosysteem' van de PIMS zijn diverse actoren betrokken. De meest relevante voor onze discussie zijn gebruikers, app-ontwikkelaars, en het platform dat de PIMS aanbiedt. Hoewel de focus in dit artikel ligt op gebruikers worden ook de andere actoren geïntroduceerd omdat het gaat over gebruikerscontrole over data en beslismacht.

Gebruikers zijn betrokkenen in de zin van artikel 4(1) AVG die een PIMS bezitten, en gebruikmaken van de functionaliteiten in die PIMS om hun gegevens te beheren. App-ontwikkelaars zijn diegenen die geïnteresseerd zijn in het verwerken van gebruikersgegevens. We beschrijven deze organisaties als *app-ontwikkelaars*, omdat ze de apps ontwerpen en bouwen die de gebruikersgegevens verwerken in de PIMS. Apps dragen vaak resultaten van de door de app uitgevoerde analyses over naar de organisatie die achter de app schuilgaat. Als de gebruiker dat wenst, kan de app ook ruwe gebruikersgegevens overdragen naar de organisatie. Daarnaast kunnen PIMS ook de overdracht van gegevens naar een organisatie, dus zonder betrokkenheid van een specifieke app, ondersteunen. Dit proces wordt beheerd via de mechanismen voor directe gegevensoverdracht die worden geleverd door de PIMS (dat zelf een soort app kan zijn die bij de PIMS wordt geleverd).

Platforms zijn de organisaties die de PIMS leveren, en/of het ecosysteem rondom de PIMS beheren (zoals de beveiliging van en het verzorgen van updates voor de PIMS). Het aanbod van typen PIMS en diensten is op dit moment divers. Sommige platforms bieden (doorgaans ervaren) gebruikers enkel de codebasis om de werking van hun PIMS te 'compileren', en deze zelf te beheren. Andere leveren een volledige operationele infrastructuur – inclusief een fysieke PIMS, een clouddienst voor dataopslag, etc.[23] Sommige platforms overwegen ook 'appstores' of 'datamarktplaatsen' te hosten, die bemiddelen tussen de gebruiker en de organisaties die hun gegevens willen verwerken. Andere platforms stellen uitdrukkelijk de naleving van *best practices* voorop, waarbij het platforms de voorwaarden definieert waaronder app-ontwikkelaars toegang kunnen krijgen tot gebruikersgegevens, of sluiten overeenkomsten met gebruikers en de organisaties achter de app-ontwikkelaars. Op deze manier variëren platforms in hun mate van betrokkenheid bij de werking van het ecosysteem rondom de PIMS.

2.3 *Juridische aspecten*

Naast technische aspecten brengen veel platforms ook juridische regulering met zich mee. Deze zorgen ervoor dat het 'gedrag' van de app, en het datagebruik meer in het algemeen, in overeenstemming is met gebruikersvoorkeuren en de vereisten die het platform stelt. Sommige hiervan zijn neergelegd in de servicevoorwaarden van een platform. Deze definiëren hoe het platform kan worden gebruikt, en reguleren de toewijzing van verantwoordelijkheden en aansprakelijkheden. Platformservicevoorwaarden vereisen vaak dat app-ontwikkelaars passende maatregelen nemen om gebruikers te beschermen tegen onrechtmatige verwerking[24] en om gebruikers te beschermen tegen onopzettelijk verlies of vernietiging van gegevens, terwijl ze gebruikers kunnen verplichten om hun wachtwoorden of om hun PIMS regelmatig te *updaten* voor veiligheidsdoeleinden.[25]

Platforms kunnen ook contracten sluiten met app-ontwikkelaars; deze bevatten vaak bedrijfsspecifieke voorwaarden, die de interacties met en verwerking van gebruikersgegevens, de functionaliteit van hun apps etc. nader regelen. Servicevoorwaarden en contracten kunnen bijvoorbeeld bepalen dat app-ontwikkelaars volledig moeten voldoen aan het beleid van het platform en zijn principes met betrekking tot de verwerking van gebruikersgegevens. Wanneer dit wordt nagelaten, kan het contract of de servicevoorwaarden bepalen dat het platform zijn gegevensverwerkingsactiviteiten met de app-ontwikkelaar beëindigt.[26]

2.4 *Geclaimde gebruikersvoordelen*

Platforms zeggen dat zij gebruikers functionaliteiten bieden, meer specifiek dat zij hen met de PIMS controle en transparantie inzake de verwerking van hun

23 Janssen e.a. (noot 18).
24 Dataswift (noot 11).
25 Dataswift (noot 11).
26 Mydex (noot 12).

persoonsgegevens bieden. Voordelen voor gebruikers omvatten onder meer het navolgende:

- Gebruikers hebben gedetailleerde controle over de gegevens die over hen worden vastgelegd, en inzicht in hoe die gegevens worden overgedragen en gebruikt.[27]
- Gebruikers genieten betere bescherming van persoonsgegevens (inclusief 'gevoelige' persoonsgegevens) tegen toegang door derden, door middel van de geboden technische functionaliteit.[28]
- PIMS leiden tot werkelijk geïnformeerde toestemming van de gebruiker, omdat PIMS meer informatie geven over de gegevensverwerking door de app-ontwikkelaar. Dit kan worden verwerkelijkt door middel van bijvoorbeeld de bewakingsfunctionaliteit van de PIMS; door de specificaties van het datagebruik van de app; door platformfuncties, zoals appstores die het gebruik van appgegevens rangschikken en beschrijven, en/of PIMS die *good practices* op het gebied van transparantie vereisen.[29]
- PIMS kennen een gecompartimenteerde gegevensopslag en analyses om te voorkomen dat apps ongepast, onbedoeld en zonder gebruikersovereenkomst in aanraking komen met gegevens (en andere apps).[30]
- PIMS bieden gebruikers mogelijkheden om meer inzichten uit hun data te halen.[31]
- PIMS staan gebruikers toe transacties uit te voeren of geld te verdienen met hun persoonlijke gegevens.[32]
- PIMS stimuleren ontwikkelaars over het algemeen tot meer privacyvriendelijke benaderingen.[33]

PIMS hebben ook de aandacht getrokken van beleidsmakers. De Europese Commissie verklaarde in haar Datastrategie dat PIMS en soortgelijke hulpmiddelen een aanzienlijk potentieel hebben, omdat ze gebruikers de instrumenten (veelal gericht op toestemmingsbeheer, toepassing voor het beheer van persoonlijke informatie) en mogelijkheden bieden om op detailniveau te beslissen wat met hun gegevens gebeurt.[34]

2.5 *Geclaimde voordelen voor app-ontwikkelaars (en organisaties)*

Volgens PIMS-platforms en -ontwikkelaars is de aantrekkingskracht van PIMS voor app-ontwikkelaars gelegen in de belofte van toegang tot meer gebruikersgegevens – in termen van volume, rijkdom, snelheid en variëteit. Omdat PIMS een grote verscheidenheid aan gebruikersinformatie kunnen verzamelen, kunnen gebruikers app-ontwikkelaars toegang bieden tot een breder scala aan gegevenstypen, dan wanneer ze zouden proberen de gegevens direct bij de gebruiker te verzamelen.[35] Diverse platforms stellen dan ook dat wanneer gebruikers eenmaal begrijpen hoe hun gegevens worden verwerkt, en zij zich door de controlemechanismen van de PIMS gesterkt voelen, zij minder weerstand ervaren tegen het gebruik van hun data, en een grotere bereidheid zouden tonen over te gaan tot (beheerde) gegevensuitwisseling en -verwerking.[36]

Hoewel PIMS doorgaans de voordelen voor individuele gebruikers uitlichten, zijn de meeste platforms (en organisaties) met name geïnteresseerd in het ondersteunen van 'collectieve' analyses, waarbij de verwerking van gegevens van veel gebruikers of van (bepaalde) populaties mogelijk wordt gemaakt, via apps die op hun PIMS zijn geïnstalleerd.[37] Collectieve analyses brengen vaak gebruikers- of groepsprofilering met zich mee met het oog op het ondersteunen van verschillende organisatorische doelen, zoals klantinzicht, marktonderzoek, details van productgebruik, of inderdaad, en zoals gebruikelijk is in online-diensten, om een op surveillance gebaseerd advertentieverdienmodel te ondersteunen (zie hieronder, par. 2.6). Op deze manier bieden de platforms in feite een architectuur voor de verwerking van gebruikersgegevens die op grote schaal in een populatie kan doorwerken. Dit is aantrekkelijk voor organisaties, omdat de platforms met een groot gebruikersbestand toegang kunnen bieden tot een grotere populatie, en dus tot meer gegevens dan wanneer de organisatie van elke individuele gebruiker data zou moeten opvragen.

Belangrijk argument voor organisaties om apps op PIMS te laten installeren is daarnaast dat gedecentraliseerde opslag en verwerking van data veelal ook gepaard gaat zonder de voor organisaties gebruikelijke kosten, risico's en overheadkosten, die verbonden zijn aan de naleving met het verzamelen, opslaan en beheren van gegevens.[38]

---

27 Article 29 Data Protection Working Party, *Opinion 8/2014 on Recent Developments on the Internet of Things*, WP 223 16 september 2014; Crabtree e.a. (noot 8); Urquhart e.a. (noot 17).
28 Crabtree e.a. (noot 8); T. Lodge & A. Crabtree, 'Developing GDPR compliant apps for the edge', in: *Proceedings of the 13th International Workshop on Data Privacy Management,* Barcelona: Springer 2018, p. 313-328.
29 MyData (noot 10).
30 Crabtree e.a. (noot 8).
31 Mydex (noot 12); MyData (noot 10).
32 I. Ng & H. Haddadi, 'Decentralised AI has the potential to upend the online economy', *Wired* 28 december 2018; Dataswift (noot 11).
33 Crabtree e.a. (noot 8).
34 Europese Commissie (noot 16).
35 MyData (noot 10).
36 Dataswift (noot 11); MyData (noot 10); Digi.me (noot 19); CitizenMe (noot 13) vermelden dit in hun beschrijvingen.
37 MyData (noot 10); Databox (noot 14); CitizenMe (noot 13); Digi.me (noot 19).
38 Crabtree e.a. (noot 8), N. Anciaux e.a., 'Personal Data Management Systems: The security and functionality standpoint', *Information Systems* 2019, afl. 21, p. 21-35.

2.6 *Commerciële perspectieven voor PIMS*

Sommigen voorspellen dat PIMS aanzienlijke economische voordelen kunnen opleveren voor zowel bedrijven als consumenten.[39] De verdienmodellen van platforms voor PIMS zijn echter nog in ontwikkeling.[40] Er is een reeks mogelijke inkomstenstromen ontwikkeld en voorgesteld, waaronder:

- Platforms die organisaties kosten in rekening brengen voor toegang tot het PIMS-ecosysteem (bijv. jaarlijkse vergoeding,[41] kosten voor toegang tot de appstore van het platform, per download van hun app door een gebruiker, enz.);
- Platforms die organisaties kosten in rekening brengen per 'gegevenstransactie' met een PIMS, waarbij het type transactie (toegang, berekening en/of overdracht van gegevens, inclusief ruwe data)[42] en/of het type gegevens dat wordt opgevraagd (bijv. zoekvragen, gedragsgegevens) de prijs veelal bepalen;[43]
- Organisaties die inkomsten delen met het platform via in-app aankopen door gebruikers;[44]
- Platforms die organisaties kosten in rekening brengen voor ondersteunende diensten;[45]
- Gebruikers die het platform een abonnementsgeld betalen, of betalen voor het ontgrendelen van extra functionaliteit in de PIMS;[46]
- Platforms die PIMS verkopen, huren of leasen aan gebruikers, waaronder service- of onderhoudscontracten;[47] of
- Platforms in het algemeen belang (bijv. een platform dat de volksgezondheid dient) kunnen 'gratis' zijn, gefinancierd via bijvoorbeeld donaties en publieke fondsen.[48]

Omdat PIMS nog in ontwikkeling zijn, zijn de verdienmodellen van veel platforms nog onzeker. Verwacht wordt dat platforms een reeks mechanismen en verdienmodellen voor het genereren van inkomsten zullen gebruiken.

3 Gegevensbescherming

Een belangrijk doel van PIMS is gebruikers meer zichtbaarheid en controle geven over de verwerking van hun persoonsgegevens. PIMS verwerken daarmee persoonsgegevens, hetgeen betekent dat de Algemene Verordening Gegevensbescherming (AVG) van toepassing is. Deze kent drie belangrijke rollen en daarbij behorende verantwoordelijkheden: verwerkingsverantwoordelijken (alleen handelend of samen met anderen als gezamenlijke verwerkingsverantwoordelijken (art. 4(7), 26 AVG); verwerkers (inclusief subverwerkers, art. 4(8), 28(4) AVG), en betrokkenen (art. 4(1) AVG). De rol van een bepaalde actor als verwerkingsverantwoordelijke of verwerker is over het algemeen een kwestie van de feitelijke invloed van een actor op de gegevensverwerking. De wijze waarop een actor zijn of haar rol beschrijft (bijvoorbeeld in een contract) kan indicatief zijn, maar hoeft niet altijd definitief te zijn.[49]

De AVG belast zowel verwerkingsverantwoordelijken als verwerkers met een reeks verantwoordelijkheden en verplichtingen, waarvan het grootste deel op de verwerkingsverantwoordelijken rust, gezien hun rol bij het bepalen van de aard van de gegevensverwerking. Verplichtingen voor verwerkingsverantwoordelijken zijn onder meer het naleven van de beginselen van gegevensbescherming (art. 5(1) AVG), dat deze naleving aangetoond kan worden is (verantwoordingsplicht ex art. 5(2) AVG), of dat de verwerking van persoonsgegevens is gebaseerd op een rechtmatige grondslag (art. 6(1) AVG). Typische rechten die worden verleend aan betrokkenen waaraan de verwerkingsverantwoordelijken moeten voldoen, omvatten het recht op toegang tot de eigen persoonsgegevens, het recht bezwaar te maken tegen gegevensverwerking, of het recht op gegevenswissing of gegevensoverdracht naar een andere verwerkingsverantwoordelijke.

Hoewel PIMS-technologieën nog in ontwikkeling zijn, bestaan er nog onopgeloste problemen op het gebied van gegevensbescherming. De toewijzing van rollen en verantwoordelijkheden in PIMS-ecosystemen is complex, omdat deze veelal worden gekenmerkt door een gelaagde en veelal complexe samenwerking van meerdere partijen, waaronder de hier genoemde gebruikers, platforms en app-ontwikkelaars (en hun organisaties). Deze realiteit is soms lastig te verenigen met de benadering in de AVG met verwerkingsverantwoordelijken waarvan veelal wordt verondersteld dat zij het gehele gegevensverwerkingsproces in het ecosysteem 'orkestreren'.[50] In de praktijk kan het ecosysteem van een PIMS verschillende vormen aannemen, en is de rechtspositie van betrokkenen veelal afhankelijk van de specifieke omstandigheden in de PIMS context. Onopgeloste kwesties met betrekking

39 Control-Shift, *Personal Information Management Services – An analysis of an emerging market: Unleashing the power of trust,* rapport 2014; G. Brochot e.a., 'Personal Data Stores (report 2015). Study for the European Commission (DGCNECT)', Europese Commissie 2015 (noot 16).
40 I. Bolychevsky & S. Worthington, 'Are Personal Data Stores about to become the NEXT BIG THING?', medium.com 8 oktober 2018.
41 Mydex (noot 12).
42 Digi.me (noot 19).
43 CitizenMe (noot 13).
44 Digi.me (noot 19).
45 Mydex (noot 12).
46 Digi.me (noot 19).
47 Crabtree e.a. (noot 13).
48 BBC-Box, bbc.co.uk/rd/blog/2019-06-bbc-box-personal-data-privacy, bezocht 18 juni 2021.
49 Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of controller and processor*, WP169 16 februari 2010 en EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, 2 september 2020.
50 Janssen e.a. (noot 18).

tot de rollen en verantwoordelijkheden onder de AVG in verschillende PIMS-contexten werden recentelijk in detail onderzocht.[51]

In dit deel van het artikel staan we stil bij twee belangrijke overwegingen op het gebied van gegevensbescherming met betrekking tot de 'gebruiker': de wijze waarop PIMS, die gericht zijn op toestemming, verband houden met de wettelijke grondslagen voor de verwerking in de AVG; en de relatie tussen PIMS en rechten van betrokkenen.

3.1 *Grondslagen voor rechtmatige verwerking*

De AVG vereist dat elke verwerking van persoonsgegevens is gebaseerd op een van de wettelijke grondslagen zoals vastgelegd in art. 6(1) AVG. Verwerkingsverantwoordelijken moeten bepalen welke rechtsgrond in een bepaalde situatie het meest geschikt is, afhankelijk van de specifieke doeleinden en de context voor het gebruik, de aard van de betrokken partijen, en hun motivaties en relaties, en de vereisten voor de rechtsgrond waarop zij zich beroepen.

Wanneer een PIMS een *fysiek* apparaat betreft, is in het algemeen de ePrivacyrichtlijn van toepassing. Dit betekent dat in het algemeen steeds toestemming van de gebruiker vereist zal zijn voor app-ontwikkelaars om gegevens te verwerken (art. 5(3) ePrivacyrichtlijn).[52] In deze context is toestemming de enige beschikbare grondslag voor verwerking (art. 6(1)(a) & 7 AVG; Overwegingen 32, 42, 43 AVG) en expliciete toestemming bij de verwerking van bijzondere persoonsgegevens (art. 9, lid 1, en Overwegingen 51-56 AVG). Voor 'virtuele' PIMS (momenteel de meest voorkomende PIMS) zijn ook de andere verwerkingsgronden beschikbaar (tenzij het bijzondere persoonsgegevens betreft, dan resteert enkel expliciete toestemming).

PIMS zijn van nature gericht op het ondersteunen van (gebruikers)toestemming en contract (waar de verwerking noodzakelijk is voor de uitvoering van een contract waarbij de gebruiker partij is). PIMS-platforms zijn over het algemeen expliciet ontworpen om dit te ondersteunen; zij vereisen veelal een actieve gebruikersovereenkomst met betrekking tot gegevensverwerking.[53] Waar voor de andere verwerkingsgronden een passieve houding van de betrokkene doorgaans voldoende is, verplichten PIMS de gebruiker tot het ondernemen van actie, door bijvoorbeeld akkoord te gaan met de voorwaarden bij het installeren van de app, door het configureren van voorkeuren en beleid voor gegevensgebruik, zodat de verwerking kan plaatsvinden.

Er zijn ook rechtmatige gronden voor verwerking, zoals de wettelijke verplichting, het openbaar belang of gerechtvaardigd belang, waarbij de verwerkingsverantwoordelijken – niet de betrokkenen (gebruikers) – beslissen of verwerking kan plaatsvinden. De toestemming van de gebruiker is niet vereist voor bepaalde openbare taken (bijvoorbeeld bij belastingheffing), of voor legitieme belangen van de verwerkingsverantwoordelijke (bijvoorbeeld voor de verwerking van bepaalde gegevens om fraude op te sporen).

De vereisten verschillen per rechtsgrond en kunnen (afhankelijk van de grond) overwegingen omvatten zoals de noodzaak van die verwerking (art. 6(1)(b)-(f) AVG), dat de belangen van de verwerkingsverantwoordelijke in evenwicht zijn met de grondrechten van de betrokkene (art. 6(1)(f) AVG[54]), en een stichting in verenigbare lidstaatwetgeving (art. 6(1)(c) en (e) AVG). Deze gronden voor verwerking, die niet gebaseerd zijn op specifieke en actieve gebruikersbetrokkenheid of overeenkomst, worden zelden overwogen in PDS-architecturen, en op dit moment is het onduidelijk hoe PIMS-ontwerpen deze gronden zouden kunnen ondersteunen waar ze van toepassing zijn.[55]

3.2 *Rechten van betrokkenen*

De AVG kent betrokkenen verschillende rechten toe met betrekking tot de verwerking van hun persoonsgegevens.[56] De verwerkingsverantwoordelijken zijn belast met het nakomen van deze rechten. De rechten van betrokkenen zijn niet absoluut – de AVG stelt voorwaarden aan de uitoefening van sommige rechten, en niet alle rechten zijn in elke situatie van toepassing.

Rechten van betrokkenen hebben nog weinig aandacht gekregen in een PIMS-context. Met het oog op verbetering van transparantie van de verwerkingen bieden PIMS gebruikers wel enig inzicht in wat er in de PIMS gebeurt, en informeren ze gebruikers over de gegevensuitwisselingen apparaat met organisaties.[57] Ze bieden gebruikers vaak ook bedieningselementen om de verwerking op een PIMS te beheren. Als zodanig hebben sommigen gesuggereerd dat PIMS (tenminste voor gegevens binnen het apparaat) tot op zekere hoogte de behoefte van een gebruiker om bepaalde rechten van betrokkenen uit te

51 Janssen e.a. (noot 18).
52 Janssen e.a. (noot 18).
53 Crabtree e.a. (noot 8); Urquhart e.a. (noot 17).
54 I. Kamara & P. De Hert, 'Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: a Pragmatic Approach', *Brussel Privacy Hub* (4) 2018, afl. 12, p. 1- 33.
55 Janssen e.a. (noot 1).
56 Deze omvatten het recht op toegang tot hun persoonsgegevens (art. 15), rectificatie van onjuiste persoonsgegevens (art. 16), wissing (art. 17), het recht bezwaar te maken (art. 21), beperking van verwerking van hun gegevens (art. 18), hun gegevens over te dragen naar een andere verwerkingsverantwoordelijke (art. 20), en om niet te worden onderworpen aan uitsluitend geautomatiseerde besluitvorming of profilering die juridische of vergelijkbare significante effecten heeft (art. 22 AVG).
57 Urquhart e.a. (noot 17).

oefenen overbodig maken,[58] omdat PIMS gebruikers al middelen zouden bieden om zelf bepaalde verwerkingen te beperken en gegevens te wissen, of over te dragen. De huidige PIMS-technologie geeft gebruikers op dit moment alleen bepaalde inzichten. De rechten van betrokkenen zijn echter breder en omvatten meer dan alleen inzicht geven in de gegevensverwerking op het apparaat. Gebruikers zullen bijvoorbeeld belang hebben bij het gedrag van organisaties die bij de verwerking zijn betrokken.

De AVG vereist dat verwerkingsverantwoordelijken rekening houden met gegevensbeschermingsoverwegingen, inclusief die met betrekking tot rechten, in hun technologische en organisatorische processen (*privacy-by-design*, art. 25(1) AVG). Dit heeft niet alleen gevolgen voor app-ontwikkelaars, maar ook voor PIMS-platforms, die gebruikers mechanismen zouden kunnen bieden die hen specifiek en meer algemeen kunnen helpen bij het uitoefenen van hun rechten.

Er kunnen echter vragen rijzen of PIMS-platforms hiertoe wettelijk verplicht zijn, omdat art. 25(1) AVG van toepassing is op verwerkingsverantwoordelijken, terwijl niet altijd duidelijk is wat de rol van een PIMS-platform is in het licht van de AVG.[59] Ongeacht enige wettelijke verplichting zou elk platform ernaar moeten streven gebruikers beter te ondersteunen bij de verwezenlijking van hun gegevensrechten, omdat dit in ook overeenstemming is met het vaak gestelde doel gebruikers meer autonomie over hun persoonsgegevens te geven.

Naast een PIMS-functionaliteit die specifiek gericht is op rechten, zouden transparantiemechanismen in PIMS gebruikers meer in het algemeen kunnen helpen bij het uitoefenen van hun rechten. PIMS kunnen, bijvoorbeeld door informatie te verstrekken over de verwerking zoals eerder genoemd onder (4) gebruikers helpen bij het nader specificeren van hun betrokkenenrechten. Een melding door het platform aan gebruikers dat specifiek toepassingsgedrag van een app-ontwikkelaar blootlegt, kan gebruikers aanmoedigen om hun recht uit te oefenen 'meer te weten te komen', of hen eventueel aansporen na te gaan of hun inzageverzoeken correct zijn uitgevoerd. Dit kan hen helpen bij het bepalen of de verwerking door de app-ontwikkelaar moet worden voortgezet, of bij het nagaan of de door de verwerkingsverantwoordelijke verstrekte informatie overeenkomt met de handelingen die in de PIMS werden waargenomen.

Eén recht dat vaker wordt genoemd door PIMS-platforms en dat hier nader wordt uitgelicht, is het recht op gegevensoverdracht (art. 20 AVG).[60] Dit geeft gebruikers het recht kopieën te ontvangen van de gegevens die zij in elektronische vorm aan een verwerkingsverantwoordelijke hebben verstrekt, en het recht die gegevens over te dragen of te laten overdragen aan een andere verwerkingsverantwoordelijke. Dit kan enkel worden ingeroepen als de verwerking was gebaseerd op toestemming of contract (art. 20(1)(a) AVG), en mag alleen die gegevens betreffen die door betrokkenen zelf zijn verstrekt (art. 20(1) AVG.[61]

Overdraagbaarheid wordt beschouwd als een belangrijk middel voor gebruikers om hun PIMS te 'vullen' omdat zij daarmee hun gegevens uit de databases van organisaties naar de PIMS brengen (art. 20 AVG).[62] Sommige PIMS-platforms beschrijven het recht als een middel voor gebruikers om hun gegevens van organisaties 'terug te vorderen', en overwegen technische mechanismen aan te bieden die gebruikers in staat stellen gebruik te maken van overdraagbaarheidsrechten.[63]

Inzageverzoeken (art. 15, lid 3 AVG) kunnen eveneens helpen bij het vullen van PIMS, met name omdat ze minder beperkt zijn waar het de voorwaarden bij het inroepen van het recht betreft, en doorgaans resulteren in meer informatie dan zou worden ontvangen uit een overdraagbaarheidsverzoek. Voor inzageverzoeken is het echter niet nodig dat de gegevens worden geretourneerd in een machineleesbare vorm, hetgeen het gebruik van de ontvangen gegevens in PIMS kan bemoeilijken. Bij de uitoefening van overdrachtsrechten is levering van informatie in machineleesbare vorm wel vereist. Echter, zonder overeengekomen interoperabiliteitsnormen zal het inzageverzoek (en tot op zekere hoogte zelfs overdraagbaarheidsverzoeken) om PIMS te vullen vaak lastig te realiseren zijn.

4 PIMS lossen bestaande informatie- en machtsongelijkheid niet op

Platforms die PIMS aanbieden stellen vaak dat ze gebruikers zelfbeschikking over hun data geven door hen middelen te bieden voor meer transparantie en controle, waardoor gebruikers betere, en beter geïnformeerde beslissingen kunnen nemen over (het al dan niet beëindigen van) een bepaalde verwerking. Dat is echter gemakkelijker gezegd dan gedaan. De bestaande informatie- en machtsongelijkheden zijn immers systemisch: ze zijn inherent aan de huidige digitale ecosystemen die met de zeer complexe en grotendeels ondoorzichtige aard van gegevensverwerking de ongelijkheid tussen gebruikers en de organisaties die hun gegevens verwerken, verder vergroten.[64] Deze divergenties, die het gevolg zijn

58 Urquhart e.a. (noot 17).
59 Janssen e.a. (noot 18).
60 CitizenMe (noot 13); Dataswift (noot 11); Digi.me (noot 19).
61 Article 29 Data Protection Working Party, *Guidelines on the right to data portability,* WP 242 rev. 01 13 december 2016; Urquhart e.a. (noot 17).
62 Article 29 Working Party (noot 61).
63 CitizenMe (noot 13); Dataswift (noot 11); Digi.me (noot 19).
64 A. Mantelero, 'Social Control, Transparency, and Participation in the Big Data World', *Journal of Internet Law* april 2014, p. 23-29.

van een ongelijke verdeling van toegang tot en het kunnen benutten van begrip, kennis, voorspelling of risicobeoordeling[65] maken het zelfs voor goed geïnformeerde gebruikers moeilijk, zo niet onmogelijk om een verwerking te kunnen beoordelen, en tot werkelijk geïnformeerde beslissingen te komen over de verwerking van hun gegevens.[66]

De ondoorzichtige aard van de huidige gegevensverwerking is grotendeels *systemisch*. Een aantal oorzaken daarvoor ligt bij gebruikers van digitale diensten. Zij hebben vaak geen kennis of begrip van: (1) de praktijken binnen organisaties, die gebruikersgegevens vastleggen en verwerken, met inbegrip van de details, redenen voor en implicaties van het bewaren van bepaalde gegevens, of het uitvoeren van bepaalde analyses; (2) de gebruiken rondom het overdragen van gegevens van die organisaties met derden en daarbuiten; (3) de technische details van de technische systemen; (4) de datagestuurde, vaak surveillancegestuurde verdienmodellen van bedrijven[67] en (5) de inzichten en macht die organisaties kunnen verkrijgen door toegang tot gegevens, met name waar gegevens worden geaggregeerd of analyses op grote schaal plaatsvinden (collectieve analyses, zie par. 2.5).

Diverse rechten dragen eveneens bij aan het in stand houden van systemische informatie- en machtsdivergenties tussen gebruikers en organisaties digitale ecosystemen.[68] Zo kunnen auteursrechten, handelsgeheimen, of eigendom over documenten of databases van grote organisaties zodanig uitwerken dat informatie, die voor het publiek beschikbaar zou kunnen komen, wordt beperkt. Deze beperkingen zijn echter niet absoluut, en gelden ook niet voor iedere belanghebbende. Onder bepaalde voorwaarden kunnen rechters of toezichthouders toegang krijgen tot gegevens met betrekking tot handelsgeheimen of databases die niet algemeen beschikbaar zijn voor het publiek.[69]

Cruciaal is dat PIMS deze ondoorzichtigheden en verwerkingsgewoonten slechts gedeeltelijk kunnen oplossen, en daarmee de systemische aard van de informatieongelijkheden in digitale ecosystemen zeer beperkt doorbreken. Het bieden van een gedecentraliseerde, op de gebruiker gerichte opslag van, toegang tot en controle over gegevens en de verwerking ervan kan gebruikers helpen om enige kennis op te doen van wat er met hun persoonlijke informatie gebeurt, al is dat in beperkte mate. Waar gebruikers mogelijk meer inzicht krijgen in de gegevensverwerking die plaatsvindt in hun PIMS, is het erg onwaarschijnlijk dat PIMS de genoemde systemische problemen zullen oplossen. Het is eerder zo dat PIMS gebaseerd zijn op de verkeerde aanname, namelijk dat met het presenteren van voldoende informatie, op de juiste manier, gebruikers beter in staat zullen zijn om belemmeringen te overwinnen die structureel en systemisch van aard zijn.[70] Dit wordt hierna uitgewerkt.

4.1 *Dataverwerking door organisaties blijft grotendeels ondoorzichtig*

De bedoelingen, motivaties en gedragingen van organisaties zijn zoals hiervoor gesteld niet altijd doorzichtig voor gebruikers.[71] In een poging meer duidelijkheid te geven over de dataverwerking, eisen PIMS dat app-ontwikkelaars informatie verstrekken over hun organisatorische processen en bedoelingen. Dergelijke informatie, die organisaties veelal opnemen in de eerdergenoemde appnotificatie die de werking van de app beschrijft, kan details bevatten over de soorten gegevens die een app zal verwerken; de doeleinden van de app-ontwikkelaar voor die verwerking; de risico's van de app; of aan wie de app-ontwikkelaar gegevens zal overdragen die deze heeft ontvangen vanuit de PIMS.[72] De informatie in dezelfde notificatie zal echter veelal niet verhelderen waarom *die* specifieke gegevens nodig zijn (in tegenstelling tot andere, misschien minder gevoelige gegevens), waarom *deze* gewichten worden toegekend aan bepaalde gegevens in het analyseproces, en, meer in het algemeen, waarom *die* specifieke gegevensverwerking moet plaatsvinden, en welke mogelijke implicaties voor gegevensbescherming hieraan kleven.

Hierna wordt dieper ingegaan op hoe de ondoorzichtige dataverwerking door organisaties die transparantie en gebruikerscontrole over data in de PIMS veelal belemmeren. Deze belemmeringen vinden hun oorsprong in: (i) het gebrek aan beschikbare informatie over gegevens die buiten de grenzen van de app-ontwikkelaar (en diens organisatie) stromen, en (ii) de ondoorzichtigheid van de processen van app-ontwikkelaars (en hun organisaties) die vervolgens de informatie over die processen en over de gegevensverwerking binnen PIMS kunnen belemmeren.

Zelfs wanneer PIMS aanvullende informatie zouden kunnen bieden over de verwerkingspraktijken van organisaties, is het nut hiervan voor veel gebruikers onduidelijk. Bovendien kan hierdoor onterecht een beeld ontstaan dat gebruikers adequaat geïnformeerd zijn, terwijl de problemen die worden veroorzaakt door informatie-

65 Mantelero (noot 64).
66 D. Solove, 'Privacy Self-Management and the Consent Dilemma', *Harvard Law Review* (126) 2013, afl. 7, p. 1888-1903; D. Solove, 'The Myth of the Privacy Paradox', GWU Legal Studies Research Paper No. 2020-10, 11 februari 2020.
67 S. Zuboff, 'Big other: surveillance capitalism and the prospects of an information civilization', *Journal of Information Technology* (30) 2015, afl. 1, p. 75-89.
68 J. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism*, Oxford: Oxford University Press 2019; K. Pistor, *The code of capital. How the law creates wealth and inequality,* Princeton: Princeton University Press 2019.
69 Art. 58(1)(e) AVG; Overweging 63 AVG.
70 H. Nissenbaum, 'A Contextual Approach to Privacy Online', *Dædalus* (140) 2011, afl. 4, p. 32-48.
71 J. Burrell, 'How the machine "thinks": Understanding opacity in machine learning algorithms', *Big Data & Society* 2016, afl. 3, p. 1-12.
72 Crabtree e.a. (noot 8); Janssen e.a. (noot 1).

en machtsongelijkheden blijven voortbestaan (deze dimensie wordt toegelicht in par. 4.2).

4.1.1 *Transparantie en controle nemen af naarmate gegevens buiten organisatiegrenzen gaan*

Zodra gebruikersgegevens de grenzen van een systeem (de PIMS) of organisatie overschrijden, neemt de zichtbaarheid van en controle over die gegevens doorgaans af, evenals de mogelijkheid om eventuele latere verwerkingen te controleren.[73] Dit houdt in dat hoewel PIMS gebruikers inzicht kunnen geven in de dataverwerking *binnen* de PIMS, deze, althans op technisch niveau, gebruikers geen informatie verstrekken over – laat staan toegang geven tot – gegevens die aan app-ontwikkelaars (en daarbuiten) zijn overgedragen. Ook binnen de PIMS zullen gebruikers aldus weinig informatie van betekenis ontvangen over de details van de gegevens die daadwerkelijk worden overgedragen tussen organisaties en derden.[74]

Het feit dat gegevensverwerking buiten het zicht plaatsvindt, brengt diverse risico's met zich mee. Zulke risico's kunnen onder meer omvatten het secundair gebruik van gegevens door een organisatie waar een gebruiker het niet mee eens zou zijn, het genereren van niet kenbaar gemaakte inkomsten,[75] of onverwachte of ongewenste gevolgtrekkingen op basis van een profiel, die kunnen worden gebruikt om personen (de gebruiker, maar ook anderen) te beïnvloeden, aan te sporen of te manipuleren.[76] Omdat veel online diensten veelal ketens van actoren inzetten[77] – waarbij diensten van verschillende organisaties worden gebruikt om functionaliteiten te leveren – wordt het zicht op de specifieke organisaties die betrokken zijn bij de verwerking verder verminderd zodra de gegevens buiten de PIMS worden verplaatst.

Deze problemen zijn niet typisch voor PIMS, maar hebben betrekking op de bredere doelstellingen en inzet van de techniek voor de gegevensverwerking in de huidige ecosystemen. PIMS kunnen dit mogelijk verbeteren: zo zouden technische mechanismen de zichtbaarheid van de gegevensverwerking en overdracht van de PIMS naar de eerste ontvanger (de app-ontwikkelaar en diens organisatie) kunnen verbeteren. De servicevoorwaarden van het platform zouden organisaties kunnen verplichten tot het meer inzichtelijk maken van overdrachten naar derden (par. 2.2). Zo bepaalt Mydex in haar servicevoorwaarden dat app-ontwikkelaars geen gebruikersgegevens die zij via de service van het platform hebben verkregen, mogen overdragen aan derden, behalve voor zover dit uitdrukkelijk is afgesproken in het contract tussen de app-ontwikkelaar en het platform.[78] Met deze maatregelen kunnen PIMS gebruikers wellicht iets beter informeren over – en mogelijk iets meer controle bieden over – welke data vanuit de PIMS aan de organisatie wordt overgedragen. De mogelijkheid om gegevens daadwerkelijk te monitoren, te volgen en te controleren terwijl deze technische en beheersmatige grenzen van de PIMS overschrijden, is al langer voorwerp van onderzoek.[79]

4.1.2 *Problemen met ondoorzichtigheid en niet-naleving voor platforms die PIMS aanbieden*

De genoemde ondoorzichtigheden in de gegevensverwerking van organisaties kunnen ook platforms hinderen bij het blootleggen en beoordelen van de risico's van niet-conform gedrag van app-ontwikkelaars.[80] De monitoring- en nalevingsmaatregelen van platforms kunnen tot op zekere hoogte de risico's verminderen van een (doorgaans) beperkt begrip van gebruikers van de gegevensverwerking door app-ontwikkelaars: niet-naleving door een app-ontwikkelaar kan bijvoorbeeld leiden tot beëindiging van hun gegevensverwerking, verwijdering van de app van het platform, een waarschuwing, of betaling van schadevergoeding.[81] Platforms kunnen het gedrag van app-ontwikkelaars in de PIMS nagaan door analyse van logbestanden, audits over de apps, en door handmatige beoordelingen. Ook kunnen platforms overgaan tot *sandboxing* (het onderzoeken van het gedrag van een app in een door het platform opgezette testomgeving) en tot het opstellen van rapportages wanneer in een PIMS niet-naleving wordt gedetecteerd (vergelijkbaar met 'crashrapporten' zoals die bijvoorbeeld door Microsoft worden opgesteld).

Het is echter onduidelijk hoe effectief platforms kunnen zijn bij het detecteren van niet-naleving door app-ontwikkelaars. Veel platformoperators profileren zich – met het oog op de bescherming van de gegevensbescherming

73 J. Singh e.a., 'Big Ideas paper: Policy-driven middleware for a legally-compliant Internet of Things', *Proceedings of the 17th ACM International Middleware Conference* (november 2016, Trento); Crabtree e.a. (noot 8); J. Singh, J. Cobbe & C. Norval, 'Decision Provenance: Harnessing Data Flow for Accountable Systems', *IEEE Access* (7) 2019, p. 6562-6574.

74 Voor wat betreft verkeersgegevens zie De Montjoye e.a. die een PIMS-model hebben voorgesteld dat ziet op bescherming van die gegevens: Y.A. de Montjoye e.a., 'OpenPDS: Protecting the Privacy of Metadata through SafeAnswers', *PlosOne* 9 juli 2014, doi.org/10.1371/journal.pone.0098790. Uit de informatie van diverse PIMS-platforms blijkt dat meer algemeen wordt gesproken over 'gegevens' (zie bijvoorbeeld dev.mydex.org/data-sharing-agreement.html). Daarmee is evenwel niet uitgesloten dat verkeersgegevens deel kunnen uitmaken van de overeenkomsten tussen gebruikers en app-ontwikkelaars die de gegevensdeling nader vastleggen.

75 C. Silverman & J. Singer-Vine, 'Popular Apps In Google's Play Store Are Abusing Permissions And Committing Ad Fraud', *Buzz Feed* 14 april 2019.

76 S. Wachter & B. Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI', *Columbia Business Law Review* (2) 2019, afl. 1, p. 494-620.

77 J. Cobbe, C. Norval & J. Singh, 'What lies beneath: transparency in online service supply chains', *Journal of Cyber Policy* (1) 2020, afl. 5, p. 65-93.

78 Mydex dienstverleningsvoorwaarden, dev.mydex.org/terms-for-connections.html.

79 Singh e.a. 2017 (noot 73); Singh e.a. 2019 (noot 73); S. Pearson & M. Casassa-Mont, 'Sticky Policies: An Approach for managing Privacy across Multiple Parties', *Computer* (44) 2011, afl. 9, p. 60-68.

80 Crabtree e.a. (noot 8).

81 Mydex dienstverleningsvoorwaarden (noot 78).

en/of privacy van gebruikers, en het hen bieden van exclusieve controle over de data – met de boodschap dat zij geen directe toegang hebben tot de PIMS (inclusief gegevens, verwerking en logboeken daarvan) omdat die door gebruiker worden beheerd. Dit zal het zicht van platforms op wat er in de PIMS gebeurt, beperken. Platforms die zich daarentegen actiever tonen bij het monitoren van gegevensverwerking en -stromen, en daardoor zicht krijgen op wat meer precies gebeurt in de PIMS, brengen extra risico's met zich mee voor gegevensbescherming, terwijl deze platforms ook een 'achterdeur' in de PIMS moeten inbouwen die weer beveiligingsimplicaties heeft, en die het ecosysteem van de PIMS zou kunnen ondermijnen. Vragen rijzen echter ook over de bereidheid van een platforms om op te treden tegen app-ontwikkelaars en hun organisaties, met name wanneer dit gevolgen heeft voor het inkomen of de activiteiten van het platform.

4.2 *Bij gebruikers ontbreekt vaak kennis en ervaring*

PIMS zijn gericht op gegevensbeschermingsproblemen, met name op de moeilijkheden bij het verkrijgen van geïnformeerde toestemming en bij het verwerkelijken van controle van gebruikers. Willen PIMS deze problemen effectief kunnen bestrijden, dan moeten gebruikers ook de mogelijke implicaties van de gegevensverwerking voor de gegevensbescherming kunnen begrijpen. Dit betekent dat gebruikers enige expertise en kennis op het gebied van gegevensbescherming moeten hebben om de implicaties van analyses en het overdragen daarvan (en het overdragen van ruwe data) met app-ontwikkelaars te begrijpen. Hoewel platforms gebruikers meer informatie bieden over gegevensverwerking die plaatsvindt in hun PIMS, zal het voor gebruikers niet altijd duidelijk zijn wat de volledige implicaties zijn van bepaalde analyses, en van het overdragen ervan, omdat de risico's die met analyses samenhangen, vaak contextueel zijn. Een gebruiker kan bijvoorbeeld een app-ontwikkelaar toestaan een gedetailleerd profiel op te bouwen, zich niet realiserend dat dit vervolgens door de app-ontwikkelaar of door derden kan worden gebruikt om de gebruiker zelf en anderen te beïnvloeden, te *nudgen*, of te manipuleren.[82]

Evenzo kunnen de uitleg en visualisaties van gegevensstromen, technische parameters, configuraties of voorkeursbeheermechanismen door een app of platform ingewikkeld en lastig te begrijpen zijn voor niet-experts.[83] Het kan zelfs voor ervaren gebruikers, laat staan voor niet-technisch deskundige gebruikers, moeilijk zijn om vast te stellen waar appgedrag niet overeenkomt met de gebruikersvoorkeuren. Gebruikers zullen daarom ook enige technische expertise en kennis nodig hebben om de functionaliteiten van het platform op een zinvolle manier te gebruiken, te bevragen en te controleren.[84]

Het resultaat is dat hoewel PIMS de gebruikers in het algemeen beter informeren, het eenvoudigweg verstrekken van meer informatie niet leidt tot aanzienlijk beter geïnformeerde en mondigere gebruikers. Dat betekent dat de systemische machtsverschillen en grote verschillen in toegang tot en begrip van informatie zoals we die kennen van veel digitale ecosystemen, grotendeels niet kunnen worden doorbroken, en dat ook veel PIMS-gebruikers grotendeels machteloos en onbeschermd blijven.

4.3 *App-ontwikkelaars kunnen data nog steeds op grote schaal verwerken*

Veel platforms proberen met hun PIMS collectieve analyses te ondersteunen, zodat app-ontwikkelaars met gebruikersgegevens op grote schaal inzichten uit een hele populatie kunnen genereren (par. 2.5). Dit is immers één van de beweerdelijke voordelen waarmee PIMS-platforms app-ontwikkelaars en hun organisaties trachten over te halen zich bij hun platform aan te sluiten. In de praktijk zal dit eerder bijdragen aan het verder consolideren van de bestaande machtsongelijkheden tussen gebruikers en organisaties, dan dat het eraan zal afdoen. PIMS kunnen gebruikers helpen om deze machtsverschillen tot op zekere hoogte te begrijpen, omdat ze gebruikers in staat stellen inzicht te krijgen in de persoonlijke gegevens in hun eigen PIMS.

Het feit dat app-ontwikkelaars persoonsgegevens in PIMS van veel gebruikers tegelijkertijd kunnen verwerken – en daartoe door platforms ook worden aangemoedigd (par. 2.5) – betekent echter ook dat de app-ontwikkelaars en hun organisaties dus beter geïnformeerd blijven dan individuele gebruikers ooit zouden kunnen zijn. Hoewel de gegevens van één persoon interessant kunnen zijn voor die persoon, is het op grote schaal analyseren van persoonsgegevens met behulp van PIMS die inzichten in gebruikersgedrag en voorkeuren kunnen leveren, pas echt waardevol voor organisaties. Het is onwaarschijnlijk dat PIMS dit systemische probleem zullen aanpakken. Door de collectieve analyses en gegevensdeling mogelijk te maken en aan te moedigen, dragen PIMS waarschijnlijk verder bij aan de bestaande machtsverschillen, dan dat ze eraan afdoen.

4.4 *Problemen met 'zelf-management' bij gegevensbescherming*

Zoals besproken in par. 2 trachten PIMS zorgen rondom de huidige wijze en omvang waarmee private organisaties persoonsgegevens verwerken weg te nemen, door gebruikers meer 'controle' te geven over hun gegevens en de verwerking ervan, en door hen meer inzicht en opties te verstrekken met betrekking tot verwerking, zodat zij hun keuzes daarop kunnen afstemmen (en afdwingen). Daarmee hanteren PIMS een benadering van privacy en gegevensbescherming die gericht is op toestemming voor

82 Wachter e.a. (noot 76).
83 Anciaux e.a. (noot 38).
84 Crabtree e.a. (noot 8).

de verwerking en trachten ze gebruikers meer algemeen een effectievere 'kennisgeving en toestemming' te bieden.

Hoewel de benadering van PIMS beoogt gebruikers meer controle te geven, zijn de problemen met kennisgeving en toestemming als een manier om gebruikers in digitale ecosystemen te beschermen, genoegzaam bekend,[85] en daagt de PIMS-logica de huidige bedrijfsmodellen niet fundamenteel uit. PIMS zijn en blijven tot dusver stevig verankerd in de logica van 'privacy-zelfmanagement',[86] waarbij van gebruikers wordt verwacht dat ze hun eigen privacy beheren en zelf verantwoordelijk worden gehouden waar ze dit niet adequaat doen. Dit past in een bredere trend waarin steeds meer verantwoordelijkheid bij individuen wordt gelegd om risico's in verschillende aspecten van hun leven te beheersen,[87] ondanks het bestaan van systemische problemen waarover zij geen controle hebben en die dit moeilijk, zo niet onmogelijk maken (zoals de grote verschillen tussen gebruikers en organisaties als beschreven in par. 4, en die PIMS ook niet kunnen adresseren).

Daarnaast lijken PIMS geen rekening te houden met de realiteit van collectieve analyses, waarbij app-ontwikkelaars geaggregeerde gebruikersgegevens op grote schaal verwerken (par. 4.2). Collectieve berekeningen zijn grotendeels het gevolg van de commerciële drijfveren voor app-ontwikkelaars (par. 2.5) en PIMS-platforms (par. 2.6). Door het op grote schaal gebruiken van de geaggregeerde gegevens maken PIMS een consolidering van de bestaande machtsverschillen mogelijk, en dragen ze daar actief aan bij (par. 4.3).

Alles overziend kan de vaak individualistische benadering van PIMS, die geworteld zijn in het zelfbeheer van privacy en gegevensbescherming door gebruikers, deze meer collectieve dimensies van privacy en gegevensbescherming niet effectief doorbreken. Het onvermogen van PIMS om deze zorgen adequaat aan te pakken, leggen een meer fundamenteel probleem met PIMS als concept bloot: ze benadrukken te zeer wat het individu moet doen om zichzelf te beschermen, en te weinig wat de huidige digitale ecosystemen met hun verdienmodellen zouden moeten doen. Sterker, veel PIMS willen de bestaande verdienmodellen juist faciliteren met verbetering van de bescherming van persoonsgegevens. Dat wringt zoals uit het voorgaande blijkt.

De zorgen over en problemen met de huidige verwerking van persoonsgegevens is over het algemeen niet het gevolg van individueel falen om controle over persoonsgegevens uit te oefenen, maar van de wijze waarop de bedrijfsmodellen op dit moment functioneren. Deze modellen werken op systeemniveau, ondersteund door het in stand houden van grote verschillen in toegang tot informatie, vanuit commerciële overwegingen, gesteund door juridische regelingen,[88] netwerkeffecten en andere structurele factoren, die zich buiten de controle en het zicht van een individuele gebruiker bevinden.

5 Afsluitende opmerkingen

PIMS zijn in opkomst. Aanbieders van deze systemen beweren dat ze gebruikers in staat stellen meer uit hun gegevens te halen, meer inzicht krijgen in de verwerking van hun gegevens, en dat zij zichzelf beter kunnen beschermen tegen mogelijke privacyschendingen en verlies van controle over gegevensverwerking, omdat PIMS gebruikers technische en juridische mechanismen bieden waarmee zij hun keuzes rond de verwerking van persoonsgegevens tegenover organisaties zelf kunnen organiseren en afdwingen.

Hoewel PIMS wellicht een aantal nuttige gebruikersgerichte instrumenten voor gegevensbeheer voor een individuele gebruiker bieden, zijn ze veelal gebaseerd op het idee dat wanneer voldoende informatie op de juiste manier wordt aangeboden, gebruikers in staat zullen zijn om machtsverschillen en informatieachterstanden te overwinnen die uiteindelijk structureel en systemisch van aard zijn. Belangrijker nog is dat het vermogen van PIMS om bestaande machtsverschillen in de huidige ecosystemen te doorbreken, erg beperkt lijkt. Het decentraliseren van de gegevensverwerking naar de gebruiker brengt niet vanzelfsprekend decentralisatie van controle naar dezelfde gebruiker met zich mee.

Daarmee lijkt het antwoord op de vraag of PIMS gebruikers zich in een privacyfort bevinden, of in een privacyluchtkasteel, wel gegeven. Op enkele onderdelen (bijvoorbeeld het bieden van inzicht in de gegevensverwerking zoals die in de PIMS plaatsvindt) kunnen PIMS toegevoegde waarde bieden, maar in het bredere privacyperspectief is hun betekenis voor de 'empowerment' van gebruikers tegenover de huidige digitale ecosystemen beperkt.

---

85 S. Barocas & H. Nissenbaum, 'On Notice: The trouble with Notice and Consent, in: *Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information*, oktober 2009; R.H. Sloan & R. Warner, 'Beyond Notice and Choice: Privacy, Norms and Consent', *Suffolk University Journal of High Technology Law* 2013, afl. 14, p. 1-37; E. Bietti, 'Consent as a Free Pass: Platform Power and the Limits of the Informational Turn', *Pace Law Review* 2020, afl. 40, p. 317-398.

86 Solove (noot 66).

87 K. Hannah-Moffat, *Punishment in Disguise: Penal Governance and Canadian Women's Imprisonment*, Toronto: University of Toronto Press 2001; R. Ericson & A. Doyle, *Risk and Morality*, Toronto: University of Toronto Press 2003; W. Brown, *Undoing the Demos:Neoliberalism's Stealth Revolution*, New York: Zone Books 2015.

88 Cohen (noot 68); Pistor (noot 68).