COMMERCIEEL GEBRUIK VAN PERSOONSGEGEVENS: HOE BEÏNVLOEDT DE AVG DE BELGISCHE VRIJHEID VAN ONDERNEMEN?

Arno De Bois

I. Introductie

Deze thesis beoogt een antwoord te geven op de vraag naar de verhouding tussen de (nieuwe) gegevensbescherming en de vrijheid van ondernemen. Meer in het bijzonder wordt gezocht naar een antwoord op de vraag hoe de Algemene Verordening Gegevensbescherming[1] (AVG), die vanaf mei 2018 van toepassing is op de verwerking van persoonsgegevens, de vrijheid van ondernemen zal inperken.

De digitale markt is vandaag in volle groei. Met steeds nieuwe elementen zoals de big-data, cloud computing, machinaal leren, geavanceerde profilering en algemener de moderne verwerkingstechnieken, is dit volatiele landschap in toenemende mate het voorwerp van nieuwe soorten risico's, belangenafwegingen en conflicten. Er vindt continu een poging tot synchronisatie van de markt, de technologie en het recht plaats, waar zowel de belangen als de risico's binnen de sector sterk wijzigden doorheen de laatste decennia.

Dagelijks geconfronteerd met het raakvlak tussen deze digitale markt en de bescherming van gegevens, is het geen luxe om over een momentopname te beschikken.[2] Daarbij wordt in het bijzonder aandacht geschonken aan de AVG, die echter pas begrepen kan worden door een analyse van de huidige richtlijn gegevensbescherming[3] (richtlijn).

Met dit stuk wordt dus gepoogd door middel van juridisch onderzoek te evalueren wat de verwachte weerslag van de nieuwe AVG is op de vrijheid van ondernemen in België. Hiertoe worden eerst de fundamentele rechten geschetst die elkaar wederzijds lijken in te perken: enerzijds het recht op de vrijheid van ondernemen, en anderzijds de privacy en andere fundamentele rechten die worden beschermd door het fundamentele recht op gegevensbescherming. Vervolgens wordt geschetst wat moet worden begrepen onder economisch gebruik van persoonsgegevens alsook hoe de markt er feitelijk uit ziet. Daarna wordt aan de hand van het juridisch kader uiteengezet wie de relevante actoren zijn en hoe hun verhouding wordt geregeld binnen het nieuwe juridische kader van de AVG. Tot slot worden een aantal specifieke knelpunten aangekaart om uiteindelijk synthetiserend te antwoorden op de centrale onderzoeksvraag.

[1] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).
[2] Zie bijvoorbeeld de kritiek van de COB inzake algemene voorwaarden bij sociale media: Advies (COB) over de algemene voorwaarden van sociale netwerksites, 16 december 2015, COB 38.
[3] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

II. Juridisch kader

II.1. Algemeen

Om de onderzoeksvraag te kunnen beantwoorden richten we ons op de economische exploitatie van persoonsgegevens door bedrijven, die vaak een afweging zal vragen tussen enerzijds de vrijheid van onderneming en mogelijk toepasselijke intellectuele eigendomsrechten en anderzijds het recht op privacy en het autonome recht op gegevensbescherming van de betrokkenen.[4] Verder worden de belangen van de exploitant ook beschermd via andere elementen, zoals het auteursrecht op software of nog het bedrijfsgeheim. Hieronder wordt, na een korte uiteenzetting van het fundamentele recht op de vrijheid van ondernemen, het relevante wettelijk kader omschreven met aandacht voor de meest centrale fundamentele rechten die de vrijheid van ondernemer kunnen inperken waar het gaat om de verwerking van persoonsgegevens.

II.2. Vrijheid van ondernemen

Dit fundamentele recht is ontstaan uit een bottom-up proces van de lidstaten van de Europese Unie (EU) en is opgenomen art. 16 van het Handvest van de Grondrechten van de Europese Unie (Handvest). In België gold reeds sinds 1795 artikel 7 van het Franse Decreet d'Allarde[5] dat onder meer de vrijheid van bedrijf proclameerde. Met de invoering van het Wetboek van Economisch Recht (WER) werd het decreet opgeheven en de vrijheid van ondernemen opnieuw geformuleerd in boek 2, titel 3 WER.[6] De vrijheid van ondernemen heeft in België alsnog geen grondwettelijke basis.

De vrijheid van ondernemen bestaat volgens de toelichting van de Raad van de Europese Unie (RvEU) uit twee elementen. Het recht is enerzijds gebaseerd op de contractuele vrijheid en de jurisprudentie van het Hof van Justitie van de EU (het Hof) voor wat betreft het *recht op het uitoefenen van een economische activiteit*.[7] Ten tweede steunt het op artikel 119, leden 1 en 2 Verdrag betreffende de Werking van de Europese Unie (oud artikel 4 Verdrag tot oprichting van de Europese Gemeenschap) voor het aspect *mededingingsvrijheid*.[8]

Concreet vertaalt de vrijheid van ondernemen zich in een principiële vrijheid te kiezen op welke wijze en met welke middelen een economische activiteit wordt gevoerd. Behoudens waar de wet anders luidt of deze vrijheid in strijd komt met andere fundamentele rechten (art. 52 Handvest), staat dit toe innoverend om te springen met marktsituaties. Anderzijds impliceert dit ook de mogelijkheid om de wet voor te zijn en ongestraft grijze zones in de economische reglementering

[4] Voor een verdere uiteenzetting van het spanningsveld tussen de rechten van de betrokkenen, deze van de verantwoordelijke van de verwerking en deze van derden, alsook de positie van de rechtspraak hierover, zie A. DE BOIS, *Economisch gebruik van persoonsgegevens in België: Hoe beïnvloedt de (nieuwe) gegevensbescherming de vrijheid van ondernemen?*, VUB, 2017, 6.1.

[5] Loi du 2 et 17 mars 1791 (Décret d'Allarde).

[6] Art. 3 Wet 28 februari 2013 tot invoering van het Wetboek van economisch recht, *BS* 29 maart 2013, 19975.

[7] Onder meer HvJ 14 mei 1974, C-4/73, ECLI:EU:C:1974:51, Nold, III, b, 4.

[8] Raad van de Europese Unie, *Handvest van de grondrechten van de Europese Unie: Toelichtingen bij de volledige tekst van het handvest*, december 2000, 34. Zie ook FRA, *Freedom to conduct a business: exploring the dimensions of a fundamental right*, augustus 2015, 21.

te misbruiken (voor zover geen sprake is van strijd met genoemde juridische inperkingen). Hierbij kan bijvoorbeeld worden verwezen naar de recente Facebook-situatie voor de Belgische rechtbanken. Dankzij een gebrek aan concrete bepalingen en een zuiver procedureel verweer, is de internetgigant nog steeds vrij 'om veiligheidsredenen' door middel van *datr-cookies* het gedrag van Belgische niet-gebruikers te observeren.[9]

De vrijheid van ondernemen brengt binnen de gegevensbeschermingsregeling op meerdere wijzen een bescherming van de belangen van de verantwoordelijke met zich mee. In grote mate gaat het hier om de afweging van de rechten van betrokkenen tegen de economische belangen van de verantwoordelijke, ten einde de onredelijke gevolgen van een formele toepassing van de beschermingsregeling of nog misbruik van rechten hieruit in te perken.

II.3. Privacy en gegevensbescherming

Slechts weinig bindende regels zijn op wereldwijd niveau beschikbaar met betrekking tot de bescherming van persoonsgegevens en het recht op privacy. Als niet-bindende tekst kan worden verwezen naar de (niet-bindende) richtlijn van de OESO in verband met het internationaal verkeer van persoonsgegevens en een aantal relevante specifieke ISO-normen (vrijwillige onderwerping) met betrekking tot persoonsgegevens (Zoals ISO's Informatietechnologie, beveiligingstechnieken, managementsystemen voor informatiebeveiliging: 27001 houdende eisen hieromtrent en 27002 over de goede praktijken) alsook een algemener reglement inzake persoonsgegevens voor alle ISO-leden. [10] [11] [12]

Een regel van legale aard op het internationaal niveau is te vinden in artikel 12 van de Universele Verklaring van de Rechten van de Mens (UVRM) onder de bescherming van het privé- en gezinsleven. Daarnaast wordt nog in artikel 17 van het Internationaal verdrag inzake burgerrechten en politieke rechten (BUPO) en 16 van het Internationaal Verdrag inzake de Rechten van het Kind (IVRK) dit beginsel in verdragsvorm gegoten. Al deze teksten kwamen tot stand binnen de Verenigde Naties.

Op het Europees niveau vindt het recht op privacy vertaling in artikel 8 van het Europees Verdrag tot bescherming van de Rechten van de Mens (EVRM) tot stand gekomen binnen de Raad van Europa (RvE) alsook in artikel 7 van het Handvest van de EU.

Uit een samenlezing van artikelen 22 en 29 van de Grondwet (respectievelijk eerbied voor privéleven en briefgeheim) kan tevens een recht op privacy worden afgeleid dat speelt in het kader van persoonsgegevens.

In het kader van de technische ontwikkelingen lijkt geschikter het recht op privacy ruimer te interpreteren dan Warren & Brandeis' klassieke ''the right to be left alone''.[13] Er heeft een

[9] De Redactie, *Facebook en Privacy* http://deredactie.be/cm/vrtnieuws/cultuur%2Ben%2Bmedia/media/2.37414.
[10] OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
[11] Zie https://www.privacycommission.be/nl/node/3844.
[12] https://www.iso.org/iso-member-data-protection-policy.html.
[13] L.D. BRANDEIS & S.D. WARREN, "The Right to Privacy", *Harvard L.R.*, 1890.

verschuiving plaatsgevonden van het negatieve, strikt private recht op privacy zoals artikel 8 EVRM het omschrijft, naar een positief recht op controle op de veruitwendiging van persoonlijkheid. Om hanteerbaar te zijn in de moderne infrastructuur omvat het begrip noodzakelijk een recht op de constructie van de identiteit, gekend als 'informationele privacy'. In dat verband wijst Hildebrandt naar de Franse filosoof Ricoeur's onderscheid tussen *ipse*-identiteit (de kern van de persoonlijkheid, evolutief van aard) en *idem*-identiteit (de indentiteit als aanspreekpunt voor de buitenstaander, vast gegeven). Het (positieve) recht op privacy betreft dan de vorming van de *ipse*-identiteit.[14] Dit positieve recht op privacy vindt ergens vertaling in het autonome recht op gegevensbescherming uit artikel 8 van het Handvest.

Het negatieve ('to be left alone') en positieve ('construction of identity') aspect van privacy synthetiserend en daarbij een absoluut karakter uitsluitend, lijkt een geschikte invulling van het recht op privacy te zijn gegeven door Agre en Rotenberg als de 'vrijheid van onredelijke beperking op de constructie van de eigen identiteit'.[15]

Als fundamenteel recht uit het EVRM heeft artikel 8 directe werking. Het Europese Hof voor de Rechten van de Mens (EHRM) heeft zelfs meermaals het bestaan van een indirecte horizontale werking bekrachtigd, waar bij gebreke van daadwerkelijke bescherming door tussenkomst van de staat, laatste kan worden aangesproken.[16] Verder heeft het EHRM ook onderstreept dat het als dusdanig evenwaardig is aan de andere grondrechten, omdat niet houdbaar zou zijn dat het geschil tussen twee concurrerende grondrechten (in casu artikelen 8 en 10) anders ontknoopt naargelang het grondrecht dat ter inleiding wordt aangevoerd.[17] Op deze wijze zal de bescherming van persoonsgegevens als element van het recht op privacy uit 8 EVRM, wanneer in strijd met andere grondrechten, naar het EHRM geen principiële voorrang hebben.

Wat betreft het beroep op artikel 7 (en 8) van het Handvest zijn de zaken weliswaar minder duidelijk. Alvast heeft het Hof zich over de toepasbaarheid van de richtlijn (waarvan het handvest retroactief een grondslag vormt) uitgesproken. In de zaken Rechnungshof en ASNEF stelt het HvJ dat de bepalingen van de richtlijn directe werking hebben in zoverre ze duidelijk genoeg zijn en geen weerklank vinden in het (tegenstrijdige) nationale recht. Waar de bepalingen geen interpretatieruimte overlaten, geldt een directe inroepbaarheid voor de nationale instanties.[18]

Waar reeds blijkt dat sommige bepalingen van het Handvest wel, dan geen directe horizontale werking hebben, moet in afwachting van een interpretatie worden gesteund op andere

[14] P. DE HERT, *Artikel 8 EVRM en Het Belgische Recht: De bescherming van Privacy, Gezin, Woonst en Communicatie*, Mys & Breesch, Gent, 1998, 68-71, B. VAN DER SLOOT, "Privacy as Personality Right: Why the ECtHR's Focus on Ulterior Interests Might Prove Indispensable in the Age of "Big Data", *UJIEL*, 2015, 44, M. HILDEBRANDT, *Privacy en identiteit in slimme omgevingen*, 2010, 4-5, P. DE HERT, *A right to identity to face the internet of things?*, Unesco, Strasbourg, 2008, 1-4.

[15] P.E. AGRE & M. ROTENBERG (Eds), *Technology and Privacy: The New Landscape*, MIT Press, Cambridge, 1997, 6-7, vertaald door M. Hildebrandt in M. HILDEBRANDT, *Privacy en identiteit in slimme omgevingen*, 2010, 9.

[16] Zie bijvoorbeeld EHRM 9 oktober 1979, nr. 6289/73, Airey/Ierland, 32-33. Hier gaat het specifiek om art. 8 EVRM.

[17] EHRM 16 juni 2015, nr. 64569/09, Delfi/Estland, 139.

[18] HvJ 20 mei 2003, gevoegde zaken C-465/00, C-138/01 en C-139/01, Rechnungshof, 98 en HvJ 24 november 2011, gevoegde zaken C 468/10 en C 469/10, ASNEF, 52.

indicatoren om het effect van de rechten in te schatten.[19] Met de indirecte horizontale werking van artikel 8 EVRM (rekening houdende met artikel 52 Handvest) en de directe werking van de richtlijn zou alvast kunnen worden uitgegaan van minstens een indirecte horizontale werking van het recht op privacy uit 7 Handvest.[20]

Verder zijn op het Europees niveau in de eerste plaats een aantal beginselen en grondrechten uit het EVRM en het Handvest van belang. Naast het reeds aangehaalde recht op privacy uit 8 EVRM en 7 Handvest, is nog relevant het recht op eerlijk proces geboden door 6 EVRM. Uit het Handvest spelen naast de vrijheid van ondernemen [supra] uit artikel 16 nog mee het recht op informatie uit artikel 11, het recht op eigendom uit artikel 17 en het autonome recht op de bescherming van persoonsgegevens uit artikel 8. Merk op dat wanneer een inbreuk op artikel 8 Handvest tevens een inbreuk op de privacy inhoudt, de bescherming uit artikel 8 EVRM alsnog toepassing vindt.

Artikel 8 Handvest:

''1. Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens.

2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan.''

Er is hierbij ruimte voor discussie over de draagwijdte van 8, 2 als een omschrijving van de bescherming in 8, 1 (beperkend), dan wel een toevoeging aan de in 8, 1 omschreven algemene bescherming (uitbreidend). In het licht van de aparte verwijzing naar aspecten als kwaliteit en bescherming van gegevens (bijvoorbeeld beginselmatig artikel 5 f & §2 AVG met betrekking tot kwaliteit en beveiliging), die noch onder 8, 2 worden geëxpliciteerd, noch zonder discussie onder het recht op privacy vallen[21], lijkt artikel 8, 1 ergens wel een autonoom vangnet te vormen. Verder zou het interpreteren als een beperking tevens moeilijk verzoenbaar zijn met de beperkingsgronden zoals omschreven in artikel 52, eerste lid van het Handvest. Anderzijds kan weer worden geargumenteerd dat kwaliteit en gegevensbescherming als tools ter constructie van de identiteit onder het (positieve) recht op privacy vallen, wat dan weer de meerwaarde van het eerste lid gedeeltelijk zou uithollen in de mate dat de overlappende bescherming kan worden herleid tot de bescherming van de privacy. In ieder geval is 8, 2 minstens te interpreteren als een minimumbescherming. Daarbinnen vallen een vijftal elementen [infra] te onderscheiden: eerlijke verwerking, doelbinding, transparantie, vereiste grondslag en rectificatierecht.

[19] H. SEVERIJNS, "Inroepbaarheid van het Handvest van de grondrechten van de Europese Unie", *JF*, 2013-2014, 1020.
[20] Ik besef dat dit een overbodige redenering is in het licht van de inroepbaarheid van 8 EVRM, maar ik haal dit voornamelijk aan om infra de werking van 8 Handvest te evalueren.
[21] Zie bijvoorbeeld standpunt in P. DE HERT & S. GUTWIRTH, *"Data protection in the case law of Strasbourg and Luxemburg : constitutionalisation in action" Reinventing Data Protection?*, 2009, 5-6.

Ter gedachte moet worden gehouden dat het Handvest retroactief de grondslag vormt van de richtlijn en bijgevolg van de Wet van '92 (PW, Privacywet)[22]. Deze wet werd gewijzigd ter implementatie van de richtlijn en vormt op nationaal niveau het centrale stuk van de gegevensbescherming. Ook de e-privacyrichtlijn[23] vindt er vertaling in.

Rekening houdend met de grondslag van artikel 8 Handvest in 8 EVRM (en de indirecte horizontale werking van 8 EVRM), deze in de gegevensbeschermingsregeling (en de directe horizontale werking van de richtlijn) en de rechtspraak van het Hof waaruit voor zover de directe werking van bepaalde rechten uit het Handvest blijkt, is verdedigbaar dat – net als eerder opgemerkt inzake artikel 7 – ook artikel 8 Handvest, al dan niet rechtsreeks, horizontale werking heeft. Dit zou inhouden dat overheden minstens een positieve verplichting hebben om de eerbiediging van dit recht te waarborgen en bovendien dat een maatregel afbreuk aan het recht kan doen, zonder daarom in strijd te zijn met de relevante uitwerkende regeling.[24] In het licht van artikel 8 als aanvulling van het negatieve recht op privacy van artikel 7, kan bovendien (voorzichtig) worden gesteld dat het recht op gegevensbescherming tevens directe horizontale werking heeft, waar de beschermingsregeling een uitwerking van het recht vormt en ergens de balanceringsoefening ervan met andere rechten uitmaakt.[25]

Uit het autonome recht op gegevensbescherming vloeien onder meer voort de rechten van verzet, bezwaar en vergetelheid [infra].

Een eerste gespecialiseerd bindend instrument op Europees niveau was Verdrag 108[26] van de RvE. Met betrekking tot het besproken economisch gebruik is de waarde hiervan echter beperkt, aangezien het vooral van belang is gebleven voor aspecten die buiten de bevoegdheid van de Europese Rechtssystemen liggen (zoals strafrecht). De meerderheid van de inhoud die wel binnen die bevoegdheden past is dan ook overgenomen in een aantal instrument van de Unie (waaronder de richtlijn).[27]

Een deel van de privacy in verband met persoonsgegevens wordt naast de richtlijn gegevensbescherming tevens beschermd met de reeds aangehaalde e-privacyrichtlijn van 2002. Deze vormt een lex specialis ten aanzien van de richtlijn en handelt voornamelijk over het verwerken van informatie met betrekking tot telecommunicatie en locatie.

---

[22] Wet 8 december 1992 voor de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *BS* 18 maart 1993, 5801.

[23] Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie).

[24] Zie zaak Promusicae, waar de gegevensbescherming in de ruime zin wordt afgewogen tegen andere fundamentele rechten. HvJ 29 januari 2008, C-275/06, Productores de Música de España (Promusicae)/Telefónica de España SAU, 65 & 68.

[25] H. KRANENBORG, *Art 8 – Protection of Personal Data in The EU Charter of Fundamental Rights, a commentary*, Hart Publishing, 2014, 265.

[26] Verdrag 108 tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens.

[27] https://www.privacycommission.be/nl/raad-van-europa.

Vanuit het economisch perspectief bekeken speelt ook de databankenrichtlijn van '96 mee.[28] De auteursrechtelijke en sui generis beschermingssystemen uit deze richtlijn zijn vandaag in het WER terug te vinden.[29]

Valt nog op te wijzen de Privacy-Shield Agreement gesloten tussen de US Department of Commerce en de Europese Commissie (Commissie). Deze overeenkomst komt in de plaats van de vorige Safe Harbor Principles[30] die als waarborg voor de bescherming van privacy werden afgewezen door het HvJ.[31] [32] De nieuwe geschiktheidsbeschikking van de Commissie, deze keer betreffende de Privacy Shield[33], is echter al ter discussie gesteld en staat momenteel te wachten op een uitspraak van het Hof.[34]

Uiteindelijk zal nog onrechtstreeks meespelen in de beschermingsregeling het verbod op discriminatie uit artikelen 10 en 11 Grondwet.

Wat betreft aanbevelingen zijn van belang ten eerste de publicaties van de Commissie.[35] Een gespecialiseerd orgaan daarbinnen is de Werkgroep artikel 29. Steunend op artikel 29 richtlijn, werd dit orgaan opgericht met als opdracht raad te geven in verband met de bescherming van persoonsgegevens.[36] Uiteindelijk zijn ook een aantal publicaties van de EU Fundamental Rights Agency (FRA) relevant in het kader van persoonsgegevens, dan eerder bekeken vanuit een mensenrechtelijk perspectief.[37]

Het belangrijkste adviserend orgaan inzake de bescherming van persoonsgegevens in België is de Commissie voor de Bescherming van de Persoonlijke Levenssfeer (CBPL, Privacycommissie), opgericht bij artikelen 23 e.v. van de Privacywet. Naast adviezen aan overheidsorganen en aanbevelingen houdt de CBPL zich bezig met het toegankelijk maken van de hele privacybescherming, de behandeling van klachten en de controle op de naleving van de wet.

II.4. Naderend kader

Op 24 mei 2016 is de AVG in werking getreden. Vanaf 25 mei 2018 zal deze verordening in België van toepassing zijn[38] en daarmee zal ook de eerdere richtlijn worden ingetrokken.[39] Het

[28] Richtlijn 96/9/EG van het Europees Parlement en de Raad van 11 maart 1996 betreffende de rechtsbescherming van databanken.
[29] Zie ook inzake doelstellingen van de commissies: 31e Conferentie van de commissarissen voor gegevensbescherming, Madrid, Spanje 4-6 november 2009 Resolutie betreffende internationale privacynormen.
[30] http://web.archive.org/web/20150908060809/http://export.gov/safeharbor/eu/eg_main_018475.asp.
[31] K. DAUGIRDAS, & J.D. MORTENSON, (ed.), "Contemporary Practice of the United States Relating to International Law", *amerjintelaw*, 2016, 360-368.
[32] HvJ 6 oktober 2015, C-362/14, ECLI:EU:C:2015:650, Schrems, 106.
[33] 2000/520 en 2016/1250 (C(2016)4176).
[34] Verzoekschrift OJ C 410 van 07 november 2016, p.26, Digital Rights Ireland v Commission. Zie verder ook een trend in evaluaties ten aanzien van de Verenigde Staten, vb. C-317 & 318/04, Parlement v Raad, 30 mei 2006, 67-70.
[35] http://ec.europa.eu/justice/data-protection/.
[36] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec21.
[37] http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection.
[38] Art. 99 AVG.
[39] Art. 96 AVG.

gaat om een verordening met rechtstreekse toepassing, die weliswaar verdere uitvoering vereist. Waar de verordening heel wat ruimte laat voor invulling door de staten, heeft deze soms wel het karakter van een richtlijn.[40]

Belangrijk gegeven is dat parallel hieraan tevens een regeling inzake elektronische communicatie het licht ziet.[41] De naderende e-privacyverordening zal als lex specialis bij voorrang op de AVG gelden. Dit betekent dat bepaalde aspecten zoals de geldigheid van de toestemming voor de verwerkingen die onder de verordening in kwestie vallen, tevens in het licht hiervan zullen moeten worden geëvalueerd. Voor deze proef wordt de verordening slechts aangehaald met betrekking tot een specifiek knelpunt inzake hergebruik van gegevens.

Daarnaast werd door de Commissie in 2015 een richtlijn voorgesteld inzake contracten over digitale inhoud.[42] Artikel 3 van deze ontwerprichtlijn omschrijft als onderdeel van het toepassingsgebied de overeenkomsten waarbij digitale inhoud wordt geleverd met als tegenprestatie persoonsgegevens. In artikel 13 van het ontwerp staan inzake de ontbinding van dergelijke contracten heel wat waarborgen voor de consument zoals het recht de toestemming vormvrij in te trekken en het recht op toegang tot de door hem verstrekte en door de leverancier gegenereerde gegevens.

Met de AVG wordt een nieuw orgaan als opvolger van de Werkgroep 29 ingevoerd: het Europees Comité voor gegevensbescherming. Dit onafhankelijke orgaan is samengesteld uit vertegenwoordigers van alle nationale toezichtsorganen en heeft tot taak voornamelijk het uitvaardigen van aanbevelingen, richtsnoeren en beste praktijken inzake persoonsgegevens, alsook een adviesbevoegdheid naar de Commissie toe inzake gegevensbescherming.[43]

[40] D. DE BOT, "De uitvoering van de algemene verordening gegevensbescherming – enkele bemerkingen bij de Belgische context", *TVW*, 2016, 234.
[41] Voorlopig is het voorstel nog ter bespreking: http://eur-lex.europa.eu/procedure/EN/2017_3
[42] Voorstel 2015/0288 (COD) voor een richtlijn van het Europees Parlement en de Raad betreffende bepaalde aspecten van overeenkomsten voor de online-verkoop en andere verkoop op afstand van goederen.
[43] Art. 68-70 AVG.

III. Begrippen, afbakening en context

III.1. Economisch gebruik

Dit onderzoek centreert zich rond de voorwaarden en beperkingen op het exploiteren van persoonsgegevens door private actoren. Elke handeling die valt onder 'verwerking' en daarbij gesteld wordt met een -al dan niet direct- winstoogmerk, wordt hierbij beschouwd als economische exploitatie. Deze definitie sluit alvast uit de daden door zuiver publieke instellingen (ook de uitzonderingen en plichten voor zuiver publieke instanties worden genegeerd) gesteld, zoals de verwerking in een strafrechtelijke of fiscale context, en deze gesteld met een ander dan winstgevend oogmerk. Dit laatste omvat enerzijds de verwerking voor onder meer historische en wetenschappelijke doeleinden, maar ook het gebruik voor zuiver private doeleinden (zoals het bijhouden van een telefoonboek). Overigens maken een meerderheid van deze doeleinden de verwerking het voorwerp van een bijzondere regeling binnen de gegevensbescherming. Sommige activiteiten zonder winstoogmerk worden naar de wettelijke definitie geacht onder de regeling te vallen (bijvoorbeeld de 'self-tracking' activiteit van de NGO Quantified Self), maar zullen bij gebrek aan economisch karakter buiten beschouwing worden gelaten.[44] Uiteindelijk zal ook worden vermeden in te gaan op het economisch gebruik dat de facto wordt beschermd door de vrijheid van informatie en meningsuiting. De verwerking als component van de pers valt als dusdanig buiten beschouwing. In eenzelfde lijn wordt het conflict tussen de monetarisering van persoonsgegevens en sommige andere belangen die met andere middelen dan de gegevensbescherming op zich kunnen worden beschermd, tevens buiten beschouwing gelaten. Zo zal bijvoorbeeld niet worden ingegaan op de overlappende bescherming die aan foto's wordt geboden via het portretrecht of nog de intellectuele eigendom.

Het economisch gebruik betreft dan voornamelijk het vergaren en interpreteren van persoonsgegevens om efficiënter op te treden binnen de markt (bijvoorbeeld doelgerichte reclame, prijsefficiëntie, 'op maat' contact met klanten,…), maar uiteraard ook de activiteit die in hoofdzaak gericht is op de verwerking van persoonsgegevens om daaraan toegevoegde waarde te onttrekken. Zo is recent een enorme opkomst vast te stellen van ondernemingen waarvan het gebruik van persoonsgegevens een centraal element van het verdienmodel uitmaakt.

III.1 §1. Andere doeleinden

Naar artikel 89 AVG gaat de verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden gepaard met bepaalde waarborgen ter eerbied van het beginsel van minimale gegevensverwerking. Dit houdt onder meer in dat de gegevens zodra het mogelijk is in het kader van dat doel, horen te worden gepseudonimiseerd, dan wel geanonimiseerd (1). Mits aan deze waarborgen voldaan wordt en in de mate dat anders handelen de doeleinden in het gedrang zou brengen, is het mogelijk om bij voor de verwerking met oog op wetenschappelijk of historisch onderzoek of statistisch

[44] http://quantifiedself.com/about/.

onderzoek, bij wet af te wijken van de rechten van [infra] inzage, rectificatie, bezwaar en beperking (2). Bij de verwerking met het oog op archivering in het algemeen belang kan daarboven in dezelfde omstandigheden een uitzondering gelden op de kennisgevingsplicht met betrekking tot de rectificatie, uitwissing of verwerkingsbeperking alsook op de overdraagbaarheid van gegevens (3). De uitzonderingsregelingen gelden dan ook enkel ten aanzien van de verwerking in het kader van de besproken doeleinden (4).

Hierbij behoort even aandacht te worden geschonken aan de definitie van aangehaalde statistische doeleinden, waar naar de volksmond een marktonderzoek alvast een statistisch doeleind uitmaakt, maar de gedachte dat alle profilering [infra] zich via deze omweg aan de regeling kan onttrekken, wringt. Overweging 162 van de AVG omschrijft de statistische doeleinden en veronderstelt alvast dat dit meer bestrijkt dan statistiek in een wetenschappelijke context.

Er kan dus worden besloten dat zelfs binnen een economisch kader, statistisch onderzoek steeds onder de uitzondering valt, in zoverre het resultaat ervan niet wordt aangewend om ten aanzien van een welbepaalde natuurlijke persoon beslissingen te nemen. Met andere woorden wordt net toegepaste profilering uitgesloten. A contrario zou elk ander statistisch onderzoek ten einde bijvoorbeeld marktstrategie aan te passen, hier wel onder vallen, waar het effect ervan gelijk is voor alle betrokkenen. Uiteindelijk is hier wel wat speelruimte in te zien, waar bijvoorbeeld een marktstrategie op basis van locatie in zekere zin neerkomt op een onderscheiden behandeling tussen categorieën betrokkenen.[45]

III.1 §2. Verwerking[46]

Art 1 PW, letterlijk overgenomen uit art 2 van de richtlijn, omschrijft de verwerking met een lijst werkwoorden (verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, uitwissen,...). In art 4 AVG worden voor een aantal begrippen nauwverwante alternatieven gebruikt. Uit de niet-limitatieve formulering van de teksten ('zoals', 'such as') blijkt dat deze opsomming nog kan aangevuld worden met zowat alle denkbare bewerkingen. Zo zou de verplaatsing van data (dat technisch gezien niet meer is dan kopiëren en de oorspronkelijke locatie opkuisen) of het toevoegen van metadata en labels eveneens een verwerking uitmaken, hoewel de tekst hierover zwijgt.

III.2. Persoonsgegevens

III.2 §1. Definitie

In eerste instantie wordt hier gekeken naar de wettelijke invulling.

[45] De CBPL zou er goed aan doen deze begrippen toe te lichten, teneinde de rechtssubjecten in staat te stellen dit in te schatten, <<www.privacycommission.be/nl/lexicon/doeleinden-historische-statistische-wetenschappelijke>>.
[46] Zie A. DE BOIS, *Economisch gebruik van persoonsgegevens in België: Hoe beïnvloedt de (nieuwe) gegevensbescherming de vrijheid van ondernemen?*, VUB, 2017, annex 'Verzameling van persoonsgegevens'.

Naar een samenlezing van artikelen 4,1 AVG, 1 PW en overweging 26 van zowel de richtlijn als de AVG, gaat het om alle denkbare gegevens[47] betreffende identificeerbare natuurlijke personen. Evenwel besliste het Hof in een prejudicieel arrest van 2010 dat rechtspersonen beroep kunnen doen op de door de artikelen 7 en 8 van het Handvest geboden bescherming voor zover uit de officiële naam van de rechtspersoon de identiteit van een of meer natuurlijke personen blijkt.[48] Uit de toelichting bij artikel 8 (bescherming van persoonsgegevens) van het handvest blijkt dat dit artikel onder meer steunt op de richtlijn.[49] Bijgevolg zou de uitspraak zich ook uitstrekken tot de toepasselijkheid van de gegevensbeschermingsregeling.[50]

Het gaat dus om gegevens die het mogelijk maken natuurlijke (en onder omstandigheden juridische) personen (in)direct te identificeren. Anonieme gegevens vallen hierbuiten.[51] Merk op dat geanonimiseerde gegevens weliswaar buiten de gegevensbeschermingswetgeving vallen, maar dat de betrokkenen nog steeds bescherming genieten op grond van andere bepalingen zoals bijvoorbeeld deze met betrekking tot het vertrouwelijk karakter van communicatie.[52]

III.2 §2. Anonieme gegevens

In de zin van richtlijn spreekt men van anonimisering wanneer persoonsgegevens zodanig worden verwerkt dat (redelijkerwijze) elke mogelijkheid tot (re)identificatie van betrokkenen onherroepelijk wordt uitgesloten.[53]

Aangezien de wetgeving geen bepalingen bevat omtrent de wijze waarop zodanige verwerking gebeurt, bestaan er verschillende technieken van anonimisering. Deze moeten steeds per geval worden bekeken in functie van alle contextuele factoren. Dit houdt in dat moet worden gekeken naar alle middelen die redelijkerwijs zijn in te zetten door de betrokken actoren. Hierbij beschouwt men dan ook de huidige stand van de techniek (mogelijkheden van computers, hulpmiddelen…).[54]

Het Hof benadrukte dat deze kwestie niet enkel in hoofde van de verantwoordelijke voor de verwerking moet worden beoordeeld, maar dat hierbij ook rekening moet worden gehouden met de mogelijkheid tot re-identificatie door derden en de middelen die door deze zijn in te zetten.

---

[47] Zie A. DE BOIS, *Economisch gebruik van persoonsgegevens in België: Hoe beïnvloedt de (nieuwe) gegevensbescherming de vrijheid van ondernemen?*, VUB, 2017, annex 'Persoonsgegevens'.
[48] HvJ 9 november 2010, gevoegde zaken C-92/09 en C-93/09, Schecke, 53.
[49] Raad van de Europese Unie, *Handvest van de grondrechten van de Europese Unie: Toelichtingen bij de volledige tekst van het handvest*, december 2000, 26.
[50] In dit verband valt tevens kort op te merken dat een deel van de beschermingsregeling inzake persoonsgegevens voortvloeiend uit de e-privacyrichtlijn tevens voor rechtspersonen geldt. Zo stelt artikel 1, 2 van de richtlijn. Artikelen 12, 4 en 13, 5 breiden dan ook gedeeltelijk de bescherming inzake de opneming in abonneelijsten en ongewenste communicatie uit tot abonnees andere dan natuurlijke personen.
[51] Advies (WP29) over anonimiseringstechnieken, 10 april 2014, 5/2014, 3.
[52] Zie art. 5,3 e-privacyrichtlijn.
[53] Advies (WP29) over anonimiseringstechnieken, 10 april 2014, 5/2014, 3. Zie ook overweging 26 richtlijn.
[54] ibid, 7.

Het is dus ook niet vereist dat alle middelen voor de re-identificatie bij eenzelfde persoon rusten.[55]

Geanonimiseerde data kunnen dus in beginsel door derden worden verwerkt zonder rekening te moeten houden met de beschermende regeling. Niettemin zijn derden verplicht rekening te houden met de contextuele factoren inzake mogelijke re-identificatie bij het bepalen van de doeleinden van dit gebruik. Indien dat gebruik op zich een risico vormt voor (re)identificatie van de betrokkenen, valt de verwerking opnieuw onder de gegevensbeschermingsregeling.[56] [57]

Er is bovendien een verschil tussen anonimisering en pseudonimisering.

Artikel 4,5 AVG omschrijft voor het eerst pseudonimisering, zijnde:

''het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld'' [58]

AVG overweging 26 maakt daarboven duidelijk dat:

''Gepseudonimiseerde persoonsgegevens die door het gebruik van aanvullende gegevens aan een natuurlijke persoon kunnen worden gekoppeld, moeten als gegevens over een identificeerbare natuurlijke persoon worden beschouwd.''[59]

III.2 §3. Territoriale afbakening

Het onderzoek betreft de situatie in België en bijgevolg wat als 'Belgische persoonsgegevens' (vallende onder de Belgische invulling van de regeling) moet worden beschouwd. Ter afbakening wordt gevolgd de logica van het toepassingsgebied van de nationale en supranationale regelgeving. Daarbij wordt uitgesloten wat zou leiden tot de studie van vreemd recht.

Naar een samenlezing van 3bis PW en 4 richtlijn is de toepasselijke wetgeving telkens te beoordelen in functie van de vestiging (wat ruim wordt uitgelegd) van de verantwoordelijke voor de verwerking.[60] Zo de gegevens technisch gezien worden verwerkt in de ene lidstaat, maar worden verworven in het kader van een vestiging in een andere lidstaat, zal a fortiori de

[55] HvJ 19 oktober 2014, C-582/14, Breyer/Duitsland, 42 & 43.
[56] Advies (WP29) over anonimiseringstechnieken, 10 april 2014, 5/2014, 11
[57] Zie A. DE BOIS, *Economisch gebruik van persoonsgegevens in België: Hoe beïnvloedt de (nieuwe) gegevensbescherming de vrijheid van ondernemen?*, VUB, 2017, annex 'Anonimiseringstechnieken'.
[58] Zie ibid annex 'Pseudonimiseringstechnieken'.
[59] Zie ook artikelen 5, 6 & 9 e-privacyrichtlijn. Onder de richtlijn horen verkeersgegevens te worden geanonimiseerd zodra de identificatie niet meer essentieel is ter verwezenlijking van het doel en andere locatiegegevens dan verkeersgegevens slechts mogen worden verwerkt in de mate dat deze reeds geanonimiseerd zijn, behoudens toestemming van de betrokkene en de gevallen waarin dit de uitvoering van de overeenkomst in de weg staat.
[60] HvJ 1 oktober 2015, C-230/14, Weltimmo, 30-33. Zie ook verwijzing naar L'oreal in HvJ 13 mei 2014, C-131/12, Google/Spain, 53. Van een vestiging is reeds spreke zodra enkel een vertegenwoordiger aanwezig is in de lidstaat waarop een activiteit gericht is.

wetgeving van deze laatste van toepassing zijn. Dit schakelt meteen een reeks rechtsmachtsproblemen uit binnen de Unie, waar als aanknopingsfactor de plaats van vestiging wordt aangenomen. Dit is verantwoord aangezien het gaat om een geharmoniseerde minimumbescherming.

Art 3 AVG verruimt en preciseert het toepassingsgebied tot de verwerking van persoonsgegevens binnen de Unie.

In het kader van de verordening wordt de locatie van de betrokkene als aanknopingsfactor gehanteerd. De alternatieve voorwaarden 'aanbieden van goederen of diensten' en 'monitoren van gedrag binnen de Unie' bestrijken een meerderheid van de redenen waarvoor persoonsgegevens van betrokkenen binnen de Unie zouden worden verwerkt.[61] De AVG bestrijkt met 'monitoren' eveneens de verwerking die losstaat van enige (klaarblijkelijk voorgenomen) activiteit binnen de Unie.[62]

Anticiperend op de toekomstige inwerkingtreding van de AVG worden beschouwd als relevant de persoonsgegevens die verwerkt worden enerzijds voor een in België gevestigde actor en anderzijds voor een buiten de EU gevestigde actor in de mate dat de verwerking ofwel gebeurt door een in België gelegen middel en niet slechts doorvoer binnen België betreft, ofwel verstrekking van goederen en diensten in België betreft, ofwel de monitoring van betrokkenen op het Belgische grondgebied betreft. Verwerking voor een in een andere lidstaat gevestigde actor wordt buiten beschouwing gelaten omdat dit zou leiden tot een comparatieve studie van het omgezet EU recht, waartoe hier de ruimte ontbreekt.

III.2 §4. Juridische kwalificatie van persoonsgegevens

Persoonsgegevens betreffen informatie gerelateerd aan identificeerbare personen onder welke vorm ook opgenomen. Het medium kan bijvoorbeeld akoestisch, grafisch, alfanumeriek of binair zijn. De informatie zelf kan betrekking hebben op elk aspect van de betrokken persoon. De gegevens kunnen dus betrekking hebben op het privéleven, maar ook gegevens over zaken buiten deze kwalificatie, zoals deze over iemands beroepsrelaties of economisch of sociaal gedrag, vallen te beschouwen als persoonsgegevens.[63] Overigens blijkt uit het later tot stand gekomen handvest eveneens een afzonderlijke beschouwing van de bescherming van persoonsgegevens te bestaan naast -en overlappend met- het recht op privacy.[64]

---

[61] Volgens overweging 23 van de AVG wordt het 'aanbieden' bedoeld in art 3, 2, a) beoordeeld op basis van een 'klaarblijkelijk voornemen' diensten aan te bieden aan betrokkenen in één of meer lidstaten in de Unie. Er hoeft dus niet per definitie reeds een dienst te zijn aangeboden. Dit kan bijvoorbeeld van belang zijn in situaties van voorafgaand (markt)onderzoek, waarbij een strikte uitlegging van 'aanbieden' de beschermingsregeling buiten spel zou zetten. Het voornemen wordt per geval afgeleid uit verschillende elementen (zoals taal en geografische toegankelijkheid van de website, gehanteerde valuta…) die op zichzelf niet per definitie doorslaggevend zijn ter bepaling van die intentie.

[62] Overweging 24 van de AVG licht de bedoelde 'monitoring' toe als het volgen op het internet van natuurlijke personen met in het bijzonder aandacht voor technieken van profilering.

[63] Advies (WP29) over het begrip persoonsgegeven, 20 juni 2007, 4/2007, 7.

[64] Artikelen 7 & 8 Handvest.

Persoonsgegevens zijn als privaatrechtelijk rechtsobject moeilijk te kwalificeren omdat ze in de eerste plaats vallen onder de rubriek 'data' waarvan de kwalificatie op zich al problematisch is, maar daarboven ook een bijzondere categorie uitmaken vanwege hun verworvenheid met identiteit en privacy. Het is onweerlegbaar dat bepaalde persoonsgegevens een zekere economische waarde vertegenwoordigen (kijk naar het toenemende aantal diensten die in ruil voor gegevens worden verleend), maar een strikt vermogensrechtelijke benadering is niet voor de hand liggend.

Hoewel de term 'persoonsgegevens' alle mogelijke dragers omvat, gebruiken we verder '*data*' als gedigitaliseerde gegevens omdat deze het voorwerp van dit onderzoek vormen maar ook omdat ze vandaag de facto de relevante gegevens zijn. In de volksmond betreft de bezorgdheid om het gebruik van 'data' doorgaans ook veeleer dat van de gedigitaliseerde databestanden zelf dan dat van de informatie op zich, omdat de niet-gedigitaliseerde gegevens veel minder risico's op verspreiding inhouden.[65] Naast het feit dat digitale gegevens op zo veel meer manieren kunnen worden verwerkt dan niet-gedigitaliseerde gegevens, maakt ook hun (voorspelde) volume dat van de andere vormen verwaarloosbaar. Zo voorspelde DCI dat tegen 2020 het wereldwijde volume aan digitale gegevens ongeveer 44 ZB zou bedragen, wat neerkomt op 44.10^{21} bytes (waarbij 1 byte een leesteken vertegenwoordigt).[66] De Berkeley University of California zou hebben geschat dat de totale omvang van alle menselijke kennis, muziek, woorden en beelden in het jaar 1999 wereldwijd aanwezig zo'n 12 EB vertegenwoordigde, soit 12.10^{18} bytes. Als beide schattingen juist zijn, betreft het grofweg een driehonderdvoud over een termijn van twintig jaar.[67]

De moeilijkheid met betrekking tot de kwalificatie van persoonsgegevens onder de vorm van data maakt deze daarom niet minder hanteerbaar in het recht. Bij gebrek aan daadwerkelijke erkenning van eigendomsrechten op data, is het evenwel mogelijk een privaatrechtelijke oplossing te verzinnen voor een grote meerderheid van de met een vermogensrechtelijke kwalificatie nagestreefde doelstellingen.[68] [69]

Daarbij zou in het bijzonder voor de persoonsgegevens een eigendomsrechtelijke benadering onverzoenbaar zijn met de richtlijn. Voornamelijk omdat laatste een uitsluiting van het absoluut beschikkingsrecht veronderstelt en daarboven als een beschermingsregeling ten gunste van de zwakkere partij is opgesteld, lijkt een uitoefening van de klassieke, erga omnes geldende eigendomsrechten niet mogelijk met betrekking tot de persoonsgegevens. Daarboven komt dat de contractuele vrijheid met betrekking tot persoonsgegevens niet alleen door de indirecte

[65] T.F.E. TJONG TJIN TAI, "Data in het vermogensrecht", *WPNR*, 2015, 2.
[66] EMC, *The digital universe of opportunities*, 2014, 2.
[67] J. ENRIQUEZ, "The data that defines us", CIO winter 2003.
[68] Zie T.F.E. TJONG TJIN TAI, "Privaatrecht voor de homo digitalis: eigendom, gebruik en handhaving", *Homo Digitalis* over vermogensrechtelijke alternatieven in Nederland, waarvan een meerderheid naar analogie in België toepassing kunden vinden. Infra worden overigens een aantal andere knelpunten besproken.
[69] Zie ook A. DE BOIS, *Economisch gebruik van persoonsgegevens in België: Hoe beïnvloedt de (nieuwe) gegevensbescherming de vrijheid van ondernemen?*, VUB, 2017, annex 'Persoonsgegevens als software'.

werking van de richtlijn zelf beperkt is, maar ook door bijvoorbeeld de privacybeschermende regeling.[70]

Voor een aantal persoonsgegevens is het gemakkelijk te stellen dat er hoe dan ook geen enkele vorm van zakelijk recht op kan worden uitgeoefend. Bijvoorbeeld omdat het de productie van bepaalde gegevens niet noodzakelijk aan de betrokkene te danken is, dan wel omdat het niet wenselijk is dat die er bij uitsluiting over zou kunnen beschikken. Zo kan onmogelijk een 'eigendom' of naburig recht worden geclaimd op bijvoorbeeld een strafblad of kredietgeschiedenis.[71]

Los van de discussie over de vermogensrechtelijke kwalificatie is het bovendien voor een aantal strikt relationele persoonsgegevens geen sinecure om te bepalen wie over de rechten (welke dan ook) met betrekking tot die gegevens beschikt. Zo is het bijvoorbeeld voor discussie vatbaar wat er mag gebeuren met groepsfoto's of nog relatienetwerken als persoonsgegevens.[72]

III.2 §5. Persoonsgegevens als onderdeel van een gegevensbestand of dataset

Verschillende gegevens met betrekking tot eenzelfde betrokkene vormen een *record*. Dit record bestaat dus uit een reeks *waarden* (bv '2017') voor bepaalde *attributen* (bv 'jaar'). Een verzameling van records (of ongestructureerde gegevens) wordt een *dataset* genoemd. Gestructureerde datasets kunnen de vorm aannemen van een tabel, maar ook bijvoorbeeld een grafiek.[73]

Artikel 1 §3 PW maakt gewag van een *bestand* wanneer het gaat over een:

''… gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd dan wel gedecentraliseerd is of verspreid op een functioneel of geografisch bepaalde wijze.''

Wanneer (persoons)gegevens het voorwerp uitmaken van een systematische of methodische ordening waarbij ze afzonderlijk toegankelijk zijn (i.e. bestand naar het WER), spreken we volgens het WER van een *databank* (I.12,6°).[74]

III.3. Moderne context verwerking

Het is vanzelfsprekend dat de toegenomen opslag- en verwerkingscapaciteit van computers een enorme weerslag heeft op de omgang met data. Deze kunnen vandaag veel gemakkelijker en

[70] N.N. PURTOVA, *Property rights in personal data: A European perspective*, Oisterwijk, BOXPress, 2011, 211-212.
[71] WEF, *Personal Data: The emergence of a new asset class*, 2011, 16.
[72] M. HILDEBRANDT, *Privacy en identiteit in slimme omgevingen*, 2010, 4.
[73] Advies (WP29) over anonimiseringstechnieken, 10 april 2014, 5/2014, 13.
[74] Onder deze vorm vallen de gegevens als inhoud van de databank binnen de werkingssfeer van de sui-generisbescherming van het WER wanneer dit het product van een substantiële investering uitmaakt (XI.306). Zo de vormgeving of uitdrukking van de databank een intellectuele schepping uitmaakt, valt de databank onder de auteursrechtelijke bescherming (XI.186). Dit is van belang voor de producent van de databank.

op ongeziene schaal worden verwerkt.[75] Naast de verwerking binnen de computer zelf is daarboven de communicatie onderling sterk geëvolueerd. Data worden dus ook gemakkelijker vervoerd over het internet. Zo heeft *cloud-computing* het licht gezien. Hierbij wordt data niet langer opgeslagen of verwerkt op een lokale eenheid, maar op een 'cloud' ('ergens' op het internet). Uit een samenspel van enerzijds deze verbetering van de communicatietechnologie en anderzijds de evolutie naar steeds krachtigere, kleinere computers (niet alleen smartphones, maar in de toekomst elk denkbaar voorwerp, inclusief bijvoorbeeld sportschoenen), ontstaat wat '*the internet of things*' wordt genoemd. De digitale samenleving bestaat in steeds toenemende mate uit een netwerk van allerhande kleine, zelfstandige computers die allemaal eigen data genereren, verwerken en met elkaar uitwisselen. Aan het concept is wellicht een element 'intelligentie' verbonden. Wanneer deze onderling verbonden slimme computers het gedrag van mensen monitoren en hun output daaraan aanpassen spreken we van de '*ambient intelligence*'. In een doorgetrokken visie hiervan wordt randapparatuur (toetsenborden, zelfs knoppen in het algemeen) overbodig door de monitoring en verwerking van de computers.[76]

We spreken van 'big data' wanneer we wijzen op de gigantische volumes data van allerhande aard die vandaag worden gegenereerd door uiteenlopende bronnen. Daarbij hoort te worden benadrukt dat het concept eveneens slaat op de complexiteit van de gegevens en eisen van verhoogde verwerkingscapaciteit en modernisering van de verwerkingstechnieken dat dit met zich meebrengt.[77] Deze data worden vandaag niet langer uitsluitend via expliciete query's verzameld (enquetes, formulieren,…) maar worden voor een groot deel passief gecreëerd - denk maar aan cookies, maar ook het algemenere concept van het internet der dingen - en geïnfereerd (deductie onbekend uit bekende gegevens).[78]

De volumes data (big data) die worden verwerkt en de versnipperde aard van deze opslag en verwerking (cloud computing) maken ondoorzichtig welke data er exact opgeslagen zijn en hoe deze worden aangewend. In deze overvloed aan data bestaat de uitdaging voor diegene die deze wil interpreteren er in de informatie te extraheren uit het ruis. Met profileringstechnieken worden verbanden gelegd binnen deze massa persoonsgegevens om tot zinvolle correlaties en conclusies te komen.[79] In art 4 AVG wordt '*profilering*' gedefinieerd.

---

[75] A. SANDBERG & N. BOSTROM, *Whole Brain Emulation: A Roadmap, Technical Report*, Oxford University, 2008, 81-96.

[76] P. KLEVE, *Juridische iconen in het informatietijdperk,* Kluwer, 2004, 61-66, T.F.E. TJONG TJIN TAI, "Privaatrecht voor de homo digitalis: eigendom, gebruik en handhaving", *Homo Digitalis*, Kluwer, 2016, 249-250, N.N. PURTOVA, *Property rights in personal data: A European perspective*, Oisterwijk, BOXPress, 2011, 17-21, Working document (EC) Advancing the Internet of Things in Europe, 19 april 2016, SWD(2016) 110 final, 4, M. HILDEBRANDT & B.J. KOOPS, "The Challenges of Ambient Law and Legal Protection in the Profiling Era", *TMLR*, 2010, 430-431.

[77] Communication (EC) Towards a thriving data-driven economy, 2 juni 2014, COM(2014) 442 final, 4, E. WILDER-JAMES, *What is big data? An introduction to the big data landscape*, 11 januari 2012, <<www.oreilly.com/ideas/what-is-big-data>>, Gartner IT glossary, big-data: <<http://www.gartner.com/it-glossary/big-data>>.

[78] WEF, *Unlocking the Value of Personal Data: From collection to usage*, 2013, 7-8, CMA, *The Commercial Use of Consumer Data*, juni 2015, 6-7.

[79] M. HILDEBRANDT, "Defining Profiling: A New Type of Knowledge?", in M. HILDEBRANDT & S. GUTWIRTH (Eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer, 2008, 29-30.

Profilering betreft vaak een toepassing van inferentie op persoonsgegevens. Deze inferentie brengt met zich mee wat een 'inferentieprobleem' wordt genoemd, wanneer het gededuceerde gegeven eigenlijk van vertrouwelijke aard is.[80] In een Big Data context zal profilering weliswaar eerder een kwestie van abductie (meest logische verklaring) uit kruising van empirisch vergaarde gegevens betreffen, wat net tegenover inferentie staat.

Dit inferentieprobleem wordt aangescherpt wanneer de profilering gebeurt door lerende computersystemen[81], waarbij zowel de inferentie zelf als de eraan verbonden gevolgen onvoorspelbaar worden.[82]

De regulering heeft volgens het World Economic Forum (WEF) de neiging achter te lopen op de modernisering van dataverwerking, wat zorgt voor een kloof tussen de gevestigde modellen die onderworpen zijn aan een toezicht en de nieuwe spelers die aan de grens van het legale opereren om de facto dit toezicht en de verantwoordelijkheid omzeilen.[83]

Weliswaar is de AVG een tamelijk progressief stuk. Op verschillende vlakken heeft de nieuwe regeling zelfs wat voorsprong geboekt ten aanzien van de praktijk [infra]. Zo zien we bijvoorbeeld een onderdeel inzake profilering waarbij wordt uitgegaan van een principieel verbod van de toepassing van profilering als automatische verwerkingstechniek op natuurlijke personen[84] en bijhorende informatieplichten wanneer dit krachtens een van de uitzonderingen op het verbod toch gebeurt.[85] Daarnaast voorziet de AVG tevens de mogelijkheid voor NGO's om gemandateerd te worden inzake privaatrechtelijke aansprakelijkheid. Het gaat hier eigenlijk om een soort class-action.[86] Er kan uiteindelijk tevens worden verwezen naar het recht op overdraagbaarheid, het recht op minstens even gemakkelijke intrekking als mededeling van de toestemming en het recht om een elektronische kopie op te vragen van aangeleverde gegevens.

De big data maken het nodig moderne technieken te hanteren voor het omzetten van deze data naar informatie. Profilering, in het bijzonder wanneer deze door lerende computers wordt gedaan, zorgt voor onzekerheid met betrekking tot wat de gegevens betekenen en wat er mee gebeurt. In het 'internet der dingen' (en later de 'ambient intelligence' wereld) is er daarbij een sterke aanwezigheid van kleine, slimme computers die zelf data verwerken (of via intermediare servers zoals bij fog- en edge computing) en onderling uitwisselen, wat de zaak des te delicater maakt. Met deze ontwikkelingen ontstaat een toegenomen risico op schade door persoonsgegevens, maar wordt daarbij ook de potentiële schade sterk geïntensifieerd. Het is onder meer met oog op deze context dat het kader wordt besproken.

[80] C. DWYER, *The inference problem and persuasive computing*, Pace University, 4.
[81] Zie A. DE BOIS, *Economisch gebruik van persoonsgegevens in België: Hoe beïnvloedt de (nieuwe) gegevensbescherming de vrijheid van ondernemen?*, VUB, 2017, annex 'Lerende computers'.
[82] M. HILDEBRANDT, *Privacy en identiteit in slimme omgevingen*, 2010, 9.
[83] WEF, *Personal Data: The emergence of a new asset class*, 2011, 18.
[84] Art. 22 AVG.
[85] Art. 13, f AVG.
[86] Art. 80, 1 AVG.

IV. Waarde van- en schade door persoonsgegevens:

IV.1. Economische waarde

Voor de exploitanten is de materiële waarde van persoonsgegevens in te schatten met een blik op de markt. In wat zich vandaag ontwikkelt en kan worden omschreven als een 'aandachtseconomie', wenden ondernemingen persoonsgegevens aan om efficiënter op te treden binnen de markt, vraag te stimuleren, banden te scheppen of gewoon rechtsreeks omzet te creëren.[87]

De gegevens die economisch aangewend worden, omvatten onder meer de digitale identiteit ('aanspreekpunt': gsmnummer, e-mail adres…), relatienetwerken, communicatie (logs, posts,…), media (foto's, video's,…), gedrag (voorkeuren, verplaatsingen, activiteit,…), financiële, institutionele en gezondheidsdata.[88]

De data worden door bedrijven verzameld door middel van cookies, clicks, query's, profielen, trackers, gezichtsherkenning en uiteraard onderlinge handel in gegevens.[89]

Ondernemingen proberen hun marktoptreden te verbeteren door middel van data analyse. Data worden zo aangewend ten einde doelgerichte advertentie te creëren, consumenten te analyseren (en risico's te evalueren), ondernemingsstrategieën aan te passen, producten en diensten te verbeteren en deze uiteindelijk op maat van de consument aan te bieden (onder meer door op maat te communiceren).[90]

Daarnaast bestaan ondernemingsmodellen waarvan het verwerken van gegevens een centrale activiteit vormt. Dit omvat onder andere ondernemingen die data verzamelen, examineren of verhandelen. Hierbinnen kan een ruime scheiding worden gemaakt tussen de handelaars in *data* en deze in *informatie*/*kennis*, waarbij het aanbod van de eerste soort rauwe data zonder betekenis bevat, terwijl de laatsten geïnterpreteerde gegevens verhandelen. De informatie kan het product van een beschrijvende, voorspellende of nog voorschrijvende analyse zijn.[91]

Dit soort ondernemingen zijn de zogenaamde 'databrokers'. Deze ondernemingsmodellen steunen hoofdzakelijk op het verhandelen en verwerken van gegevens die in beginsel niet bij de betrokkenen zelf werden verzameld. Naast het verhandelen van rauwe gegevens of specifieke sets (bijvoorbeeld: een bepaald gegeven over een bepaalde leeftijdsgroep in een bepaalde regio), doen deze ondernemingen ook aan zekere profielhandel. Het delicate aspect in verband met dit soort activiteiten ligt voornamelijk bij de doelbinding en toestemmingsvereiste.[92]

Records persoonsgegevens worden verhandeld aan prijzen variërend tussen de paar duizendsten van een cent en de paar euro per stuk. Factoren zoals het eigen vermogen, familiale toestand en het reeds gekend zijn van bepaalde gegevens, beïnvloeden sterk de marktwaarde van

[87] WEF, *Personal Data: The emergence of a new asset class*, 2011, 8.
[88] Ibid, 13-14, CMA, *The Commercial Use of Consumer Data*, juni 2015, 24-25.
[89] <<www.baynote.com/infographic/big-brother-is-a-tech-company/>>.
[90] CMA, *The Commercial Use of Consumer Data*, juni 2015, 50.
[91] P.M. HARTMANN, M. ZAKI, N. FELDMANN, & A. NEELY, *Big Data for Big Business? A Taxonomy of Data-driven Business Models used by Start-up Firms*, University of Cambridge: Cambridge Service Alliance, Cambridge, 2014, 9.
[92] Upturn, *Data brokers in an open society*, 2016, 5, 12 & 23.

persoonsgegevens van de betrokkenen. Voor een tamelijk volledig gegevensrecord bestrijkende zowel burgerlijke gegevens als interesses en economisch gedrag, is de waarde per e-mailadres gemiddeld ongeveer 7 cent.[93]

De ontwerprichtlijn met betrekking tot contracten over digitale inhoud handelt onder meer over diensten die worden verleend in ruil voor persoonsgegevens en de voorwaarden waaraan zulke ruil moet voldoen. Dit wijst alvast op een erkenning door de Commissie van de persoonsgegevens als betaalmiddel. Daartegen zegt dit niets over de doorspeling van deze gegevens aan derden.[94]

Als grondslag voor economische activiteiten waarbij persoonsgegevens worden verhandeld zou, bij gebrek aan een expliciet verbod (en gezien de voorwaarden en beperkingen die de AVG stelt, a contrario), in de eerste plaats kunnen worden gegrepen naar de vrijheid van ondernemen en daarbij begrepen de contractuele vrijheid. Waar persoonsgegevens een in geld waardeerbaar goed zijn en contracten daarover prima facie in overeenstemming met artikelen 1128 en 1129 BW zijn, zou hier geen bezwaar tegen lijken te bestaan. Daartegen is hier een delicaat element bij betrokken wat betreft de toestemming van de betrokkene. Zonder de verhandeling van persoonsgegevens expliciet toe te staan of te verbieden (weliswaar zal deze verhandeling een verwerking uitmaken, met alle geldigheidsvoorwaarden daaruit voortvloeiend), verplicht artikel 13 AVG wel tot het spontaan informeren van de betrokken over alle ontvangers van de gegevens en de doeleinden van de verwerking. Uitgaande van een expliciete, geïnformeerde toestemming, zou in principe de praktijk van het verhandelen van persoonsgegevens alvast toegelaten zijn. Daarnaast voorziet de beschermingsregeling nog heel wat maatregelen inzake de verhouding tot die ontvangers, bijvoorbeeld inzake de verplichte melding aan derden van rectificatie of uitwissing. Doch is dan moeilijk verzoenbaar met artikel 7 en overweging 32 AVG, de doorgifte van persoonsgegevens aan ontvangers voor wiens verwerkingsdoel geen expliciete en geïnformeerde toestemming werd gegeven. Als dusdanig is naar de tekst in principe de handel van persoonsgegevens de facto slechts toegelaten voor zover de gegeven toestemming zowel de doorgifte als het verwerkingsdoel van de ontvangers bestrijkt. Evenwel is de vereiste van geïnformeerde toestemming uit de overweging niet even uitdrukkelijk omschreven in artikel 7. Anderzijds kan hiervoor eventueel worden gegrepen naar de nieuwe vereiste van transparante communicatie.

In principe belet de tekst niet dat deze verwerkingen zouden plaatsvinden op grond van het gerechtvaardigde (economisch) belang uit artikel 6, f AVG, zolang maar aannemelijk wordt gemaakt dat dit zwaarder doorweegt dan de gegevensbescherming. Merk op dat een belang vrij

[93] Financial Times, personal data value simulator: http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html?ft_site=falcon#axzz4aGWxpsRQ, Towerdata batch estimate: http://intelligence.towerdata.com/pricing-append.

[94] Art. 13 voorstel richtlijn digitale inhoud.

gemakkelijk als gerechtvaardigd zal worden beschouwd, maar daarom niet per se doorslaggevend zal zijn ten opzichte van de rechten van de betrokkene.[95]

Alternatief worden de gegevens niet rechtsreeks doorgespeeld aan derden, maar wordt het voordeel van de toegepaste profilering slechts indirect aan de 'gebruikers' gegund. Zo zal het bieden van adverteerruimte binnen een website het voordeel van gerichte reclame kunnen bieden zonder dat de gegevens bij een andere verantwoordelijke terechtkomen.

Waar de handel in persoonsgegevens voortbouwt op consumentencontracten, zijn tevens te beschouwen de voorwaarden gesteld door het WER inzake deze contracten, meer bepaald de transparantievereisten. De omschrijving van de draagwijdte van de toestemming voor het gebruik van de persoonsgegevens (onder meer het doorspelen aan andere actoren) zal dan eng genoeg moeten zijn om geen onrechtmatig beding uit te maken.[96]

Volgens de halfjaarlijkse voorspelling van IDC zou de wereldwijde omzet van alle goederen en diensten in Big Data en Business analyse evolueren van 122 miljard dollar in 2015 naar 187 miljard dollar in 2019.[97]

Voor de betrokkenen is de materiële waarde van persoonsgegevens een kwestie van persoonlijke invulling. Er zal door de een gemakkelijker dan door de ander worden toegegeven aan een ruil van deze gegevens tegen geringere diensten of kortingen. Een prijs zal er dan op geplakt worden wanneer de betrokkene instemt met de ruil. Het is daarbij tamelijk alarmerend hoe snel wordt ingegaan op zo'n voorstel.[98] Zo valt bijvoorbeeld te wijzen op de 1.8 miljard gebruikers[99] van Facebook, waarvan de CEO een vooraanstaand figuur van het technologisch determinisme (i.e. technocratische invulling) ten aanzien van privacybegrip is.[100]

Daarnaast heeft de gekendheid van sommige data een al dan niet rechtsreekse weerslag op het vermogen van de betrokkene (bijvoorbeeld tarieven van verzekeraars of kredietgevers).

Idealiter wordt er gestreefd naar een transparantie over de waarde van persoonsgegevens, zodat de betrokkenen hierover meer inzicht krijgen en geïnformeerd instemmen. Bepaalde toekomstvisies spreken zelfs over persoonsgegevens als een betalingseenheid.[101]

---

[95] Advies (WP29) over het begrip "gerechtvaardigd belang van de voor de gegevensverwerking verantwoordelijke" in artikel 7 van Richtlijn 95/46/EG, 9 april 2014, 06/2014, 30.
[96] Advies (COB) over de algemene voorwaarden van sociale netwerksites, 16 december 2015, COB 38, 30.
[97] IDC, *Worldwide Big Data and Business Analytics Revenues Forecast to Reach $187 Billion in 2019, According to IDC*, 23 mei 2016, <<www.idc.com/getdoc.jsp?containerId=prUS41306516>>.
[98] V. SAGAERT & D. SCHEERS, "De relatieve waarde van privacy", *RW*, 2014.
[99] <<www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>>.
[100] M. HILDEBRANDT, et al. (Eds.), *Digital Enlightenment Yearbook 2013*, IOS Press, 2013, 13.
[101] WEF, *Personal Data: The emergence of a new asset class*, 2011, 10.

IV.2. Persoonlijke waarde

Voor de betrokkene hebben persoonsgegevens op zich een zekere extrapatrimoniale waarde. Zo bestaat er bijvoorbeeld een niet in geld waardeerbare gebruikswaarde van bepaalde persoonlijke data, zoals het genot bij het terugkijken naar persoonlijke foto's en video's.[102]

Persoonsgegevens hebben daarnaast een veel belangrijkere extrapatrimoniale waarde als onderdeel van de identiteit. In een negatieve formulering hebben zij waarde in de mate dat de controle over de persoonsgegevens controle over de constructie van de identiteit meebrengt. In die optiek valt de waarde van persoonsgegevens eerder samen met de waarde van privacy met daarin begrepen de waarde van identiteit. De controle over de veruitwendiging van de identiteit heeft betrekking op meerdere belangen van de betrokkene.

In eerste instantie heeft elke betrokkene graag controle over de presentatie van zijn identiteit binnen verschillende sferen. De selectieve bekendmaking van gegevens staat toe zijn beeld aan te passen aan de verwachtingen en bepaalde gevolgen uit te lokken of te vermijden.[103]

Zo zal in een professionele sfeer altijd een andere identiteit worden gepresenteerd dan in bijvoorbeeld een vriendschappelijke kring. In zekere mate kan dit zich uiteindelijk vertalen in pecuniaire gevolgen. Het lekken van data kan in dit opzicht leiden tot zeer verstrekkende gevolgen voor de betrokkenen, gaande van de uitsluiting van bepaalde groepen of voordelen (eventueel door blacklisting in gemeenschappen) tot het verlies van een job.[104]

Met de Amerikaanse Sweet v Linkedin zaak werd ook mooi geïllustreerd hoe de verwerking van persoonsgegevens die de facto afbreuk doet aan de privacy verregaande gevolgen voor het professionele leven kan meebrengen. In deze casus werd weliswaar niet veroordeeld de praktijk van Linkedin die erin bestond aan premium leden toe te laten zonder enige kennisgeving aan of toestemming van de betrokkenen van laatsten een lijst (potentiële) betrouwbare referenties in te kijken (zonder weliswaar zelf informatie over de referentie mee te geven). Het hof oordeelde zo in het licht van het doel van LinkedIn, onderstrepende dat de gegevens met het oog op de publicatie ervan vrijwillig werden medegedeeld, alsook het gebrek aan bewijs dat de medegedeelde informatie effectief werd aangewend ter selectie van kandidaten. Opmerkelijk beschouwde het hof de aanbrenging van 'potentiële referenties' niet als de mededeling van persoonlijke informatie zoals onder de FCRA.[105] Dit laatste werpt toch de vraag op naar het statuut van strikt relationele gegevens (d.i. die zuiver ontstaan door de interactie tussen verschillende betrokkenen, zoals groepsfotos of vriendenlijsten op sociale netwerken), althans voor wat betreft de Verenigde Staten.

Wanneer gelekte data bijzonder gevoelig zijn (bijvoorbeeld een seksvideo), kan dit een permanente beschadiging van de eer en goede naam met zich meebrengen. Met de mogelijkheid

[102] T.F.E. TJONG TJIN TAI, "Privaatrecht voor de homo digitalis: eigendom, gebruik en handhaving", *Homo Digitalis*, Kluwer, 2016, 255.
[103] M. HILDEBRANDT et al. (Eds.), *Digital Enlightenment Yearbook 2013*, IOS Press, 2013, 14.
[104] Ibid, 4.
[105] USDC (N.D. Cal.) 14 april 2015, Case No. 5:14-cv-04531-PSG, Sweet/Linkedin Corp, 58-62, 94, 102.

anoniem te posten op het internet is de aanpak van dergelijke situaties overigens bijzonder moeilijk geworden.[106]

Nog zorgwekkender kunnen de gevolgen van zo'n lek met betrekking tot de veiligheid van de betrokkene zijn. Zo kunnen persoonsgegevens misbruikt worden ten einden van identiteitsfraude, inbraak of nog chantage. Algemener kunnen gelekte persoonsgegevens zorgen voor een asymmetrie van informatie die in uiteenlopende situaties weerslag kan hebben. Materiële en immateriële schade hierdoor kan zich voordoen in private verhoudingen (bijvoorbeeld contractuele), maar het is ook denkbaar dat dit eerder publieke belangen schaadt (zoals het recht op eerlijk proces).[107]

In een commerciële sfeer heeft de gepresenteerde identiteit eveneens gevolgen voor de betrokkene. Ondernemingen verzamelen en verwerken persoonsgegevens om onder meer efficiënter hun aanbod te presenteren en algemener op maat om te gaan met klanten. Hierbij worden heel wat geïnfereerde data gecreëerd in de vorm van profielen en statistieken. Dit kan echter leiden tot al dan niet juiste labelling waarvan de betrokkene niet wil weten. Door bijvoorbeeld een opzoeking te doen of een bestelling voor iemand anders te plaatsen, kan langdurig ongewenste reclame verschijnen in een browser.[108]

Naast dit externe aspect van de identiteit, heeft de bekendheid van persoonsgegevens ook een impact op eerder interne processen. Bedrijven wenden zoals gezegd de persoonsgegevens aan om een activiteit op maat van de consument aan te bieden, maar voorbij het onschuldigere aanbod op maat 'voor het comfort van de consument', kan het hierbij eveneens gaan over *nudging*. Dit houdt in dat het in werkelijkheid gaat over manipulatie van het keuzeproces van het individu.[109]

Verder is deze targeting (of nudging) niet beperkt tot de economische sfeer en komt de autonomie van het individu in het gedrang door de profilering op basis van persoonsgegevens. In de mate dat de betrokkene in een op maat gemaakte wereld leeft, wordt de realiteit aan hem onttrokken. Dit houdt op een dieper niveau in dat de 'ware' identiteit wordt aangetast wanneer de informatie selectief aan de betrokkene wordt meegedeeld op basis van zijn profiel.[110]

Uiteindelijk moeten deze risico's nogmaals gekaderd worden in het ondoorzichtige landschap waarbinnen de persoonsgegevens worden verwerkt. Volgens de EuroBarometer report over databescherming van 2015 zou één op drie Belgen het gevoel hebben absoluut geen controle te hebben over zijn persoonsgegevens.[111]

---

[106] T.F.E. TJONG TJIN TAI, "Privaatrecht voor de homo digitalis: eigendom, gebruik en handhaving", *Homo Digitalis*, Kluwer, 2016, 281.
[107] T.F.E. TJONG TJIN TAI, "Aansprakelijkheid bij datalekken", *WPNR*, 2016, 6-8, N.N. PURTOVA, *Property rights in personal data: A European perspective*, Oisterwijk, BOXPress, 2011, 52-53.
[108] T.F.E. TJONG TJIN TAI, "Privaatrecht voor de homo digitalis: eigendom, gebruik en handhaving", *Homo Digitalis*, Kluwer, 2016, .279
[109] Ibid, 280.
[110] Ibid, 281, M. HILDEBRANDT, et al. (Eds.), *Digital Enlightenment Yearbook 2013*, IOS Press, 2013, 13.
[111] EC, Special Eurobarometer 431 "Data protection", 2015, 10.

V. Betrokken actoren en hun rol

V.1. Betrokkene

De identificeerbare, natuurlijke persoon waarop de persoonsgegevens betrekking hebben wordt als 'betrokkene' aangeduid.[112] Weliswaar kan onder bepaalde omstandigheden ook door een rechtspersoon beroep worden gedaan op de beschermingsregeling [supra].

Artikel 25, 1 AVG maakt daarnaast gewag van 'personen verbonden aan de verwerking' dat volgens de Engelstalige versie slaat op 'natural persons posed by the processing'.

V.2. Verwerker en verantwoordelijke voor de verwerking

Onder de verwerker wordt verstaan de natuurlijke persoon of rechtspersoon, de overheidsinstantie, de dienst of enig ander orgaan of feitelijke vereniging die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.[113] In het kader van de aansprakelijkheid en verantwoordelijkheid is het belangrijk een onderscheid te maken tussen de verwerker en de verantwoordelijke voor de verwerking.

De verwerkingsverantwoordelijke is de natuurlijke persoon of rechtspersoon, overheidsinstantie, dienst, feitelijke vereniging of enig ander orgaan die/dat, al dan niet alleen het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.[114] Wanneer door meerdere verantwoordelijken gezamenlijk het doel en de middelen worden bepaald, zijn zij naar artikel 26 AVG gezamenlijke verantwoordelijken. In dat geval moeten zij behoudens wettelijke bepalingen hun onderlinge verhouding en deze met de betrokkenen op een transparante wijze regelen (Art. 1 & 2). De betrokkenen kunnen weliswaar elke van deze verantwoordelijken aanspreken met betrekking tot hun rechten (3). Dit houdt dus een hoofdelijke aansprakelijkheid in. De AVG bepaalt ook dat indien de verwerker in strijd met de regeling zelf het doel en de middelen bepaalt, hij, onverminderd de aansprakelijkheidsregeling, als de verantwoordelijke wordt beschouwd.[115]

Onder de geldende regeling ziet de verantwoordelijke toe op de naleving van de technische en organisatorische beschermingsmaatregelen.[116]

De AVG preciseert dat indien de verwerker zelf iemand aanneemt om zijn opdrachten te vervullen, deze tweede verwerker aan dezelfde verplichtingen inzake gegevensbescherming is onderworpen als de eerste verwerker. De eerste verwerker blijft in geval van tekortkomingen van de tweede verwerker wel aansprakelijk ten aanzien van de verantwoordelijke.[117] Er kan overigens enkel met toestemming van (dan wel kennisgeving aan, in geval van algemene

[112] Art. 1,1 PW, 2,a richtlijn & 4,1 AVG.
[113] Art. 1,5 PW, 2,e richtlijn & 4,8 AVG.
[114] Art. 1,4 PW, 2,d richtlijn & 4,7 AVG.
[115] Art. 28, 10 AVG.
[116] Art. 16, §1, 2 PW, 17,2 richtlijn. Art. 16 §1, 1&4 & §4 PW, 17, 1, 2 & 3, 2e streepje en 4 richtlijn, 24, 1&2, 25, 1 & 28, 1 AVG.
[117] Art. 28, 4 AVG.

toestemming) de verantwoordelijke worden overgegaan tot de aanwerving of vervanging van tweede verwerkers.[118] [119]

V.3. Vertegenwoordiger

Hoewel het begrip reeds in de vigerende regeling gehanteerd wordt, is de vertegenwoordiger pas met de AVG wettelijk gedefinieerd als de in de Unie gevestigde natuurlijke persoon of rechtspersoon die schriftelijk door de verwerkingsverantwoordelijke of de verwerker is aangewezen om deze te vertegenwoordigen in verband met zijn verplichtingen.[120]

In artikel 27 AVG worden, verwijzend naar het toepassingsgebied (d.i. lidstaat waar betrokkenen wier gedrag wordt geobserveerd of wier persoonsgegevens in verband met aanbieden van goederen en diensten worden verwerkt) van de verordening, (gelijkaardig aan 3bis, 2° PW uit 4,2 richtlijn) een aanstellingsplicht (1 & 3) en aansprakelijkheid -onverminderd rechtsvorderingen tegen de verantwoordelijke zelf- (5) bepaald, met uitzonderingen op de plicht in geval van kleinschalige, incidentele verwerking van niet-gevoelige gegevens of verwerking door overheidsorganen (2). De AVG bepaalt overigens dat de vertegenwoordiger gemachtigd is naast de verantwoordelijke of de verwerker te worden benaderd door autoriteiten en betrokkenen over aangelegenheden inzake de verwerking (4).

V.4. Functionaris voor gegevensbescherming

Onder de richtlijn werd reeds voorzien dat lidstaten konden bepalen dat het aanstellen van een functionaris voor gegevensbescherming een vrijstelling of vereenvoudiging van aanmeldingsplichten met zich mee kon brengen.[121] Van deze mogelijkheid werd weliswaar geen gebruik gemaakt door de Belgische wetgever.

Met de AVG wordt onder omstandigheden de aanstelling van een functionaris voor gegevensbescherming hoe dan ook verplicht door artikel 37.

In hoofdzaak waakt de functionaris over de naleving van de gegevensbeschermingsregeling en informeert hij de verantwoordelijke of verwerker hierover. Ook inzake de gegevensbeschermingseffectbeoordeling heeft hij een adviserende en monitorende taak. Hij vormt daarnaast ook de link met en is het contactpunt voor de toezichthoudende autoriteit.[122]

De functionaris is onafhankelijk ten aanzien van de verwerker en de verantwoordelijke, maar zij moeten wel meewerken teneinde hem zijn werk te laten verrichten. Laatsten melden hem ook telkens er een aangelegenheid inzake persoonsgegevens zich voordoet en brengen hem agendapunten voor. De functionaris kan tevens aanvullende taken worden toegewezen, zolang

[118] Art. 28, 2 AVG.
[119] Zie A. DE BOIS, *Economisch gebruik van persoonsgegevens in België: Hoe beïnvloedt de (nieuwe) gegevensbescherming de vrijheid van ondernemen?*, VUB, 2017, annex 'Verhouding verantwoordelijke – verwerker'.
[120] Art. 4, 17 AVG.
[121] Art. 18, 2 richtlijn.
[122] Art. 39 AVG.

dit niet tot belangenconflicten leidt. De functionaris is ook een aanspreekpunt voor betrokkenen met betrekking tot de verwerking van hun persoonsgegevens. Hij is vanzelfsprekend tot geheimhouding verplicht.[123]

V.5. Derde

Wordt als derde beschouwd iedereen die niet de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd is om de persoonsgegevens te verwerken is.[124] In principe kan de vertegenwoordiger dus een derde zijn in de mate dat deze niet gemachtigd is persoonsgegevens te verwerken.

Hoewel deze indruk gewekt zou kunnen worden, valt dit begrip niet samen met 'ontvanger'. Laatste is diegene aan wie de gegevens worden meegedeeld, ongeacht of het al dan niet een derde betreft.[125]

V.6. Producent van de databank

Diegene die het initiatief neemt tot en het risico draagt van de investeringen waardoor de databank ontstaan is, wordt als de producent ervan beschouwd.[126]

V.7. Rechtmatige gebruiker van de databank

De persoon die met toestemming van de producent ervan, of op een door de wet toegestane wijze, opvragingen doet of de databank hergebruikt, wordt volgens het WER als een rechtmatige gebruiker beschouwd.[127]

Het naar deze context rechtmatige gebruik van een databank zou nog steeds problematisch kunnen zijn in het kader van de toestemming van de betrokkene.

[123] Art. 38 AVG.
[124] Art. 1, 6 PW, 2, f richtlijn & 4, 10 AVG.
[125] Art. 1 §7 PW, 2, g richtlijn, 4,9 AVG. Noteer dat er een uitzondering is bestaat voor overheden in functie.
[126] Art. I.17, 2° WER.
[127] Art. I.17, 1° WER.

VI. Rechten en plichten van de partijen

VI.1. Rechten van de verantwoordelijke

VI.1 §1. Vrijheid van ondernemen

De handelingen inzake persoonsgegevens die mogen worden gesteld door de verwerker, zijn in principe niet vooraf bepaald. Waar enerzijds de beschermingsregeling toepassing vindt op de verwerking van gegevens, die op zichzelf niet limitatief wordt omschreven, en anderzijds de vrijheid van ondernemen impliceert dat bij gebrek aan conflict met een andere regel elke vorm van monetarisering toegelaten is, zou a fortiori elke handeling kunnen worden toegestaan mits aan de voorwaarden van de regeling wordt voldaan. Gesynthetiseerd komt het proces voor een toegelaten verwerking neer op een aantal stappen. Vooreerst moet worden een afgebakend doel voorgelegd waarbinnen de verwerking plaatsvindt. Indien een verwerking verenigbaar met dat doel is, moet alvorens hiertoe over te gaan, een grondslag voor de verwerking bestaan. Met de AVG wordt in het bijzonder aandacht besteed aan de toestemming als grondslag. Om geldig te zijn, moet deze voortaan aan een aantal extra vereisten voldoen. Na de verwerking in overeenstemming met het besproken doel, steunend op een gerechtvaardigde grondslag, worden de gegevens niet langer bewaard dan nodig is voor dat doel. Indien de verantwoordelijke de gegevens voor een ander doel wenst te gebruiken dan datgeen waarvoor ze werden verzameld, dient steeds een verenigbaarheidstoets te worden gemaakt.

De vrijheid van ondernemen staat op bijzonder gespannen voet met de beperkingen op het hergebruik van gegevens. Er zijn situaties denkbaar waarbij de verwerking voor een herzien doeleind weliswaar niet als verenigbaar met het vorige doel kan worden beschouwd, maar niettemin redelijkerwijs op dezelfde grondslag zou kunnen steunen, bijvoorbeeld waar de toestemming redelijkerwijs op identieke wijze zou zijn gegeven. In deze situaties kan de volledige uitwissing van de database behoorlijk wat schade aan de verwerkende onderneming richten. Weliswaar kunnen geanonimiseerde gegevens in principe vrij worden verwerkt, daar zij niet meer onder het begrip persoonsgegevens vallen, wat de beperkingen inzake doel uitschakelt.

Wat betreft het verhandelen van persoonsgegevens, is te stellen dat dit bij gebreke van een gerechtvaardigd belang (f-grond)[128] toegestaan is in de mate dat dit steunt op de toestemming van de betrokkene. In dit verband zou het misbruik van algemene, vage toestemmingen zich naar de toekomst sterk ingeperkt zien. Ten eerste omdat de AVG de toestemmingsvereiste enorm heeft aangescherpt. Daarnaast kan de toestemming ook geneutraliseerd worden door gebreken op een aanvullende informatieplicht inzake consumentencontracten. De kritiek van de COB zou daarbij ook de wetgever moeten triggeren omtrent de nauwkeurigheid van de informatieplicht (bijvoorbeeld vage omschrijvingen van ontvangers zoals 'partners' verbieden). Er kan tevens opnieuw worden verwezen naar de nieuwe transparantievereiste inzake communicatie.

[128] Overigens valt op te merken dat de rechtspraak dit erkent, maar niet snel andere belangen laat doorwegen op deze van de betrokkenen. Zie HvJ 13 mei 2014, C-131/12, Google/Spain, 73-74. In casu ging het indirect om een economisch belang dat weliswaar niet tekort schoot aan de f-grond, maar geen voldoende tegengewicht vormde.

Alternatief aan de directe verhandeling van persoonsgegevens, kan bij gebreke aan toestemming hiertoe, met een gelijkaardig effect worden gemonetariseerd. Bijvoorbeeld: door het verkopen van doelgerichte adverteerruimte binnen Facebook, slaagt de website er in zijn profilering ten dienste van derden te stellen zonder dat de gegevens bij laatsten terechtkomen. Een ander alternatief hiertoe, zou bestaan in de verhandeling van gepseudonimiseerde gegevens die tevens geanonimiseerd zijn. Weliswaar is laatste toevlucht risicovol voor de onderneming in die zin dat de rechter nog steeds kan aannemen dat er geen sprake is van (toereikende) pseudonimisering.

VI.1 §2. Bescherming databank

De verantwoordelijke als producent van de databank wordt enerzijds beschermd door het auteursrecht waar het gaat om de uitingswijze van de databank en anderzijds door het sui-generis recht inzake databanken. Steunend op dit sui-generisrecht kan de verantwoordelijke de opvraging of het gebruik van de databank geheel of ten dele verbieden.[129] Hieromtrent zijn een aantal opmerkingen te maken. Vooreerst valt de inhoud van een databank slechts onder deze bescherming wanneer de exploiterende onderneming in de EU gevestigd is.[130] Ook is het moeilijk houdbaar dat het uitputtingsbeginsel neergelegd in artikel XI.307 enige uitwerking kan hebben inzake persoonsgegevens. Andersom bekeken, zou men kunnen stellen dat de bescherming van databanken ergens wordt aangevuld door de persoonsgegevensbescherming. In de praktijk zou deze situatie zich uitwerken door een gesplitste bescherming van de inhoud van de databank, waarbij de persoonsgegevens als inhoud van de databank in het belang van de betrokkenen aanvullend wordt beschermd door de specifieke beschermingsregeling, hoewel dit uiteindelijk ook een zekere bescherming voor de producent met zich meebrengt. Anderzijds is de betrokkene ten aanzien van de producent een rechtmatige gebruiker in de zin van het WER voor zover zijn handelingen steunen op de beschermingsregeling inzake persoonsgegevens, wat dan weer de grip van de producent over de inhoud van de databank vermindert, al zeker in het licht van het nieuwe recht op overdraagbaarheid van gegevens [infra].

VI.2. Plichten van de verantwoordelijke (en verwerker)

VI.2 §1. Beginselen voor de verwerking

De verwerking is in de formele regeling onderworpen aan een aantal beginselen. Een meerderheid van deze principes vinden direct hun grondslag in artikel 8,2 van het Handvest. Voor de andere kan worden verwezen naar het eerste lid van artikel 8, eventueel in samenlezing met het algemene recht op privacy.

Het is onder de AVG aan de verwerkingsverantwoordelijke aan te tonen dat de beginselen inzake verwerking worden nageleefd. Voorheen werd de verantwoordelijkheid rond het beginsel van

[129] Art. XI.307 WER.
[130] Art. XI.315 WER.

vertrouwelijkheid en integriteit gezamenlijk gedragen door de verantwoordelijke, de verwerker en eventueel de vertegenwoordiger.

a. Eerlijke verwerking:

In de eerste plaats zal de verwerking ten aanzien van de betrokkene behoorlijk ('eerlijk') en rechtmatig moeten zijn.[131]

In artikel 5, 1, a AVG worden aan de verwerking eisen van rechtmatigheid, behoorlijkheid en transparantie opgelegd. De Engelstalige versie van zowel de richtlijn als de AVG spreken van 'fairness', waardoor klaarblijkelijk de nieuwe invulling 'behoorlijkheid' wordt gegeven aan het begrip.

b. Transparantie

De AVG voegt aan deze algemene beginselen een vereiste van transparantie toe.[132] De transparantieplicht is in het kader van consumentencontracten tevens terug te vinden in de artikelen VI.37 j° VI.84 WER.

De toegangkelijkheidsvereiste uit 8 Handvest zou ruimer kunnen geïnterpreteerd worden als een transparantievereiste. Deze transparantie omvat dan naast de toegankelijkheid (als in 'inzage') zelf ook bepaalde informatieplichten en transparantievereisten met betrekking tot de communicatie (in de AVG).

Informatieplichten

Er wordt zowel in de wet als in de AVG een onderscheid gemaakt tussen de informatieplicht wanneer de gegevens rechtsreeks bij de betrokkene zelf worden verzameld[133] en wanneer dit niet het geval is.[134] Daarnaast bestaat ook een meldingsplicht ten aanzien van de betrokkene ingeval van inbreuken in verband met persoonsgegevens.

Rechtstreeks

De AVG hanteert een onderscheid tussen mee te delen informatie onder het eerste en tweede lid van artikel 13. Dit artikel verruimd in beide luiken de draagwijdte van de mededelingsplichten.

De informatie uit dit eerste lid moet in beginsel, op deze betreffende de doeleinden na, enkel bij de verzameling van de gegevens worden gemeld.[135]

De informatie vermeld in het tweede lid van artikel 13 zal moeten worden meegedeeld telkens er een voornemen is de gegevens te verwerken voor een ander doel dan hetgeen waarvoor ze werden verzameld (3). Hoe dan ook gelden beide informatieplichten niet voor de informatie

[131] Art. 4, 1° PW & 6, 1, a richtlijn.
[132] Art. 5, 1, a AVG.
[133] Art. 9 §1 PW, 10 richtlijn & 13 AVG.
[134] Art. 9§2 PW, 11 richtlijn & 14 AVG.
[135] Art. 13, derde lid *a contrario*.

waarover de betrokkene reeds beschikt (4). Artikel 21, 4 vereist daarboven dat het recht op bezwaar uitdrukkelijk en afzonderlijk ter aandacht van de betrokkene moet worden gebracht reeds bij het eerste contact.

Onrechtstreeks

Artikel 14 AVG maakt opnieuw een onderscheid tussen de gegevens die al (tweede lid) dan niet (eerste lid) moeten worden verstrekt bij de verwerking voor een ander doel dan dat waarvoor de gegevens verzameld werden. Opnieuw moet hoe dan ook het doel steeds meegedeeld worden.

In dit verband valt kort te wijzen op de situatie waarbij ondernemingen in beginsel toestemming vragen om voor andere (vaag omschreven) doeleinden te verwerken dan hetgeen waarvoor de gegevens werden verzameld, in zoverre geen beroep op anonimisering wordt gedaan om de regeling buiten spel te zetten.[136] Voortaan zal dit beperkt worden door de verzoenbaarheidstoets en daarboven helder moeten worden gecommuniceerd aan de betrokkene.

Artikel 14, eerste lid verschilt van het eerste lid van artikel 13 enkel door de vermelding van de categorieën persoonsgegevens (d) in plaats van het gerechtvaardigde belang. Ook het tweede lid is sterk gelijklopend met dat van artikel 13.

Artikel 14, derde lid preciseert daarboven het tijdstip waarop de informatie moet worden verstrekt.

De uitzonderingen op de informatieplicht in artikel 14 zijn dezelfde drie als deze die terug te vinden zijn in artikel 9 §2 van de Privacywet met daarnaast een uitzondering in geval van beroepsgeheim (d).

Toegang

De Privacywet neemt niet letterlijk de benaming van het recht van toegang uit artikel 12 richtlijn over, maar omschrijft wel een gelijkaardige inhoud in artikel 10.

Dit recht op toegang kan onder bepaalde omstandigheden worden beperkt. Ten eerste stelt overweging 41 van de richtlijn dat met het oog op de bescherming van het zakengeheim of de intellectuele eigendom, er in mate kan worden geweigerd informatie mee te delen over bijvoorbeeld de logica van de (geautomatiseerde) verwerking. Hierbij wordt dus alvast een afweging gemaakt tussen het auteursrecht en de eigendomsrechten enerzijds en de gegevensbescherming anderzijds. Daarnaast wordt in de wet gepreciseerd dat de mededeling in verband met medische gegevens kan worden uitgesteld in het kader van medisch-wetenschappelijk onderzoek (hierbij denkt men dan aan dubbelblind onderzoek).[137] Uiteindelijk hoeft ook geen gevolg te worden gegeven aan een verzoek kort volgend op een eerdere kennisgeving over persoonsgegevens.[138]

[136] M. HILDEBRANDT, *Profile Transparency by Design? Re-enabling Double Contingency*, 2013, 1.
[137] Art. 10 §2 PW.
[138] Art. 10 §3 PW.

Artikel 15 AVG omschrijft een recht op inzage van de betrokkene. Zo zal deze recht hebben op toelichting over het al dan niet verwerken van zijn persoonsgegevens en wanneer dit het geval is, op inzage van een aantal zaken. Onder meer met betrekking tot automatisering (waaronder profilering) en de logica ervan.

Dit laatste is in het kader van big-dataverwerkingen cruciaal, waar deze per definitie via geautomatiseerde procedés gebeuren. De informatieplicht met betrekking tot de geautomatiseerde verwerking is drievoudig. Het gaat ten eerste om de kennisgeving dat een beslissing wordt genomen op basis van geautomatiseerde verwerking. Daarnaast gaat het ook om betekenisvolle informatie over de onderliggende logica van de verwerking, het belang van deze verwerking en de voorziene gevolgen ervan voor de betrokkene. Overweging 63 van de verordening benadrukt wel dat er ook rekening moet worden gehouden met de auteursrechten die op de software wegen.

De wet maakt hier geen onderscheid tussen soorten automatische verwerking, zolang het maar valt onder 'geautomatiseerde beslissing'. Op die wijze zou in principe ook aan de transparantieplicht moeten worden voldaan wanneer de beslissing slechts een mineur aspect zoals de presentatie van de dienst aan de betrokkene betreft. Dit zou ook de enige logische interpretatie zijn, waar dergelijke beslissingen die niet meteen een (rechts)gevolg hebben voor de betrokkene, laatste desondanks sterk kunnen beïnvloeden. Hierbij valt bijvoorbeeld te denken aan de voorspelling van query's door Google AdSense, die de betrokkenen al dan niet (bijvoorbeeld bepaald resultaat suggereren wanneer jouw naam wordt opgezocht) rechtsreeks kunnen beïnvloeden door bepaalde stereotypes te versterken of gewoonweg zaken te suggereren die de betrokkenen nooit zouden hebben bedacht.[139] Dit zou betekenen dat aan de informatieplicht moeten worden voldaan zodra de automatische verwerking output genereert naar een betrokkene toe, ook waar bijvoorbeeld de drempel voor het recht niet te worden onderworpen aan automatische besluitvorming [infra], niet bereikt is.

In dit verband valt op te merken dat het denkbaar is dat de verantwoordelijke voor de verwerking bij een *machine learning* of *deep learning* script geen weet heeft van hoe de gegevens exact worden verwerkt, dan wel waarvoor ze in verdere fases aangewend worden en nog minder tot welke gevolgen dit zou kunnen leiden. Het is in dergelijke omstandigheden weliswaar nog steeds mogelijk betekenisvolle informatie te geven over de gehanteerde algoritmes en trainingssets. Het vereiste 'betekenisvol' karakter van de informatie valt best te kaderen binnen het doel van het recht op toegang. De medegedeelde informatie moet de betrokkene in staat stellen de juistheid van de gegevens en de rechtmatigheid van de verwerking na te gaan.[140] Dit zou dus ook inhouden dat een computerleek aan de hand van deze informatie in staat moet zijn te begrijpen hoe zijn gegevens worden verwerkt, wat de transparantievereiste op zichzelf al een uitdagende (lees: dure) aangelegenheid kan maken. Hierbij is overigens een aantekening te maken wat betreft de stimulus voor ontwikkeling van dergelijke verwerkingstechnieken. Tenzij

[139] L. SWEENEY, Discrimination In Online Ad Delivery, Harvard University, 2013.
[140] HvJ 17 juli 2014, C-141/12, YS e.a, 3. Het hof verwijst hier naar overweging 41 richtlijn.

een intellectueel eigendomsrecht kan worden geclaimd op correlaties die de vrucht van investering en experiment zijn, lijkt onwaarschijnlijk dat de transparantieplicht een positieve weerslag heeft op de ontwikkeling van big data analyse.

De vraag is nu wat te doen met de verwerkingen die omwille van de eigenheid of complexiteit van de code niet uit te leggen, dan wel onvoorspelbaar in hun gevolgen zijn. Dergelijke verwerking zou in principe verboden zijn, aangezien dan niet kan worden voldaan aan de vereisten van artikel 15. De technologieneutrale opstelling van de AVG vormt op dit punt wel een zekere rem op de ondernemingsvrijheid, waar dit de aanwending en ontwikkeling van onvoorspelbaardere (maar mogelijks ook efficientere) verwerkingstechnieken in de weg staat. In de huidige competitie tussen (processed) data-brokers zou dit weleens kunnen leiden tot een achterstelling van de ondernemingen die zich beperken tot de technologie die de voldoening aan art. 15 mogelijk maakt. Hoewel juridisch iedereen voor dezelfde beperking staat, is binnen de huidige, weinig transparante datamarkt niet uit te sluiten dat hiermee een parallelle markt in 'zwarte statistiek' in de hand wordt gewerkt.

Daarnaast heeft de betrokkene recht op een (digitale) kopie van de persoonsgegevens in kwestie, mits dit geen afbreuk aan de rechten en vrijheden van anderen uitmaakt.[141]

De uitoefening van het recht op toegang moest tot voor kort (althans vanwege overheden) niet per definitie gratis zijn, daar een proportionele vergoeding niet werd geacht hinderend te zijn.[142] Met artikelen 12, 5, a en 15, 3 AVG wordt een in principe kosteloze toegang opgelegd. Evenwel wordt voorzien dat de onderneming kan een vergoeding vragen of zelfs weigeren toegang te verlenen bij herhaalde of buitensporige verzoeken. Ergens komt dit neer op een verzwaring van de lasten van ondernemingen, waar deze om geen vergoeding te moeten aanrekenen alvast moet investeren in een systeem dat de potentiële (grootschalige) uitoefening van het recht op toegang geen zware kost maakt.

Met de invoering van de AVG vindt er dus een gedeeltelijke overheveling plaats van 'verkrijgbare' informatie naar verplicht mee te delen informatie (vb. met betrekking tot bewaringstermijn en automatisering) en worden bepaalde informatieplichten uitgebreid (bijvoorbeeld rechtsgrond, voornemens en overdraagbaarheid) of verfijnd (bijvoorbeeld tijdstip voor onrechtstreeks verzamelde informatie). Er wordt voortaan ook een onderscheid gehanteerd tussen gegevens die wel of niet moeten worden meegedeeld bij de verwerking voor een nieuw doel. Uiteindelijk wordt aan de uitzonderingen op de informatieplicht tevens het beroepsgeheim toegevoegd.

Communicatie:
Artikel 12, eerste lid AVG[143] stelt daarboven eisen met betrekking tot de transparantie van de communicatie met de betrokkene.

[141] Art. 15, 3 & 4 AVG.
[142] HvJ 12 december 2013, C-486/12, ECLI:EU:C:2013:836, X, 22.
[143] Vereist is dat de betrokkene de communicatie ''in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal ontvangt, in het bijzonder wanneer de informatie specifiek voor een kind bestemd is. De informatie wordt schriftelijk of met andere middelen, met inbegrip van, indien dit

Overweging 58 AVG verduidelijkt dat de transparantie in functie van de ontvanger moet worden beoordeeld. De wijze waarop wordt gecommuniceerd wordt niet limitatief omschreven. Naargelang de situatie zal een webpagina, dan wel een persoonlijke communicatie geschikter zijn. Verder kan het onder omstandigheden nodig zijn met bijvoorbeeld visuele ondersteuning te werken. Indien de communicatie naar een kind gericht is (merk op dat hiervoor geen definitie wordt gegeven), moet deze in een voor het kind gemakkelijk te begrijpen taal gebeuren. Een zekere speelruimte wordt dus gecreëerd ten aanzien van de plicht uit artikel 12. De invulling hiervan met het oog op de ontvanger wijst op een prioriteit van het recht op gegevensbescherming, maar tevens op een afweging ervan met onder meer de vrijheid van ondernemen waar geen *by default* minimumeisen worden opgelegd indien dit naar de betrokkene toe niet nodig is. Voor de exploitanten betekent dit dat zij hun communicatie over de verwerking van persoonsgegevens zullen moeten aanpassen aan hun doelpubliek. Zo zal de producent van een spelletjes-app in principe gevulgariseerder moeten communiceren dan bijvoorbeeld de host van een platform zoals LinkedIn.

c. Doelbinding:

Ongeacht de grond waarop wordt verwerkt geldt altijd tevens het centrale beginsel van doelbinding,[144] bestaande uit de plicht tot doelspecificatie en daarop voortbouwend het principe van minimale gegevensverwerking.[145] Laatste houdt onder de bestaande regeling in dat gegevens toereikend, ter zake dienend en niet overmatig mogen worden verwerkt in verhouding tot de welbepaalde doeleinden. Onder de AVG wordt dit klaarblijkelijk verstrengd met de vereiste dat de verwerking 'noodzakelijk' is voor de doeleinden.[146] Een ander beginsel voortbouwend op deze doelbinding is dat van de opslagbeperking, dat stelt dat de gegevens hun identificerend karakter niet mogen behouden verder dan wat noodzakelijk is voor de doeleinden[147] Uiteindelijk valt in dit verband nog aan te halen dat het de verantwoordelijke is die het doel bepaald en dat de verplichting tot heldere mededeling ervan nauw samenhangt met de vereiste van geldige toestemming [infra].

Beperking

In artikel 4, 2° tot 5° Wet '92 (6, 1, b tot e richtlijn) werd reeds een doelbeperking ingeschreven.[148]

De AVG omschrijft een gelijkaardige beperking in artikel 5, 1, b tot e en benoemt daarboven de principes als deze van de *doelbinding* (verenigbaarheid met doel) (b), *minimale gegevensverwerking* (proportionaliteit ten aanzien van doel) (c) en *opslagbeperking* (bewaring

passend is, elektronische middelen, verstrekt. Indien de betrokkene daarom verzoekt, kan de informatie mondeling worden meegedeeld, op voorwaarde dat de identiteit van de betrokkene met andere middelen bewezen is.''

[144] Art. 4, 2° PW, 6, b richtlijn & 5, 1, b AVG.

[145] Art. 4, 3° PW & 6, c richtlijn.

[146] Art. 5, 1, c AVG.

[147] Art. 4, 5° PW, 6, e richtlijn & 5, 1, e AVG.

[148]

afhankelijk van doel) (e). In de AVG wordt weliswaar aan de lijst bijzondere doeleinden de 'archivering in het algemeen belang' toegevoegd. In punten c en e spreekt de AVG bovendien van 'noodzakelijk' in plaats van 'ter zake dienend', wat lijkt op een voortaan verzwaarde eis ten aanzien van het doel.

In verband met de uitzondering om bepaalde doeleinden is de vraag op te werpen hoe de abstracte profilering als onderzoek zich verhoudt tot deze beperking en meer bepaald tot de algemenere informatieplichten, waar de statistische verbanden aan de grondslag van profielen in beginsel aan de persoonsgegevensbescherming ontsnappen in zoverre zij niet concreet toegepast worden. Een samenlezing van 89, 4 en 14, 5, b AVG geeft de indruk dat zuiver empirische profilering door databrokers, zonder dat de betrokkenen hiervan weten, mogelijk is. Daarnaast zou door de verkoop van aggregaten gegevens en conclusies, in de mate dat deze op voldoende wijze zijn geanonimiseerd (dan wel door middel van pseudonimisering) nog steeds geen recht op informatie bestaan, daar het vanaf dat punt niet meer om persoonsgegevens gaat. Dit alles zou impliceren dat de activiteit van vele databrokers die er in bestaat gegevens te verzamelen bij andere verantwoordelijken en deze bij te houden en te verwerken onder het 'statistisch' oogmerk om vervolgens te handelen in astracte of voldoende gepseudonimiseerde profielen, volledig achter de rug van de betrokkenen mogelijk is in zoverre het argument van de 'zware last' aannemelijk wordt gemaakt. Argument dat zeer aannemelijk blijkt bij de verwerving van een massa datasets zonder contactgegevens. Anderzijds moet ter herinnering worden gebracht dat via de informatieplicht inzake de logica van de verwerking, toch een zekere informatieplicht betreffende de gehanteerde statistische verbanden (en de oorsprong ervan?) voorafgaand aan de toepassing van een profiel, ontstaat.

Hergebruik van gegevens

Artikel 6, 4 AVG[149] preciseert hoe de verenigbaarheidstoets (behoudens toestemming van de betrokkene en toegestane gronden) moet gebeuren wanneer de persoonsgegevens worden verwerkt voor een ander doel dan hetgeen waarvoor ze werden verzameld. Het betreft hier eigenlijk een ontwikkeling van de zinsnede ''alle relevante factoren, met name...'' uit de richtlijn.

De verwerking onverenigbaar met het aanvankelijke doel is toch toegelaten wanneer dit steunt op de toestemming van de betrokkene of een wettelijke bepaling ter vrijwaring van de belangen uit artikel 23, mits evenredigheid ten aanzien van de gegevensbescherming.[150]

In de relatie tot het hergebruik van de persoonsgegevens voor andere doeleinden zal het spanningsveld tussen de bescherming en de vrijheid van ondernemen zich sterk aftekenen, waar bijvoorbeeld lichte wijzigingen in het beleid of de activiteit van een onderneming in beginsel steeds een verenigbaarheidstoets met zich meebrengen aangezien het uitdrukkelijk 'welbepaalde' doel daarmee a fortiori ook gewijzigd zal zijn (ervan uitgaande dat een ruim omschreven, flexibel doel hiermee in strijd is). Naast de zware lasten dat dit eventueel

[149] Hoewel er niet expliciet naar wordt verwezen, zal dit andere doel vanzelfsprekend ook rechtmatig en welbepaald moeten zijn.
[150] Art. 6, 4 AVG.

meebrengt, vormt ook de kans op een verder gebruiksverbod van persoonsgegevens, die in de meeste gevallen het product van een aanzienlijke investering uitmaken, een rem op de ondernemingsvrijheid.

Wanneer de doeleinden niet langer identificatie vereisen, is naar artikel 11 AVG de verantwoordelijke niet verplicht om aanvullende gegevens te verwerken om verder aan de plichten van de verordening te voldoen. Zo zal de betrokkene wanneer de gegevens niet langer identificatie mogelijk maken, in beginsel geen beroep kunnen doen op zijn actieve rechten uit de verordening (inzage, rectificatie, …) behoudens wanneer deze zelf aanvullende gegevens bezorgt met het oog op de uitoefening van die rechten. De idee is dat de rechten van de betrokkene geen buitensporige last mogen veroorzaken en aldus een inbreuk op andere rechten (meer bepaald de vrijheid van ondernemen) uitmaken.

Er wordt in artikel 11 weliswaar geen gewag gemaakt van anonimisering of pseudonimisering, wat zou veronderstellen dat 'niet langer identificatie mogelijk maken' beide begrippen omvat. In dat geval zouden gepseudonimiseerde gegevens waarvan de ter identificatie vereiste aanvullende gegevens bij een derde liggen (zoals encryptiesleutels), voorbij het bereiken van de doeleinden niet langer vereisen dat deze aanvullende gegevens worden verzameld ter naleving van de artikelen 15 tot 20 AVG. Een strikte lezing van de tekst wijst dus op een vrijstelling van re-identificatieplichten ook in geval van pseudonimisering, in de mate dat de gegevens bedoeld in artikel 11 en de aanvullende gegevens niet bij eenzelfde actor liggen.[151]

De vrijstelling van artikel 11 staat wel op gespannen voet met de uitspraak van het Hof in Rijkeboer. Volgens dit arrest bestaan de rechten van de betrokkene niet slechts op het ogenblik van de uitoefening ervan, maar tevens retroactief. Het Hof geeft zelf weliswaar geen termijn aan voor deze retroactieve werking, maar benadrukt dat er moet worden gezocht naar een evenwicht tussen enerzijds de belangen van de betrokkene, in casu de toegang tot de gegevens, en anderzijds de lasten die met de uitoefening van zijn rechten door de betrokkene gepaard gaan voor de verantwoordelijke.[152]

Uiteindelijk valt in dit verband nog te wijzen op de e-privacyverordening waarvan de voorrang als lex-specialis ongetwijfeld de draagwijdte van de AVG aantast. Cruciaal in dit verband is het amendement 72 gemaakt naar aanleiding van het LIBE comité. Als gevolg van dit amendement zou alle data binnen het toepassingsgebied van de besproken verordening verzameld, strikt worden uitgesloten van verder gebruik.[153] Samen met bijvoorbeeld de specifieke (complementaire) vereisten voor geldige toestemming eruit voortvloeiend, doorkruist de e-

[151] S. STALLA-BOURDILLON, *A call for a common techno-legal language to speak about anonymisation, pseudonymisation, de-identification… Could this be one of the biggest challenges brought about by the GDPR?*, November 9, 2016.
[152] HvJ 7 mei 2009, C-553/07, Rijkeboer, 70.
[153] Zie voorgestelde amendement 72 van het LIBE: http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&reference=PE-606.011&format=PDF&language=EN&secondRef=01

privacyverordening de AVG en relativeert deze enigszins het belang ervan wanneer het gaat over elektronische communicatie.

d. Andere beginselen

Daarnaast bestaan er ook een aantal meer kwaliteitsgerichte beginselen. Zo zal er ook moeten worden getoetst aan het beginsel van juistheid (daarmee ook volledigheid en actualiteit) van de gegevens, waaruit onder meer het recht op rectificatie en uitwissing voortvloeien.[154] Er zal ook aan het beginsel van integriteit en vertrouwelijkheid worden voldaan wanneer passende technische en organisatorische maatregelen ter beveiliging van de gegevens worden genomen.[155] Ook uit de e-privacyrichtlijn artikelen 4, 5 en 6 vloeien een aantal plichten inzake het vertrouwelijkheidsbeginsel voort. Uiteindelijk valt in dit verband ook te verwijzen naar de kennisgevingsplicht aan ontvangers inzake rectificatie, uitwissing en verzet. Merk op dat waar de richtlijn hierin speelruimte voorzag en mogelijk maakte dat dit enkel op verzoek van de betrokkene moest gebeuren, de AVG hiervan onder alle omstandigheden een verplichting van maakt. Wel is voortaan de informatie over de ontvangers in kwestie facultatief. Infra wordt afzonderlijk de beveiliging behandeld.

VI.2 §2. Rechtmatigheid van de verwerking

Naast de overeenstemming met deze beginselen, moet de verwerking tevens berusten op een rechtvaardigende grondslag om als rechtmatig te worden beschouwd. Naargelang de aard van de verwerking en de relatie tussen verantwoordelijke en betrokkene kunnen verschillende grondslagen van toepassing zijn.

a. Grondslagen

Artikel 5 wet '92 (7 richtlijn gegevensbescherming, 6 AVG) somt limitatief de grondslagen voor de verwerking op. Hierna wordt vooral aandacht besteed aan de toestemming maar merk op dat verwerking mogelijk is op basis van vijf andere gronden: contract, het vitaal belang van betrokkene, een publiek belang, een wettelijke bepaling of het gerechtvaardigde belang van de verantwoordelijke. In alle gevallen moet de verwerking noodzakelijk zijn in het kader van de betreffende grond.

b. Toestemming

De toestemming wordt in de wet van '92 artikel 1 § 8 gedefinieerd.

Artikel 6 AVG neemt dit licht genuanceerd over. De toestemming wordt hier gepreciseerd als betrekking hebbend op een of meer specifieke doeleinden (a). Daarnaast worden algemener ook

[154] Art. 4, 4° PW, 6, 1, d richtlijn & 5, 1, d AVG.
[155] Art. 16 PW, 17 richtlijn & 5, 1, f AVG.

de vitale belangen van andere natuurlijke personen dan de betrokkene in aanmerking genomen (d). Uiteindelijk wordt ook de laatste grondslag (gerechtvaardigde belang) verruimd tot derden in het algemeen en wordt alvast gepreciseerd dat met name wanneer de betrokkene een kind is, zijn fundamentele rechten en plichten zwaarder doorwegen (f).

Artikel 8 voegt hier nog aan toe dat de minderjarige jonger dan 16 jaar in verband met een aanbod door een informatiemaatschappij (d.i. deze waarvan informatie een centraal element van de economische activiteit uitmaakt) slechts geldig kan toestemmen met machtiging of toestemming van zijn verantwoordelijken. Deze leeftijd kan door de lidstaten tot 13 jaar worden verlaagd.

De AVG is in artikel 7 ook verregaander in de bepaling van de toestemmingsvereiste. Er wordt ten eerste aantoonbaarheid vereist van de toestemming die betrekking heeft op de verwerking van de persoonsgegevens (1). Wanneer de toestemming onderdeel is van een verklaring die op meer aangelegenheden betrekking heeft, wordt op straffe van niet-binding van de toestemming vereist dat de clausule op toegankelijke en duidelijke wijze, onderscheiden van de rest wordt gepresenteerd. Dezelfde sanctie geldt overigens wanneer enig ander onderdeel van die verklaring strijdig is met de AVG (2). De betrokkene wordt alvorens toestemming te geven op de hoogte gebracht van zijn recht om op minstens even eenvoudige wijze zijn toestemming ex nunc in te trekken (3). Uiteindelijk wordt de toestemming geacht niet vrijelijk te zijn gegeven wanneer deze niet per verwerking apart kan worden gegeven of wanneer de uitvoering van de overeenkomst afhankelijk is gemaakt van een toestemming voor de verwerking van persoonsgegevens die niet noodzakelijk is voor de uitvoering van de overeenkomst (4).[156] Het laatste lid zal van cruciaal belang zijn voor de frequent voorkomende verdienmodellen waarbij toestemming wordt gevraagd voor verwerkingen die voor de dienst niet noodzakelijk zijn. Op die manier zal bijvoorbeeld niet langer toestemming voor 'verbetering van de gebruikerservaring' mogen worden geëist waar dit niet noodzakelijk is voor de dienst.[157]

Met de vereisten inzake transparantie van de communicatie in de AVG zou enigszins de opportuniteit in ruime omschrijvingen en dubbelzinnige formules in ToS kunnen worden verholpen.[158] Anderzijds tast dergelijke nauwkeurigheid ontegensprekelijk de flexibiliteit van de overeenkomsten aan, wat de intentie (zoals gemak van opstelling) ook is.

[156] Zie ook overweging 43 AVG.

[157] Uit het WER vloeit trouwens een overlappende bescherming voort waardoor de geldigheid van de toestemming tevens afhankelijk is van de transparantie. Zie artikelen VI.37, VI.82, j° VI.2 & VI.45. Er bestaat bij de interpretatie van deze beschermingsregeling overigens ruimte voor de kwalificatie van persoonsgegevens als tegenprestatie en dus element van de prijs. Dit zorgt voor speelruimte inzake de vereiste van *informed consent*. Voor meer hierover zie A. DE BOIS, *Economisch gebruik van persoonsgegevens in België: Hoe beïnvloedt de (nieuwe) gegevensbescherming de vrijheid van ondernemen?*, VUB, 2017, 7.2.2.

[158] C. DE CORT, The Right to Privacy in the digital age. A Facebook case study on the impact of the 2016 data protection reform, Universiteit Gent, 2016, 68.

c. Gevoelige gegevens

De Privacywet behandelt de gevoelige persoonsgegevens in artikelen 6 (waaruit afkomst, overtuiging, lidmaatschap blijkt of seksuele leven betreft), 7 (betrekking op gezondheid) en 8 (inzake rechtbanken en geschillen).

In de AVG worden de gevoelige persoonsgegevens in artikel 9 behandeld, op deze met betrekking tot strafrechtelijke veroordeling en vervolging na, die in artikel 10 staan.

Artikel 9 beschrijft de verwerkingsgronden voor de gevoelige gegevens die in artikelen 6 en 7 van de wet van '92 staan en breidt de draagwijdte van de bescherming tevens uit tot biometrische gegevens. De gronden zijn hier sterk gelijklopend met deze van artikel 6 van de Privacywet, op een paar details na.

In een economische context zal in principe slechts op de toestemming kunnen worden beroep gedaan om over te gaan tot verwerking van medische gegevens of gegevens waaruit een overtuiging kan worden afgeleid, waar moeilijk kan worden verwezen naar wettelijke plichten of het algemeen belang. Op een aantal vlakken wordt met de bijzondere behandeling van gevoelige gegevens zo een rem op de vrijheid van ondernemen gevormd. Zo zal bijvoorbeeld de facto de profilering in sectoren die grenzen aan de medische (bijvoorbeeld verzekeringen) bemoeilijkt worden. Daarnaast zijn bepaalde verdienmodellen in grote mate afhankelijk van de verwerking van gevoelige gegevens. Hierbij kan bijvoorbeeld gedacht worden aan de inschakeling van Facebook tijdens politieke campagnes.[159] In combinatie met de verstrengde transparantievereisten van de AVG, wordt op die wijze sterk geknaagd aan de mogelijkheden voor ondernemingsmodellen die net steunen op de nieuwe aandachtseconomie. Uiteindelijk kan nog worden aangehaald dat in de ogen van het Grondwettelijk Hof, de vrijheid van ondernemen klaarblijkelijk zal moeten wijken voor de bescherming van gevoelige (althans medische) gegevens.[160]

d. Geautomatiseerde individuele besluiten

Artikel 12bis van de Privacywet (15 richtlijn) beperkt de gevolgen van geautomatiseerde gegevensverwerkingen. De achterliggende ratio is dat voor beslissingen die voor de betrokkene een weerslag hebben op bijvoorbeeld de toegankelijkheid van krediet, er minstens een menselijke tussenkomst komt kijken.[161]

Artikel 22 AVG herformuleert dit meer in lijn met de tekst van de richtlijn dan de Privacywet als een recht van de betrokkene niet aan zulke besluiten te worden onderworpen, eerder dan een verbod. Dit recht onder de AVG geldt niet indien het besluit:

[159] A. GARCIA-MARTINEZ, "I'm an ex-Facebook exec: don't believe what they tell you about ads", *The Guardian*, 2 mei 2017.
[160] GwH 18 maart 2010, Arrest 29/2010, Belgisch staatsblad 12 augustus 2010, 51791, B.33.2-B.34.
[161] Art. 17 MvT implementatie richtlijn.

''a) noodzakelijk is voor de totstandkoming of de uitvoering van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke;

b) is toegestaan bij een Unierechtelijke of lidstaatrechtelijke bepaling...; of

c) berust op de uitdrukkelijke toestemming van de betrokkene.''

Het laatste geval is niet uit de richtlijn overgenomen. In de gevallen a en c worden opnieuw maatregelen ter bescherming van de rechten en belangen van de betrokkene getroffen. Deze omvatten naast het recht om diens standpunt te delen minstens het recht dat besluit aan te vechten en nu expliciet het recht op menselijke tussenkomst (3). De besluiten genomen op basis van deze uitzonderingen mogen echter, behoudens in geval van toestemming of redenen van zwaarwegend algemeen belang en mits passende maatregelen ter bescherming van de belangen van de betrokkene, niet steunen op gevoelige gegevens (4).

In de eerste plaats valt te onderstrepen dat dit recht vereist dat een significante impact voor de betrokkene voortvloeit uit het besluit. Wat al meteen interpretatieruimte en bijhorende onzekerheid (en dus rem op de vrijheid van ondernemen) meebrengt. Zo kan de kwestie van bijvoorbeeld gepersonaliseerde lay-out of nog suggesties van andere aanbiedingen bezwaarlijk als 'significant' worden beschouwd.

Ook hier botst de gegevensbescherming met de vrijheid van ondernemen. Zo zal bijvoorbeeld de kleine onderneming die op automatische wijze massaal dergelijke beslissingen neemt, potentieel worden geconfronteerd met een onaangekondigde grootschalige uitoefening van het recht op menselijke tussenkomst, waarop niet op voltreffende wijze kan worden geantwoord. Tegenover de situatie van een overwelmende uitoefening van het recht staat ook de situatie van mogelijks overmatige voorbereiding erop, met alle kosten van dien. Bovendien kan in de context van big data van de menselijke tussenkomst onmogelijk worden verwacht dat deze met even veel factoren als een computer rekening kan houden. Daarnaast lijkt zeer waarschijnlijk dat de menselijke tussenkomst zich grotendeels zal laten beïnvloeden door een suggestie van een computer, waar dit uiteindelijk, mits toevoeging van de interactie met de betrokkene aan de gronden waarop het besluit gebaseerd is, buiten de toepassing van artikel 22 valt. Uiteindelijk lijkt dit recht elders te wringen met de economische vrijheid waar de transparantievereisten en de vereisten van bescherming door ontwerp eventueel tot overbodige bescherming (investeringen) leidt bij een beroep op artikel 22. Zo zal ondanks de transparantie onder meer inzake de logica van dergelijke besluitvorming, zelfs na het instemmen er mee, desondanks een recht er niet aan te worden onderworpen bestaan.

Met het verbod voor deze automatische besluiten om te steunen op gevoelige gegevens wordt meteen ook een reeks activiteiten verboden (opnieuw valt te denken aan bijvoorbeeld de campagnetools van Facebook). Zo zal naargelang de interpretatie van 'significante impact' meer of minder activiteit niet mogen mee evolueren met de technologie.

Waar zo goed als alle verwerking van persoonsgegevens vandaag gebeurt via geautomatiseerde procedés, zijn wellicht een aantal opmerkingen te maken in verband met de behandeling van dit

aspect in de beschermingsregeling. Vooreerst is te noteren dat met de AVG de voorafgaande aangifteplicht inzake geautomatiseerde verwerking[162] (anderzijds moet voortaan een register worden bijgehouden), wegvalt. Daarnaast is van belang dat waar voorheen de informatie inzake de werking, logica en gevolgen van de geautomatiseerde verwerking op verzoek moest worden meegedeeld[163], voortaan alle *nuttige* info hierover reeds bij het verzamelen van de gegevens moet worden meegedeeld.[164] De mededelingsplicht wordt overigens nog steeds afgebakend door een afweging tegen de andere (economische) belangen hierbij betrokken.[165]

VI.2 §3. Beveiliging en bescherming

Naast de algemene plicht van de verantwoordelijke om maatregelen te treffen inzake gegevensbescherming en eerbied van de gegevensbeschermingsbeginselen (zoals de minimale gegevensverwerking)[166], treffen de verwerker en verantwoordelijke (of de vertegenwoordiger onder de Privacywet) ook maatregelen om een afdoend beschermingsniveau sensu stricto te waarborgen voor de gegevens.[167] Dit houdt in dat de gegevens worden beschermd tegen de gevolgen van onder meer vernietiging, verlies, wijziging of ongeoorloofde verstrekking, toegang, doorzending, opslag of enige andere ongeoorloofde verwerking. Als waarborgen verwijst artikel 32 AVG illustratief naar een aantal elementen zoals de pseudonimisering en versleuteling. Bij het toetsen aan de vereisten inzake beveiliging wordt rekening gehouden met de kosten, risico's en beschikbare technieken alsook met certificaten en gedragscodes. De AVG onderscheidt zich met een grotere focus op bescherming door ontwerp.

In artikel 33 AVG wordt bovendien een meldingsplicht voorzien ingeval een inbreuk inzake persoonsgegevens zich voordoet.

Ook ten aanzien van de betrokkene bestaat een dergelijke meldingsplicht. Artikel 34 AVG verplicht de verantwoordelijke in geval van een inbreuk die risico's voor de rechten van de betrokkenen meebrengt, aan laatsten onverwijld hierover te melden. De melding aan de betrokkenen omvat, op de details inzake de inbreuk zelf (aard, ect.) na, minstens dezelfde informatie als deze aan de toezichthoudende autoriteit. Als uitzonderingen op de meldingsplicht ten aanzien van de betrokkenen wordt ten eerste gegeven het hebben genomen van passende maatregelen, met name deze die de persoonsgegevens onbegrijpelijk maken, zoals versleuteling, zowel ter preventie van inbreuken als ter preventie van herhaling ervan (3, a & b). Daarnaast geldt de plicht ook niet wanneer de inspanningen hiervoor onevenredig zouden zijn. In dat geval zal wel voor een andere wijze om de betrokkene te informeren moeten worden

[162] Art. 17 PW & 18 richtlijn.
[163] Art. 10, 1, c PW.
[164] Art. 13, 2, f AVG, analoog 14 AVG.
[165] Overwegingen 41 richtlijn en 63 AVG.
[166] Art. 25 AVG.
[167] Art. 16,4 PW, 17 richtlijn, 32 AVG.

gezorgd (c). Uiteindelijk heeft de toezichthoudende autoriteit het laatste woord over het bestaan van deze meldingsplicht.[168]

Wanneer een soort verwerking (in het bijzonder deze met behulp van nieuwe technologie) risico's inhoudt voor de rechten van natuurlijke personen, wordt naar artikel 35 AVG door de verantwoordelijke een gegevensbeschermingseffectbeoordeling uitgevoerd alvorens tot deze verwerking over te gaan. Deze beoordeling gebeurt na advies van de eventuele functionaris voor gegevensbescherming.[169] De beoordeling is vereist wanneer besluiten worden genomen op basis van geautomatiseerde verwerking, zoals profilering (a), wanneer er sprake is van grootschalige verwerking van gevoelige gegevens (b) en bij stelselmatige en grootschalige monitoring van publieke ruimten (c). Daarnaast stelt de toezichthoudende autoriteit een lijst van hoe dan ook hieraan onderworpen soorten verwerking op.[170] Bij de beoordeling van het effect van de voorgenomen verwerking in dit kader, wordt rekening gehouden met gedragscodes.[171] Wanneer het gaat om een verwerking die voortvloeit uit een wettelijke verplichting, is behoudens andersluidende lidstatelijke of Unierechtelijke bepaling, de beoordeling niet verplicht.[172]

Na afweging met beveiliging en economische en algemene belangen wordt desgevallend naar inspraak van de betrokkenen of hun vertegenwoordigers over de voorgenomen verwerking gevraagd.[173] Minstens ingeval de risico's wijzigen, zal de overeenstemming van de verwerking met de beoordeling worden getoetst.[174]

Wanneer uit de beoordeling blijkt dat de verwerking een hoog risico zou opleveren, raadpleegt de verantwoordelijke vooraf de toezichthoudende autoriteit. Laatste zal dan zo nodig advies verlenen of op andere wijze tussenkomen.[175]

Hier is opnieuw een gespannen situatie ten aanzien van de vrijheid van ondernemen vast te stellen. Waar de beoordeling verplicht is zodra besluiten worden genomen op basis van automatische profilering, houdt dit potentieel een zware last in voor kleine data-intensieve ondernemingen. In die specifieke situatie, rekening houdende met onder meer de transparantieplichten en het recht niet aan dergelijke besluiten te worden onderworpen, lijkt enigszins een onevenredige rem op de vrijheid van ondernemen te bestaan, waar de facto een activiteit inzake gegevensverwerking wordt bemoeilijkt voor kleinere ondernemingen.

Uiteindelijk is de meerwaarde van dergelijke beoordelingen minstens voor discussie vatbaar in het licht van de verzwaarde plichten in verband met bescherming door ontwerp. Een grotere

[168] Art. 34, 4 AVG.
[169] Art. 35, 2 AVG.
[170] Art. 35, 4-6 AVG. Zie de voorlopige zwarte en witte lijst van de CBPL in annex bij: Ontwerp van aanbeveling uit eigen beweging (CBPL) met betrekking tot de gegevensbeschermingseffectbeoordeling en voorafgaande raadpleging voorgelegd voor publieke bevraging, (CO-AR-2016-004).
[171] Art. 35, 8 AVG.
[172] Art. 35, 10 AVG.
[173] Art. 35, 9 AVG.
[174] Art. 35, 11 AVG.
[175] Art. 36 J° 58 AVG.

nadruk op laatsten zou trouwens in principe tot een gelijkaardig (als niet beter) resultaat leiden.[176]

VI.2 §4. Aanmeldingsplicht en register

Onder de Privacywet geldt een aangifteplicht voorafgaand aan elke geheel of gedeeltelijk geautomatiseerde verwerking.[177] Met de AVG wordt deze aangifteplicht verlaten en vervangen door een verplicht schriftelijk (waaronder elektronisch) register van de verwerkingsactiviteiten dat op vraag van de toezichthoudende autoriteit ter hunne beschikking wordt gesteld. Voor niet-geautomatiseerde verwerking kan de Commissie tevens deze inlichtingen vragen wanneer de verwerking een mogelijke schending van de persoonlijke levenssfeer inhoudt.[178] Naar artikel 30 AVG houdt de verantwoordelijke of in voorkomend geval de vertegenwoordiger een register bij dat bepaalde gegevens bevat over de activiteit.[179]

De verwerker of zijn verantwoordelijke houdt daarnaast een register bij van alle categorieën activiteiten die zij ten behoeve van de verantwoordelijke hebben verricht.[180]

Deze verplichtingen gelden, behoudens niet-occasionele verwerking, zwaarwegende risico's en verwerking van gevoelige gegevens, niet voor ondernemingen met een personeelsbestand van minder dan 250 personen.[181] Voor kleinere, data-intensieve bedrijven kunnen deze plichten erg zwaar zijn. Waar bijvoorbeeld apps vaak door kleine teams of zelfs soloprojecten worden gedragen, zou dit dan kunnen neerkomen op een verplichte outsourcing, opleiding of aanwerving van personeel, met een zeer significante impact op de middelen van deze ondernemingen.

VI.2 §5. Doorgifte

In geval van doorgifte van gegevens aan derde landen of (sinds de AVG) internationale organisaties, gelden een aantal specifieke bepalingen die beogen deze doorgifte te onderwerpen aan passende waarborgen.[182] Deze voorwaarden moeten voortaan tevens worden nageleefd bij verdere doorgifte naar een ander derde land of een andere internationale organisatie.[183] De publicatie op het internet maakt geen doorgifte uit, al worden de data daarmee beschikbaar in derde landen.[184] De doorgifte mag in beginsel slechts geschieden naar landen (of organisaties) die een passend beschermingsniveau waarborgen. Onder de AVG wordt de aantoonbaarheid van deze waarborgen onderverdeeld in deze op zichzelf volstaand en deze die daarboven toestemming van de toezichthoudende autoriteit vereisen. Zonder toestemmingsvereiste, somt

[176] N. WALTERS, "Privacy Impact Assessment – Great Potential Not Often Realised'' in D. WRIGHT & P. DE HERT (Eds.) *Privacy Impact Assessment*, Springer, 2012, 151.
[177] Art. 17 PW & 18 richtlijn.
[178] Art. 19 PW
[179] Art. 30, 1 AVG.
[180] Art. 30, 2 AVG.
[181] Art. 30, 5 AVG.
[182] Art. 21 PW & 25richtlijn
[183] Art. 44 AVG
[184] HvJ 6 november 2003, C-101/01, Lindqvist, 68.

artikel 46, tweede lid AVG een aantal elementen op, waaronder de bindende bedrijfsvoorschriften. Het derde lid presenteert de elementen die mits besproken toestemming voldoen.

Artikel 47 AVG behandelt meer in detail de bindende bedrijfsvoorschriften die het bestaan van waarborgen aantonen. Het gaat meer bepaald om bindende bedrijfsvoorschriften die door de toezichthoudende autoriteit worden goedgekeurd in samenspraak met de Commissie.[185] De voorschriften in kwestie leggen minstens bepaalde elementen vast, opgesomd in artikel 47, tweede lid AVG. Het gaat onder meer over gegevens inzake de gebonden ondernemingen, beoogde verwerkingen, categorieën persoonsgegevens, procedures en gehanteerde beginselen. Deze bindende bedrijfsvoorschriften zijn de meest flexibele waarborg waarover de oorspronkelijke verwerker controle heeft en zijn de facto de enige optie voor de onderneming die op lange termijn binnen eenzelfde groep wil verwerken. De voorschriften komen neer op een export van de Europese beschermingsregeling binnen eenzelfde economische activiteit. Waar de voorschriften tevens procedurele aangelegenheden en andere kostelijke eisen bepalen, kan dit de vrijheid van ondernemen onder druk zetten, zowel financieel als op vlak van intern beleid. De goedkeuringsvereiste houdt in dat actieve multinationals die voorlopig op beroepscodes steunden, deze in beginsel expliciet zullen moeten laten toetsen door de autoriteiten. Daarboven kan de onderhandeling en samenstelling van dergelijke voorschriften een dure zaak zijn, waar het Eurocentrisch gegeven niet per se verzoenbaar is met andere lokale bepalingen, een administratieve procedure moet worden doorlopen en bovendien de goedkeuring op zich kan laten wachten, wat de gehele activiteit aan banden kan leggen. Deze omstandigheden maken overigens de optie van de voorschriften enigszins ontoegankelijk voor kleinere ondernemingen.[186]

Het bestaan of ontbreken van een passend beschermingsniveau kan tevens bij een besluit van de Commissie worden vastgesteld.[187] Ter zake kan worden verwezen naar het vernietigde adequaatheidsbesluit inzake doorgiften aan Amerikaanse ontvangers.

Indien noch een adequaatheidsbesluit, noch een ander instrument in de zin van artikel 46 aanwezig is, kan de doorgifte slechts geschieden in een beperkt aantal gevallen. Dit is zo ingeval de betrokkene ondubbelzinnig heeft ingestemd met de verwerking, waaraan de AVG een vereiste van informatie over de betrokken risico's toevoegt. Dit is ook zo wanneer de doorgifte noodzakelijk is ter uitvoering van een overeenkomst met de betrokkene of ter sluiting of uitvoering van een in het belang van de betrokkene gesloten overeenkomst. Daarnaast is tevens een uitzondering voorzien wanneer het gaat om gewichtige redenen van algemeen belang, de uitoefening van rechten in rechte of nog de bescherming van de vitale belangen van de betrokkene. Uiteindelijk geldt tevens een uitzondering wanneer de verwerking gebeurt vanuit openbare registers. In laatste geval mag het naar de AVG niet om alle of gehele categorieën

[185] Art. 47,1 j° 63 AVG.
[186] Allen&Overy, *Binding Corporate Rules*, februari 2013, 9.
[187] Art. 25 PW, 4-6 richtlijn & 45 AVG.

persoonsgegevens gaan.[188] Op te merken is dat de ondertekening van een ToS een contractuele band schept tussen de betrokkene en de verantwoordelijke. Op deze wijze kan een zorgvuldige opstelling van de gebruiksvoorwaarden eventueel de facto neerkomen op een omzeiling van de waarborgvereisten. Een nadere invulling van de informatieplicht inzake risico's zou hierbij uiterst welkom zijn.

Wanneer de doorgifte ook in deze mogelijkheden geen toelating vindt, voorziet de regeling een vangnet.[189] In de AVG is de laatste toevlucht te vinden in artikel 49, eerste lid in fine, dat stelt dat de doorgifte is toegelaten in zoverre:

''de doorgifte niet repetitief is, een beperkt aantal betrokkenen betreft, noodzakelijk is voor dwingende gerechtvaardigde belangen van de verwerkingsverantwoordelijke die niet ondergeschikt zijn aan de belangen of rechten en vrijheden van de betrokkene, en de verwerkingsverantwoordelijke alle omstandigheden in verband met de gegevensdoorgifte heeft beoordeeld en op basis van die beoordeling passende waarborgen voor de bescherming van persoonsgegevens heeft geboden.''

In dit geval informeert de verantwoordelijke de toezichthoudende autoriteit en de betrokkene over de doorgifte en informeert hij daarnaast de betrokkene over de dwingende gerechtvaardigde belangen.

Uiteindelijk kunnen uit internationale overeenkomsten nog andere gronden voor de doorgifte voortvloeien. Zonder dergelijke grondslag is elke doorgifte op basis van een rechterlijke uitspraak of besluit van een administratieve autoriteit niet toegelaten (onverminderd de andere gronden).[190]

VI.2 §6. Medewerking

De verwerker, verantwoordelijke en desgevallend vertegenwoordiger zijn verplicht mee te werken met de toezichthoudende autoriteit bij de vervulling van haar taken.[191] De autoriteiten in kwestie hebben naar artikel 58 AVG ruime onderzoeksbevoegdheden en kunnen eventueel corrigerende maatregelen opleggen, alsook een vordering voor de rechtbank inleiden teneinde de verordening na te doen leven. De niet-naleving van beslissingen van de toezichthoudende autoriteit kan administratief worden gesanctioneerd.

VI.3. Rechten van de betrokkene

VI.3 §1. Transparantie en toegang

In de eerste plaats heeft de betrokkene recht op transparantie ten aanzien van de verwerking van zijn persoonsgegevens. Naast de informatieplichten vanwege de verantwoordelijke, bestaat

[188] Art. 22 PW, 26 richtlijn & 49, 2 AVG.
[189] Art. 22 PW *in fine* & 26, 2 richtlijn.
[190] Art. 48 AVG.
[191] Art. 31 AVG.

dit tevens uit het actieve recht van inzage [supra]. Daarnaast heeft hij voortaan recht op een transparante en begrijpelijke communicatie vanwege de verantwoordelijke, ook in verband met de uitoefening van zijn rechten.[192]

VI.3 §2. Rectificatie en uitwissing

De betrokkene heeft het recht onjuiste persoonsgegevens onverwijld te laten verbeteren en naargelang het doel de aanvulling of vervollediging ervan te eisen. Onder omstandigheden bestaat er ook een recht op uitwissing van de gegevens.

a. Rectificatie

Artikel 4, 4° van de Wet van '92 (6, 1, d richtlijn) formuleert een recht op rectificatie en uitwissing van onjuiste, onvolledige en niet dienende gegevens.

Artikel 12 §1 (12, b richtlijn) werkt dit uit door er 'kosteloos' aan toe voegen.

In artikel 5, d AVG wordt 6, 1, d richtlijn, mits toevoeging 'onverwijld', overgenomen onder het beginsel van juistheid. Het recht op rectificatie wordt nog eens expliciet as such overgenomen in artikel 16 AVG.

Verder gaat de rectificatie zowel onder de huidige regeling[193] als onder de AVG[194] gepaard met een kennisgevingsplicht daarvan aan derden.

b. Uitwissing/vergetelheid

Er bestond reeds onder de Privacywet een recht om van de verantwoordelijke voor de verwerking een verwijdering van bepaalde persoonsgegevens te bekomen.[195]

In het arrest Google v Spain werd gezamenlijk op artikelen 7 en 8 van het Handvest met artikelen 6, 12 en 14 richtlijn gesteund om het bestaan van een recht op vergetelheid (‘*Right to be forgotten*’) te bevestigen. De uitspraak verfijnt deze situaties door op te sommen dat er een dergelijk recht bestaat ten aanzien van onjuiste en irrelevante gegevens, maar daarnaast ook wanneer de verwerking ongeschikt is of buitensporig ten aanzien van het doel. Daarnaast wordt het recht op vergetelheid als element van het recht op privacy (91) aangehaald en samen met het recht op gegevensbescherming afgewogen tegen en zwaarder doorwegend geacht dan het economische belang van de exploitant en het recht op informatie van de andere internetgebruikers (81, 93, 97 & 99).[196]

[192] Art. 12,1 AVG.
[193] Art. 12 §3 PW & 12, c richtlijn.
[194] Art. 19 AVG.
[195] Art. 12 PW, algemener in 12, b en c richtlijn.
[196] HvJ 13 mei 2014, C-131/12, Google/Spain.

Met artikel 17 AVG wordt apart (los van verzet en toegang) een recht op vergetelheid, analoog aan dit van 12, b en 14 richtlijn besproken. Onder meer wanneer persoonsgegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij. Noteer hierbij dat onder deze diensten wordt begrepen elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van een afnemer van diensten wordt verricht.[197]

Indien de persoonsgegevens reeds openbaar zijn gemaakt, worden, rekening houdend met redelijke verwachtingen en beschikbare technologie, de nodige maatregelen getroffen en kennisgevingen gedaan ter verwezenlijking van de uitwissing.[198]

Er bestaan tevens uitzonderingen op het recht op vergetelheid, met name wanneer het gaat om de uitoefening van het recht informatie of vrije meningsuiting (a), het nakomen van wettelijke verwerkingsplichten of taken van algemeen belang (b), redenen van algemeen belang op het gebied van volksgezondheid (c), situaties die verband houden met rechtsvorderingen (e) en uiteindelijk indien de uitwissing in het gedrang dreigt te brengen de archivering in het algemeen belang, het historisch of wetenschappelijk onderzoek of het onderzoek voor statistische doeleinden (d). Hierbij kan nogmaals naar het arrest Google v Spain worden verwezen, alsook naar de kwalificatie van abstracte profilering als statistisch doel.

VI.3 §3. Beperking en bezwaar

Er bestaat voor de betrokkene ook een recht zich te verzetten tegen de verwerking door de beperking van de verwerking te eisen, dan wel bezwaar te maken tegen de verwerking.

Vanuit het perspectief van privacy als omvattende zowel een positief als een negatief element, is in het recht op privacy tevens een grondslag te vinden voor het recht op verzet tegen de verwerking van gegevens.

Artikel 12 van de Privacywet (14 richtlijn) formuleerde reeds een recht van verzet.

In artikel 18 AVG wordt het recht op beperking van de verwerking afzonderlijk geformuleerd. Dit geldt wanneer de betrokkene de juistheid van de gegevens betwist gedurende een periode waarin de verantwoordelijke dit kan nagaan (a), de verwerking onrechtmatig is en de betrokkene in plaats van de uitwissing een beperking van verwerking verzoekt (b), de verantwoordelijke de gegevens niet meer nodig heeft, maar de betrokkene wel in het kader van een rechtsvordering (c) en uiteindelijk in afwachting van een reactie op een bezwaar tegen de verwerking, mits afweging van de belangen (d).[199]

Het verzet onder de AVG kan slechts worden overstemd door een toestemming van de betrokkene, belangen die op een rechtsvordering betrekking hebben, de bescherming van

[197] Art. 1, 1, b Richtlijn informatiemaatschappijen.
[198] Art. 17, 2 & 19 AVG.
[199] Art. 18, 1 AVG.

rechten van personen of gewichtige redenen van algemeen belang. Indien de verantwoordelijke voornemens is de beperking op te heffen, brengt hij hiervan de betrokkene op de hoogte.[200]

Artikel 21 AVG omschrijft afzonderlijk het recht van bezwaar, waarbij de betrokkene bezwaar kan maken tegen de verwerking op basis van redenen van algemeen belang of een gerechtvaardigd belang. De idee is dat in deze situaties moet worden afgewogen tussen de rechten en belangen van de betrokkene en deze van de andere actoren. Het recht van bezwaar vertegenwoordigt ook de tegenhanger van de intrekking van de toestemming in de situaties waarbij de verwerking op belangen steunt.[201] Wanneer bezwaar wordt gemaakt tegen de verwerking, staakt de verantwoordelijke de verwerking tenzij laatste zelf zwaarder doorwegende gerechtvaardigde gronden aanvoert, dan wel belangen in verband met rechtsvorderingen kan aantonen (1). In gevallen van direct marketing bestaat analoog met de uitwissing te allen tijde een recht op bezwaar (2). In dat geval worden de verwerkingen met oog op direct marketing gestaakt (3). Wanneer de verwerking uiteindelijk gebeurt met het oog op historisch, wetenschappelijk of statistisch onderzoek, zal het bezwaar moeten wijken voor zover hier een taak van algemeen belang aan ten grondslag ligt (6). In verband met diensten van informatiemaatschappijen mag het recht van bezwaar worden uitgeoefend via geautomatiseerde procedés (5). Dit laatste is een voorbeeld van bescherming per ontwerp en hangt nauw samen met de vereiste dat de toestemming even gemakkelijk moet kunnen worden ingetrokken als gegeven, waar het recht van bezwaar zich benut ziet bij de verwerking die niet op toestemming steunt.

Het is alvast duidelijk dat in situaties van conflict tussen enerzijds het recht niet het voorwerp te zijn van direct marketing of procesrechtelijke belangen van de betrokkene en anderzijds economische belangen van de verantwoordelijke, laatste zal moeten wijken. Dit komt in feite neer op een inperking van het eigendomsrecht en de vrijheid van ondernemen ten gunste van het negatieve recht op privacy en het recht op eerlijk proces. Anderzijds moet in het kader van bezwaar worden vastgesteld dat het recht op eerlijk proces van de verantwoordelijke voorrang kan krijgen op de gegevensbescherming. De uitzondering op het recht van verzet in geval van contractuele plicht wijst wellicht op een zekere voorrang van de vrijheid van ondernemen (althans de contractuele vrijheid) op de gegevensbescherming. Zo kan klaarblijkelijk conventioneel afbreuk worden gedaan aan het recht op verzet, waarbij kan worden gedacht aan een ruime ToS waarin dit de facto terzijde wordt geschoven. Anderzijds weer, is moeilijk denkbaar dat de verwerking op basis van een contractuele plicht niet steunt op toestemming.

Wat betreft het recht van bezwaar kan verder worden aangenomen dat dit een vangnet vormt voor de belangenconflicten waarbij het in hoofde van de verantwoordelijke noch om procesrechtelijk, noch het algemeen belang gaat. Zo kan bijvoorbeeld worden gedacht aan veiligheidsredenen, bijvoorbeeld de situatie waarbij de verantwoordelijke genoodzaakt is de gegevens (tijdelijk) bij te houden en te analyseren om de oorzaak van of de schade voortvloeiend

[200] Art. 18, 2 & 3 AVG.
[201] Advies (WP29) over de definitie van “toestemming”, 13 juli 2011, 15/2011, 11.

uit een aanval of lek te onderzoeken of verder gelijkaardige (nood)situaties te voorkomen.[202] Het lijkt in die situaties aangeraden dat de rechter de verwerking laat beperken tot het strikt noodzakelijke ter bescherming van het gerechtvaardigde belang, dan wel het bezwaar (in de mate dat het wat de betrokkene betreft niet om vitale belangen gaat) verwerpt voor zover de situatie die het gerechtvaardigde belang creëert, blijft bestaan. Het is daarbij moeilijk zich een gerechtvaardigd belang in te beelden dat de levenslange verdere verwerking grond geeft.

VI.3 §4. Overdraagbaarheid van gegevens

Nieuw sinds de AVG is het beginsel en daaruit afgeleide recht van de betrokkene op overdraagbaarheid van gegevens. In de situatie waarbij de verwerking steunt op de toestemming van de betrokkene of een contract en het gaat om verwerking door middel van automatische procedés, kan de betrokkene beroep doen op het recht op overdraagbaarheid van de gegevens. Dit recht bestaat uit twee luiken. In de eerste plaats heeft de betrokkene het recht om de persoonsgegevens die hij aan de verantwoordelijke heeft verstrekt in een gestructureerde, gangbare, machinaal leesbare vorm te verkrijgen. Daarnaast heeft de betrokkene het recht deze gegevens over te dragen aan een andere verantwoordelijke en indien technisch mogelijk deze overdracht rechtsreeks te laten gebeuren. De uitoefening van dit recht mag geen afbreuk doen aan de rechten van anderen. Overweging 68 verwijst in dit verband naar andere betrokkenen.

Onder 'aan hem verstrekt' zou moeten worden begrepen data die al dan niet zuiver door de betrokkenen gegenereerd worden. Hiermee betreft het recht op dataportabiliteit dan niet de geïnfereerde data.[203]

Ondernemingen zullen zich bij gebrek aan toestemming of andere grond vaak wenden tot het gerechtvaardigde belang uit artikel 7, f richtlijn (6, f AVG).[204] Dataportabiliteit betreft deze situatie niet. In het licht van het doel van de dataportabiliteit, dat naar overweging 68 de controle van de betrokkene over zijn gegevens is, wringt enigszins dat indirect of extracontractueel vergaarde gegevens niet het voorwerp van de dataportabiliteit zouden uitmaken, omdat deze gegevens (alsook geïnfereerde trouwens) ook van belang voor de betrokkene kunnen zijn. Geobserveerde, of (hypothetisch) extracontractueel medegedeelde gegevens zouden op die wijze kunnen ontsnappen aan het recht op dataportabiliteit. Wat betreft de uitzondering voor verwerking om wettelijke plichten te vervullen is de zaak begrijpelijker, aangezien de portabiliteit van gegevens hiermee verwerkt een zekere 'verplichte' kwetsbaarheid met zich mee zou brengen.

Daarnaast kan zich worden afgevraagd in welke mate onder 'rechten van anderen' ook de economische belangen van de verantwoordelijke (meer bepaald de rechten op de databank of

[202] Denk maar aan de argumentatie van Facebook in de recente verwikkeling met de Belgische commissie (supra), hoewel dit om procedurele redenen nog niet beslecht werd.
[203] Zie Guidelines (WP29) on the right to data portability, 13 december 2016, 8-9.
[204] HvJ 13 mei 2014, C-131/12, Google/Spain, 73-74. Artikel 7, f impliceert een afweging tussen de betrokken belangen.

algemener de ondernemingsvrijheid) worden begrepen. Overweging 68 heeft het weliswaar over de rechten van betrokkenen, maar een uitbreiding naar andere derden in het uitwerkende artikel zou niet onbegrijpelijk zijn. Zo is denkbaar dat in een kader van concurrentie, via de omweg van dit recht op overdraagbaarheid, bepaalde oneerlijke praktijken het licht zien. Hierbij kan dan gedacht worden aan bijvoorbeeld systematische vergaring van door andere ondernemingen geobserveerde data in draagbare formaten (wat zelfs een hoop verder gaat dan de inzage ervan). Overweging 63 stelt dat reeds bij de inzage moet worden afgewogen tegen de rechten of vrijheden van anderen, met inbegrip van het zakengeheim of de intellectuele eigendom en met name het auteursrecht op software. Echter, in het licht van het doel van de dataportabiliteit, dat niet hetzelfde als dat van het recht op inzage is, en de mogelijkheid rechtsreeks de gegevens van de ene naar de andere verwerker te laten doorgeven, lijkt hierbij nergens te worden gedoeld op dataportabiliteit. Ook is onduidelijk of het de bedoeling is dit recht op alle gegevens dan wel, analoog aan het recht op inzage, onder omstandigheden, op vraag van de verantwoordelijke, op aangeduide categorieën gegevens te laten slaan. De meest logische benadering lijkt dan ook te zijn dat de 'rechten van anderen' alsook deze van de verantwoordelijke omvatten. Het kan niet wezen dat de ontvangende databeheerder de zo doorgestuurde data voor eigen commerciële doelen aanwendt, al zeker niet waarbij strikt relationele data (contactenlijsten, oproepen,…) van andere betrokkenen op die wijze zonder hun toestemming of kennis bij andere beheerder terechtkomen.[205] Het is in deze optiek uiteindelijk enigszins begrijpelijk zijn dat de dataportabiliteit beperkt blijft tot de contractuele situaties, omdat de data hierbij in beginsel door de betrokkene zelf, theoretisch minstens met diens kennis ervan werden gegenereerd en in principe de uitoefening van het recht op dataportabiliteit hiermee voor minder misbruik in aanmerking komt.

VI.3 §5. Geautomatiseerde verwerking en profilering

Zodra gebruik wordt gemaakt van geautomatiseerde verwerkingsprocedés, heeft de betrokkene dus voortaan (naast de bijkomende transparantievereisten, zie supra VI.2 §2), ter verruiming van zijn zeggenschap op zijn gegevens, een recht op overdraagbaarheid ervan.[206]

De betrokkene heeft tevens het recht niet te worden onderworpen aan een besluit dat zuiver op basis van geautomatiseerde verwerking werd genomen (en een recht op menselijke tussenkomst, zie supra VI.2 §2).[207] De AVG maakt hierbij gewag van profilering als onderdeel van geautomatiseerde verwerkingsprocedés. Een exegetische interpretatie van de tekst wijst erop dat profilering dus, behoudens wat betreft het recht van bezwaar[208], enkel wordt geregeld in de mate dat dit een rechtstreekse invloed heeft op de betrokkene, waar de draagwijdte van het recht van de betrokkene in dit verband beperkt blijft tot de besluiten - *louter* - op basis van geautomatiseerde verwerking genomen.

[205] Guidelines (WP29) on the right to data portability, 13 december 2016, 10.
[206] Art. 20 AVG. Zie ook overweging 68 AVG.
[207] Art. 12bis PW, 15 richtlijn & 22 AVG.
[208] Art. 21 AVG.

Profilering zou dus niet gehinderd worden door dit recht indien deze slechts andere betrokkenen beïnvloedt. Een toelichting over wat als 'invloed' wordt beschouwd zou hierbij welkom zijn, waar technisch gezien elke input naar het opstellen van profielen uiteindelijk weerslag heeft op alle betrokkenen die ooit aan het resulterende profiel zullen worden getoetst. Daarboven is hetgeen uiteindelijk bereikt wordt met een recht op menselijke tussenkomst, in het licht van de bedoeling ervan, minstens voor discussie vatbaar.[209] Zo lijkt het weinig waarschijnlijk dat de menselijke interventie (vanuit een kostenbesparend perspectief logischerwijze beperkt tot een goed- of afkeuring van de beslissing die de computer voorstelt) de autoriteit van harde statistiek naast zich neerlegt. Uiteindelijk lijkt het recht op menselijke tussenkomst grotendeels uitgehold te zijn in het licht van de uitzonderingen, meer bepaald deze voor het besluit dat nodig is ter totstandkoming van een overeenkomst met de betrokkene. De geautomatiseerde proactieve evaluatie ter selectie van het aan te spreken cliënteel ligt immers niet zo ver van de automatische eerste weigering te onderhandelen op basis van profielen. Het besproken recht vormt zo, in het bijzonder vanwege de interpretatieruimte erdoor geboden, mogelijks een enorm knelpunt met betrekking tot de vrijheid van ondernemen.

VI.3 §6. Beperkingen

Onder de richtlijn stond het de staten vrij beperkingen op de rechten van de betrokkenen te voorzien in zoverre dit steunde op de vrijwaring van een aantal limitatief opgesomde belangen zoals de openbare veiligheid en de rechten en vrijheden van anderen.[210] Onder de AVG geldt eenzelfde regel, mits een ietwat verschillende opsomming van de bedoelde belangen, zoals bijvoorbeeld de inning van civielrechtelijke vorderingen. Ook preciseert de AVG welke elementen dergelijke wettelijke bepalingen minstens moeten vermelden.[211]

Daarnaast kan algemener worden afgeweken van de verordening ten gunste van andere rechten zoals het recht op vrije meningsuiting en informatie.[212] Er wordt ook expliciet verwezen naar de afweging van rechten ten opzichte van andere (economische) belangen.

VI.3 §7. Uitoefening

Zoals reeds aangehaald behoort er transparantie te zijn omtrent de rechten van de betrokkene en inzake de communicatie in dat verband.[213] Onder de AVG informeert de verantwoordelijke de betrokkene over het gevolg dat aan zijn verzoek wordt gegeven binnen de maand.[214] Zo dit niet is gebeurt, ontvangt de betrokkene binnen de maand uitleg over de reden hiervan alsook informatie over de mogelijkheid klacht in te dienen bij de toezichthoudende autoriteit of nog zich

[209] Cf. overweging 72 AVG.
[210] Art. 13 richtlijn.
[211] Art. 23 AVG.
[212] Art. 85 AVG.
[213] Onder de PW dient de verantwoordelijke binnen de vijfenveertig dagen in te gaan op het verzoek inzake het recht op inzage en binnen de maand op dat in verband met verzet, verwijdering of verbetering. Zie art. 10 §1 & 12 §3 PW.
[214] Art. 12, 2 AVG.

tot de rechtbank te wenden.[215] De verantwoordelijke kan voortaan onder omstandigheden weigeren op kennelijk ongegronde of buitensporige verzoeken in te gaan en zelfs een vergoeding aanrekenen.[216] In het kader van het recht op informatie moet slechts op het verzoek worden ingegaan indien de betrokkene zijn identiteit bewijst. Zo de verantwoordelijke redenen heeft om aan de identiteit te twijfelen, kan hij aanvullende gegevens vragen aan de betrokkene.[217] De informatie aan de betrokkene mag tevens verstrekt worden met gebruik van gestandaardiseerde iconen.[218]

Zo er een geschil ontstaat omtrent de uitoefening van zijn rechten, kan de betrokkene zich naar artikel 31 §3 van de Privacywet alvast wenden tot de CBPL met een klacht. Deze zal dan optreden als bemiddelaar en advies of aanbevelingen geven. In de AVG wordt het klachtrecht bij de nationale toezichthoudende autoriteit bevestigd in artikel 77. Naar artikel 32 §3 van de Privacywet kan de CBPL evenwel de geschillen doorverwijzen naar de rechtbank van eerste aanleg.

Onder de Privacywet is het de rechtbank van eerste aanleg, zitting houdende zoals in kort geding, die kennisneemt van de vorderingen inzake inzage, verbetering, verwijdering en gebruiksbeperking van persoonsgegevens.[219] Vanaf de kennisgeving van het bestaan van een dergelijk geding (behalve inzake inzage), is de verantwoordelijke ertoe gehouden bij elke mededeling van persoonsgegevens duidelijk aan te geven dat hierover betwisting bestaat.[220]

Naar de AVG is tevens een voorziening in rechte gewaarborgd. Dit is ten eerste het geval ten aanzien van het handelen of nalaten van de toezichthoudende autoriteit.[221] Daarnaast is dergelijke voorziening mogelijk rechtstreeks tegen de verantwoordelijke of de verwerker die een inbreuk op de verordening pleegt.[222]

Artikel 80 AVG voert een vertegenwoordigingsbevoegdheid voor bepaalde organen, organisaties of verenigingen zonder winstoogmerk in. Laatsten kunnen in het belang van de betrokkene de actie voor de rechtbanken op zich nemen (1). Met de invoering van dit informele recht op collectieve actie wordt een duwtje gegeven aan de daadwerkelijke aansprakelijkheid van de verantwoordelijke in gevallen van kleine schendingen op grote schaal. Daarnaast kunnen de lidstaten voorzien dat deze instanties ook het klachtrecht van de betrokkene bij de toezichthoudende autoriteit kunnen uitoefenen in diens naam (2).

De AVG voorziet ook de mogelijkheden van schorsing en verwijzing ingeval tegen eenzelfde verantwoordelijke meerdere geschillen aanhangig zijn.[223]

[215] Art. 12, 3 AVG.
[216] Art. 12, 5 AVG.
[217] Art. 12, 6 AVG.
[218] Art. 12, 7 AVG.
[219] Art. 14 §1 PW.
[220] Art. 15 PW.
[221] Art. 78 AVG.
[222] Art. 79 AVG.
[223] Art. 81 AVG.

VII. Aansprakelijkheden, sancties en privaatrechtelijke conflicten

VII.1. Burgerrechtelijke aspecten

Onder de bestaande regeling is het de verantwoordelijke die, behoudens overmacht, aansprakelijk is ten aanzien van de betrokkene voor wat betreft schade uit handelingen in strijd met de gegevensbescherming.[224] Met de AVG wordt de aansprakelijkheid verfijnd en is het naargelang de situatie de verantwoordelijke, de verwerker, dan wel beide, die, behoudens bewijs van afwezigheid van enige verantwoordelijkheid, aansprakelijk is of zijn voor schade. In beginsel is het de verantwoordelijke die zal worden aangesproken. Wanneer echter de verwerker in strijd met de instructies van de verantwoordelijke heeft gehandeld of de schade betrekking heeft op de specifieke verplichtingen van de verwerker uit de AVG, zal laatste aansprakelijk zijn. Gezamenlijke verantwoordelijken of verwerkers zijn hoofdelijk aansprakelijk, mits onderling verhaal.[225]

Er werd reeds door het Hof bepaald dat in situaties waarbij schade door de verantwoordelijke werd veroorzaakt (bijvoorbeeld door lek) en niet helemaal duidelijk is wat de schadeverwekkende handeling exact was, een omkering van de bewijslast plaatsvindt, daar de verantwoordelijke best geplaatst is om te achterhalen wat er gebeurd is. In dezelfde zaak werd enkel een morele schadevergoeding toegekend, bij gebreke van bewezen materiële schade.[226] In een ander arrest gunde het Hof een morele schadevergoeding van 20.000€ voor de onrechtmatige kennisname van gegevens.[227] Een morele schadevergoeding lijkt dus vlot te worden toegekend door het Hof bij inbreuken op de gegevensbeschermingsregeling. Ondernemingen die hiervoor verantwoordelijk zijn, zullen dus niet per definitie ontsnappen aan een schadevergoedingsplicht wanneer materiële schade moeilijk of niet te bewijzen is. Artikel 82 bevestigt overigens dat alle soorten schade in aanmerking komen voor vergoeding.

Met de AVG wordt de bewijslast van de verantwoordelijke klaarblijkelijk verzwaard ten gunste van de betrokkene. Zo zou de verantwoordingsplicht uit artikel 5, 2 kunnen neerkomen op een omkering van de bewijslast. Weliswaar wordt eerder gesproken van een plicht te 'kunnen' aantonen dat aan de verplichtingen wordt voldaan, veeleer dan een effectieve plicht dit aan te tonen. De bepaling zou alvast een de facto omkering van de bewijslast inhouden waar de betrokkene slechts prima facie de inbreuk geloofwaardig moet maken, aangezien de verantwoordelijke wordt verondersteld paraat over een onderbouw ter weerlegging ervan te beschikken. Zonder over te stappen naar een (rechtvaardige?) omkering van de bewijslast, vergemakkelijkt de AVG op meerdere vlakken weliswaar de vordering door betrokkenen, naast de verantwoordingsplicht onder meer met de gezamenlijke aansprakelijkheid van de verwerker en verantwoordelijke of nog de informele collectieve actie. Met betrekking tot het te leveren bewijs van een causaal verband tussen de geleden schade en de fout, lijkt het antwoord

[224] Art. 15bis PW & 23 richtlijn.
[225] Art. 82 AVG.
[226] Ger.EU 12 september 2007, T-259/03, Nikolaou/Commissie, 196, 340. Deze casus handelt over aansprakelijkheid van publieke organen, maar niets belet een analoge toepassing op privaatrechtelijke situaties.
[227] Ger.Ambt.EU 5 juli 2011, F-46/09, V/Parlement, 170-175. Hier eveneens in beginsel analoog toe te passen in private verhoudingen.

bevestigend. Het Hof voor ambtenarenzaken heeft reeds de vraag naar een causaal verband tussen een fout inzake persoonsgegevens en morele schade opgeworpen.[228] Een strikte lezing van 82, 1 AVG wijst trouwens op een bewijsplicht met de zinsnede 'ten gevolge van'.[229]

VII.2. Sancties

De straf- en bestuursrechtelijke aansprakelijkheid is wat persoonlijker. Het zal naargelang de situatie de verantwoordelijke, dan wel de vertegenwoordiger, aangestelde of gemachtigde verwerker zijn die de sanctie riskeert op te lopen. De AVG geeft aan de toezichthoudende autoriteiten een stevige bevoegdheid inzake sancties (tot 4% van de wereldwijde jaaromzet).[230]

Verder staat het de lidstaten vrij om sancties te bepalen voor inbreuken op de verordening, in het bijzonder voor de inbreuken waarvoor geen administratieve sanctie is voorzien, zolang deze sancties maar doeltreffend, evenredig en afschrikkend zijn.[231]

De speelruimte met betrekking tot dit aspect zou wel kunnen mislopen aan het harmoniseringsdoel van de verordening en mogelijks leiden tot forumshopping. Het is best mogelijk dat de Belgische wetgever eenvoudigweg de bestaande strafregeling van de Privacywet behoudt.

VII.3. Specifieke knelpunten

VII.3 §1. Verwerking van onjuiste/verboden gegevens

Onder de Privacywet kan de betrokkene zich richten naar de rechtbank van eerste aanleg zetelend zoals in kortgeding om zijn rechten te doen gelden. Met de AVG is het hoe dan ook een verplichting geworden om de ontvangers in te lichten over de uitwissing, rectificatie of het verzet.[232] Een inbreuk hierop is naar artikelen 19 j° 83, lid 5 alvast administratief sanctioneerbaar, naast de burgerlijke aansprakelijkheid. In hoofde van de ontvanger die deze kennisgeving miskent zou op basis van artikelen 5 j° 93, lid 5 eveneens een dergelijke boete mogelijk zijn, wegens verwerking in strijd met het beginsel van juistheid of opslagbeperking. Met betrekking tot de burgerlijke aansprakelijkheid lijkt de logische oplossing hier te zijn dat de aansprakelijkheid wordt verdeeld naargelang de oorsprong van de schade, met name wie de schadeverwekkende verwerking heeft verricht, onverminderd de aansprakelijkheid voor gezamenlijke verwerkers en verantwoordelijken.

---

[228] Ger.Ambt.EU 11 mei 2010, F-30/08, ECLI:EU:F:2010:43, Nanopoulos/Commissie, 243.

[229] B. VAN ALSENOY, "Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation", *JIPITEC*, 2016, 282-283, 288.

[230] Zie A. DE BOIS, *Economisch gebruik van persoonsgegevens in België: Hoe beïnvloedt de (nieuwe) gegevensbescherming de vrijheid van ondernemen?*, VUB, 2017, annex 'Straf- en bestuursrechtelijke aansprakelijkheid'.

[231] Art. 84 AVG.

[232] Cf. Art. 14 §6 PW.

VII.3 §2. Bewaringsplicht en overdraagbaarheid

Reeds onder de Privacywet had de betrokkene een recht op inzage op de hem betreffende gegevens. Zoals reeds besproken bestaat hier een bijzonder spanningsveld inzake de bewaringsplicht van de verantwoordelijke. Hierbij moet worden afgewogen tussen de economische belangen van de verantwoordelijke en de rechten van de betrokkene, waaronder het recht op eerlijk proces (inzake bewijs).[233] Met de invoering van het recht op gegevensoverdraagbaarheid is hier wellicht een nieuwe dimensie aan gegeven. Dit afzonderlijke recht zal zeer waarschijnlijk een impact hebben op de bewaringsplicht van de verantwoordelijke waar het aan de rechten van de betrokkene op de gegevens een belang toevoegt, namelijk de overdraagbaarheid. Het lijkt waarschijnlijk dat de invoering van het recht op overdraagbaarheid van gegevens de motieven voor een retroactieve werking van de bewaringsplicht voortaan enorm versterkt. Uiteindelijk dient ter herhaling te worden aangehaald dat de verantwoordelijke hoe dan ook gegevens behoort bij te houden om te kunnen voldoen aan de nieuwe verantwoordingsplicht.

VII.3 §3. Datalek en onrechtmatige kennisname

Indien data onrechtmatig worden ingekeken of terechtkomen bij derden waarvoor ze niet bestemd zijn, kan de betrokkene zich tegen de verantwoordelijke keren wegens inbreuk op het vertrouwelijkheidsbeginsel, maar dit zou eveneens mogelijk zijn wegens gebrekkige toestemming of algemener wegens contractbreuk. Er zal in gevallen van lek voortaan een melding moeten gebeuren ten aanzien van zowel de betrokkene als de toezichthoudende autoriteit.[234] Dit mechanisme kan worden aangeduid als 'regulation through disclosure', waarbij de vrees voor reputatieverlies ingevolge de bekendmaking van blunders reeds een corrigerend effect op het gedrag van marktspelers heeft.[235] Voorheen was deze meldingsplicht een lidstatelijke materie, behoudens voor wat betreft telecomproviders, die reeds sinds de wijziging van de e-privacyrichtlijn in 2009 deze plicht hadden.[236] Wat betreft de aansprakelijkheid van de verantwoordelijke zal rekening worden gehouden met de oorzaak van de inbreuk, met name het al dan niet bestaan van een tekortkoming inzake beveiliging. Ter begroting van de materiële en immateriële schade uit het lek zal tevens rekening worden gehouden met de eventuele publicatie die de kennisname opvolgt, alsook de aard van de betrokken gegevens.[237] Wat de (onrechtmatige) ontvanger betreft, is een aansprakelijkheid ten aanzien van de betrokkene denkbaar op basis van verwerking zonder rechtmatige grondslag. Ten aanzien van de eerste verantwoordelijke is de ontvanger mogelijks aansprakelijk wegens inbreuk op het recht van de producent van de databank, in de mate dat dit niet toegestaan werd. Daarnaast is tevens een *brute-forcing* van de databank te beschouwen als een inbreuk op de rechten van de

[233] HvJ 7 mei 2009, C-553/07, Rijkeboer, 70.
[234] Art. 33 & 34 AVG.
[235] C.R. SUNSTEIN "Informational regulation and informational standing: Akins and beyond", *U. Pa. L. Rev*., 1999, 613-614
[236] Art. 4 e-privacyrichtlijn.
[237] T.F.E. TJONG TJIN TAI, "Aansprakelijkheid bij datalekken", *WPNR*, 2016, 1-2, 6-8

databankhouder, waar dit een herhaald opvragen van gegevens die de normale exploitatie te buiten gaat, uitmaakt.[238]

Aangezien de individuele actie tegen dergelijke lekken veel kans maakt te stuiten op een geringe vergoeding, al zeker in verhouding tot de inspanning en kost die gepaard gaat met een procedure tegen een multinational, was tot voor kort voor heel wat betrokkenen met zo'n lek geconfronteerd weinig soelaas te vinden in de Europese beschermingsregeling. Er wordt een stap naar class-actions gezet met artikel 80, eerste lid AVG, waarnaar impliciet een gezamenlijke vertegenwoordiger kan worden aangesteld die in het belang van de betrokkenen een vordering kan instellen. Op het Belgische niveau bestaat daarnaast, althans in het kader van consumentenovereenkomsten, een class action sinds de invoering van het WER. Zo schrijven artikel XVII.36 j° XVII.37, 10° en 22° voor dat de consument zich kan beroepen op een schending van contractuele plichten, de Privacywet of de wet betreffende telecommunicatie (gedeeltelijk omzetting van de gewijzigde e-privacyrichtlijn) om via de collectieve actie een vergoeding te bekomen. Gezien de intentie die blijkt uit de vermelding van deze twee nationale wetten, lijkt uiterst waarschijnlijk dat de wetgever eens deze van kracht is, de AVG zal toevoegen aan de lijst wetgeving waarop voor de collectieve actie gesteund kan worden. Uiteindelijk zou dit resulteren in een soort keuzerecht tussen een class-action op basis van artikel 80 enerzijds en een formelere actie op basis van het WER anderzijds, voor zover het een geschil inzake gegevensbescherming binnen een B2C verhouding betreft.

VII.3 §4. Overgang van rechten

Een lacunaire regeling van het post-mortemregime laat ons met voldoende creativiteit (en twijfel) achter. Wat betreft de rechten van de betrokkene, is alvast te verwerpen dat het recht op toestemming (en de verwerking op grond daarvan) overdraagbaar zou zijn. Ook is de verdere verwerking steunend op bepaalde gronden moeilijk verdedigbaar.[239] Daarnaast bestaat tevens ruimte voor interpretatie met betrekking tot de positie van persoonsgegevens bij overgang van ondernemingen, bij faillissement of nog inzake de uitoefening van rechten in (of tegen) het belang van de nalatenschap van de betrokkene.[240]

VII.3 §5. Strikt relationele gegevens

Een laatste punt dat aandacht verdient betreft de verhouding tussen betrokkenen onderling. Hoewel dit prima facie niet rechtstreeks de verantwoordelijke aangaat, brengt het troebele gebied van de relationele gegevens en concurrerende rechten van betrokkenen wel een denkbare moeilijkheid mee voor de verantwoordelijke, waar deze bij gebrek aan sluiting over welk recht in een conflict tussen betrokkenen primeert, onmogelijk in staat kan worden geacht een juiste

[238] Art. XI.307 WER.
[239] Zie A. DE BOIS, *Economisch gebruik van persoonsgegevens in België: Hoe beïnvloedt de (nieuwe) gegevensbescherming de vrijheid van ondernemen?*, VUB, 2017, annex 'Overgang van rechten van de betrokkene'.
[240] Voor een uitgebreider standpunt met betrekking tot dit aspect, zie ibid, 8.3.4.

beslissing te nemen. Zo zal zich een dergelijke impasse voordoen bij een conflict tussen bijvoorbeeld een beroep op enerzijds het recht op vergetelheid en anderzijds het recht op overdraagbaarheid door verschillende betrokken, met betrekking tot een gezamenlijk gegeven (groepsfoto, netwerkrelaties, interactie…). In dezelfde zin kan zich de vraag worden gesteld of de verwerking van dergelijke gegevens nog steeds kan geacht worden op de toestemming van de betrokkene te steunen indien een van hen de toestemming intrekt. In elk geval poogt de verordening hier klaarblijkelijk een evenwicht te stellen door regelmatig te verwijzen naar de eventuele afbreuk aan rechten van derden, met bijvoorbeeld in overweging 68 de precisering 'rechten van andere betrokkenen'. De werkgroep artikel 29 onderstreept sporadisch dit spanningsveld en meldt dat er rekening mee moet worden gehouden[241], maar nergens wordt gezegd dat de uitoefening van rechten deze van andere rechten in de weg staat. Uitgaande van een evenwaardigheid van de verschillende rechten, lijkt het best verdedigbaar te zijn dat dergelijke conflicten worden beschouwd als een belangenconflict dat door de rechter moet worden beslecht. In afwachting van een uitspraak kan de verantwoordelijke uit voorzorg alvast de betwiste gegevens aantekenen en afschermen.

[241] Zie bijvoorbeeld Guidelines (WP29) on the right to data portability, 13 december 2016, 9-10.

VIII. Evaluatie en conclusie

VIII.1. Instrumenteel

Waar de nieuwe regeling zich onder meer voorhoudt als maatregel ten gunste van activiteiten inzake verwerking van persoonsgegevens (harmonisatie, rechtszekerheid, vertrouwen in digitale economie bevorderen…)[242], blijkt de AVG in de uitwerking eerder neer te komen op een inperking van de economische vrijheid, die weliswaar ten gunste van de interne markt kan bestaan. Anderzijds wijst de afbakening van de verwerking van persoonsgegevens a contrario op een toestemming binnen de voorwaarden van de regeling naar eigen goedwil te exploiteren. Uiteindelijk wordt met de strenge behandeling van geautomatiseerde besluitvorming allesbehalve een stimulus voor de ontwikkeling en toepassing van desbetreffende technieken gecreëerd, althans worden vooral transparante toepassingen gestimuleerd.

VIII.2. Rechtszekerheid

In het licht van de snel evoluerende verwerkingstechnologie moet sterk worden afgewogen tussen flexibiliteit en voorspelbaarheid van de regeling. Er werd in de AVG geopteerd voor een technologieneutrale benadering.[243] Zoals vermeld, gaat de invullingsruimte inzake technische aspecten (zoals beveiliging) gepaard met een beperktere rechtszekerheid. Op verschillende punten, die al zeker binnen een context van monetarisering van persoonsgegevens cruciaal zijn, laat de regeling (zelfs in toenemende mate) te wensen over. Zo bijvoorbeeld zal bij gebrek aan nadere invulling voor de situatie van uiterst complexe en onvoorspelbare automatische besluitvorming, de techniek gewoon verboden blijven wanneer die aanzienlijke gevolgen heeft voor betrokkenen en geen uitzondering van toepassing is. Dergelijk verbod kan een grote hinder vormen voor ongebreidelde ontwikkeling van nieuwe verwerkingstechnieken, waar de standaard in computertechnologie inmiddels net machinaal leren is. Er wordt uitgegaan van een verbod met ruime uitzonderingen en strikte voorwaarden, zodanig de controle over de sector bewarend, ten diens kosten. Nog inzake het gebruik van automatische procedés is op te merken dat het recht hier niet aan te worden onderworpen zich slechts uitstrekt over de situaties die rechtstreeks gevolgen hebben voor de betrokkene. Op deze wijze wordt eigenlijk niets gezegd over zuiver empirische profilering voordat die wordt toegepast op een persoon. Daarnaast is uit overweging 162 AVG af te leiden dat dergelijke profilering niet tot 'statistische doeleinden' mag worden gerekend.

Met de AVG wordt wat meer duidelijkheid verschaft omtrent de toestemmingsvereiste. Ook omtrent de actiemogelijkheden van de betrokkene wordt door de uniformere werking van de toezichthoudende autoriteiten meer voorspelbaarheid teweeggebracht. De doorgifte aan internationale organisaties wordt voortaan ook uitdrukkelijk geregeld alsook de pseudonimisering en zijn gevolgen. Daartegen zijn omtrent een aantal aspecten de zaken niet per se uitgeklaard. Zo is nog steeds geen expliciete grondslag voor het hanteren van

[242] Overweging 7 richtlijn.
[243] Overweging 15 AVG.

persoonsgegevens als betaalmiddel te vinden in de vigerende regeling (wel in een voorgestelde richtlijn). Anderzijds is in de vrijheid van ondernemen en de beperkende AVG a contrario een grondslag te lezen. Ook inzake bepaalde conflicterende belangen en rechten zijn in de regeling weinig aanwijzingen te vinden. Zo is het niet duidelijk afgebakend welke de draagwijdte van de bewaringsplicht is, hoe de concurrerende rechten van betrokkenen ten aanzien van gezamenlijke gegevens zich verhouden of nog in welke mate anderen dan de betrokkene de rechten van laatste kunnen uitoefenen, dan wel algemener wat het post-mortem- en overdrachtsregime inhouden. De draagwijdte van het nieuwe recht op overdraagbaarheid van gegevens laat tevens een aantal vraagtekens achter. Uiteindelijk is nog merkwaardig dat de rechtspraak van het arrest Schecke niet werd overgenomen in de verordening. Er wordt zelfs opnieuw expliciet naar 'de natuurlijke persoon' verwezen om de betrokkene aan te duiden. Hierdoor is niet duidelijk of de interpretatie van het Hof impliciet wordt erkend dan wel genegeerd. Of dit betekent dat de onderneming waarvan de naam wijst op deze van de achterman opnieuw buiten de regeling valt, is dus door de jurisprudentie te verfijnen. Hoe dan ook valt de onderneming niet onder de aanvullende consumentenbescherming van het WER.

Verder laat de interpretatieruimte van begrippen als 'aanmerkelijk treffen' en 'betekenisvolle informatie', alsook de troebele kwalificatie van profileringsactiviteiten in het algemeen, nogal wat twijfels achter met betrekking tot het toepassingsgebied en de invulling van de regeling rond automatische besluitvorming, wat in termen van rechtszekerheid aan de economische vrijheid zal kosten.

Voor de activiteit van specifieke databrokers (in beginsel niet op de toestemming steunend), is de regeling hoogst onduidelijk. Noch een specifieke grondslag, noch een duidelijk toepassingsgebied, noch duidelijke plichten zijn terug te vinden in de regeling. Waar weliswaar prima facie lijkt een soelaas voor de activiteit te liggen in het beroep op gezamenlijk de 'statistische doeleinden', het ontsnappen aan de informatieplicht in gevallen van 'zware last' en nu erkende pseudonimisering, laat deze constructie veel te wensen over in termen van rechtszekerheid.

Met de direct werkende aard van de verordening wordt uiteraard de harmonisatie een duwtje in de rug gegeven. Weliswaar voorziet de AVG een aantal lidstatelijk in te vullen aspecten die, gezien hun weerslag op het gedrag van marktspelers, misschien best ook op communautair niveau werden geregeld. Zo kan de uiteenlopende invulling van de technische voorschriften inzake beveiliging, de afwijkingen op de gehele regeling of nog de strafsancties uiteindelijk sterk afbreuk doen aan het harmoniserend karakter van de verordening (en de nodige compliance-kosten meebrengen). Anderzijds is de uniformiteit van sommige aspecten, zoals de aanstelling van een functionaris of de administratieve sanctionering, zeker te waarderen in termen van rechtszekerheid. In het licht van de mogelijke voorbehouden is uiteindelijk niets minder zeker dan dat de verordening zijn harmoniserend doel ten voordele van transnationaal actieve ondernemingen bereikt.

VIII.3. Afweging van belangen

Het belangrijkste spanningsveld binnen het besproken kader is dat tussen enerzijds de economische belangen van de verwerkende onderneming en anderzijds het recht op privacy en bescherming van de persoonsgegevens van de betrokkene. De regeling straalt voornamelijk een inperking van de andere belangen ten voordele van de bescherming van betrokkenen uit. Zo blijkt niet enkel uit de verbijzondering van het recht op privacy als centraal element in de overwegingen van de verschillende instrumenten, maar tevens uit de compositie van de regelingen zelf, zoals bijvoorbeeld de numerus clausus inzake de verwerkingsgronden.

Anderzijds blijkt uit andere bepalingen een afbakening van de rechten van de betrokkene ten gunste van andere belangen. Zo zal de transparantie ten gunste van de betrokkene soms moeten wijken voor het auteursrecht, eigendomsrechten en bedrijfsgeheim, zonder dat dit evenwel het recht van de betrokkene volledig neutraliseert, wat dan weer wijst op een uiteindelijke voorrang van het recht van laatste. Ook inzake de bescherming van betrokkenen zelf, bijvoorbeeld met betrekking tot het hergebruik van gegevens, wordt verwezen naar een aantal andere belangen waarvoor de bescherming kan worden overruled. Weliswaar opnieuw met ultiem een verwijzing naar evenredigheid ten aanzien van de gegevensbescherming. Zo kan tevens worden verwezen naar de beperkingen op het recht op vergetelheid (die weliswaar boven de vrijheid van ondernemen werd ingeschat in het arrest Google).

Ter bescherming van de vrijheid van ondernemen wordt doorheen de regeling een afbakening van de gegevensbescherming uitgetekend. Sommige evaluaties, zoals de beoordeling van de beveiliging en inzake anonimisering, worden gevoerd in het licht van de redelijke verwachtingen van ondernemingen, alsook de kosten die met de voldoening aan de vereisten gepaard gaan. Daarnaast worden tevens sommige plichten, zoals de aanstelling van een functionaris en bepaalde kennisgevingsplichten, getoetst aan de mogelijkheden van de betrokken onderneming. Met de AVG werden bepaalde kostelijke verplichtingen verlaten of uit praktische overwegingen gemoduleerd. Voortaan zal bijvoorbeeld geen verplichte aangifte van automatische verwerking meer moeten gebeuren, maar wordt dit beperkt tot situaties die een verhoogd risico inhouden.[244] Anderzijds wordt daar weer een nieuwe plicht tot het bijhouden van een register ingevoerd. Het onderscheid binnen de informatieplichten bij verwerking voor eenzelfde, dan wel een nieuw doel, wijst eveneens op zekere zin voor de belangen van de ondernemer. Ook is bijvoorbeeld te wijzen naar artikel 11 AVG, waarnaar de verantwoordelijke niet kan worden gedwongen worden aanvullende gegevens te verzamelen voorbij de identificatievereiste. Weliswaar valt in dat verband opnieuw te verwijzen naar het arrest Rijkeboer en desbetreffende discussie inzake bewaringsplicht.

Met betrekking tot de transparantieplicht kunnen een aantal bedenkingen worden gemaakt. Vooreerst is alvast niet te ontkennen dat de regeling in zijn geheel steeds meer -al zeker met de AVG- naar transparantie ten gunste van de betrokkene kantelt, doch inzake bepaalde aspecten naar evenwicht streeft, zoals bijvoorbeeld met de vereiste van communicatie op maat.

[244] Overweging 89 AVG.

Weliswaar zou het misschien wenselijk zijn om de transparantieplicht op sommige vlakken aan te passen. Zo is in de huidige regeling de betrokkene nog steeds niet op de hoogte van de economische waarde van zijn persoonsgegevens en nog minder van de daadwerkelijke risico's (specifieker dan *gevolgen*, in die zin dat het ook weinig waarschijnlijke risico's omvat die desondanks een enorme weerslag kunnen hebben op de betrokkene, denk maar aan een datalek) die gepaard gaan met de vrijgeving ervan. Het is dus moeilijk houdbaar dat de betrokkene daadwerkelijk geïnformeerd instemt met de verwerking, waar deze in geen enkele richting over de instrumenten beschikt om de waarde van de overeenkomst in te schatten. Het is waarschijnlijk dat dergelijke informatieplichten soms economische zelfmoord kunnen inhouden – anderzijds worden dan sommige transparantieplichten (bijvoorbeeld logica) opgelegd die ontegensprekelijk botsen met de vrijheid van ondernemen en intellectuele eigendom -, maar er is dan ook geen enkele stap in die richting gezet doorheen de hele regeling, hoewel, zoals aangehaald door de Commissie, de ongelijke behandeling van data-centrische ondernemingen hiermee in de hand wordt gewerkt.[245] Als verzachte versie zou kunnen worden gedacht aan bijvoorbeeld een verplichte verwijzing naar bepaalde informatiepunten of organen, zoals in andere sectoren reeds het geval is. Uiteindelijk valt in dit verband opnieuw aan te halen dat parallel aan de gegevensbescherming uit de specifieke regeling, in de verhouding met consumenten een aanvullende bescherming te vinden is in het (ondertussen niet meer zo nieuwe) WER.

Er zijn nog een aantal opmerkingen te maken inzake delicate spanningsvelden binnen de beschermingsregeling. Een eerste punt is dat de strenge beperking van het hergebruik (incompatibele of vervallen grond) van gegevens niet enkel op het niveau van de kosten (nieuwe toestemming vragen, nieuwe toets voeren met betrekking tot elk gegeven) een inperking van de ondernemingsvrijheid inhoudt, maar tevens sterk afbreuk doet aan de vrijheid van ondernemen in die zin dat waar de persoonsgegevens als vorm van kapitaal worden aangewend, de flexibiliteit van ondernemingen enorm wordt belemmerd. De combinatie van de verzwaarde proportionaliteitstoets ten aanzien van het doel (nu 'noodzakelijk') en de verstrengde eisen inzake communicatie (nu begrijpelijk in functie van het publiek, alsook nieuwe informatieplichten) zullen onweerlegbaar een impact hebben op de flexibiliteit van data-intensieve ondernemingen, zowel in termen van wijzigingen (beleid, herstructureringen,…) als in termen van hergebruik van gegevens en interpretatieruimte van toestemmingen. Ook voor overnames en herstructureringen is de situatie moeilijker gemaakt, waar bijvoorbeeld een mogelijks zware re-identificatieplicht kan opduiken ter voldoening van de informatievereisten. Daarnaast wordt met het recht op overdraagbaarheid ook een deuk in de eigendomsrechten van de databankhouder gemaakt, waar nu de rechtmatige gebruiker voortvloeiend uit een andere regeling dan het intellectueel eigendomsrecht zijn rechten op de inhoud versterkt ziet.

Waar de zaak, al zeker met het intreden van de AVG, klaarblijkelijk het zwaarst knaagt aan de vrijheid van ondernemen, is in de regeling omtrent geautomatiseerde besluitvorming. Zowel inhoudelijk als in termen van rechtszekerheid wordt hiermee de dataverwerkingssector zwaar

[245] Overweging 13 ontwerp richtlijn contracten over digitale inhoud. Zie ook artikel 3, 4 van de richtlijn.

geraakt. Om te beginnen is (m.i) de combinatie van meerdere bepalingen ten gunste van de betrokkene in dit verband erg verregaand. De uitgebreide transparantieplicht omtrent de logica van de besluitvorming op zichzelf komt al erg intrusief over in verhouding tot het bedrijfsgeheim en de intellectuele eigendom. Daarnaast geniet de betrokkene tevens een recht hier uiteindelijk niet aan te worden onderworpen, wat in het licht van het recht op menselijke tussenkomst bovendien een significante rem op de economische vrijheid van kleine ondernemingen kan vormen. Hierbij komt dan nog eens een verplichte gegevensbeschermingseffectbeoordeling kijken, bovenop de verstrengde maatregelen ter bescherming door ontwerp. Naast het mogelijk afremmen van concrete profilering, sluit deze combinatie *de facto* een aantal kleinere ondernemingen uit van het aanwenden van automatische besluitvorming voor zover die niet onder de uitzonderingen valt.

Algemener heeft de regeling op verschillende vlakken een mogelijks nefaste impact op de mogelijkheden van nieuwkomers. Zo zullen kleine, data-intensieve ondernemingen vooraleer in dezelfde race als gevestigde spelers te zitten, moeten kampen met een gegevensbeschermingseffectbeoordelingsplicht, een verplichting inzake registers van automatische verwerkingen, plichten inzake geautomatiseerde besluitvorming (waaronder een discuteerbaar recht op menselijke tussenkomst) en uiteindelijk een de facto uitsluiting van op maat gemaakte bindende bedrijfsvoorschriften als waarborg voor de doorgifte. In deze optiek komt de regeling neer op een vooropstelling van reeds gevestigde ondernemingen, waar net de dataverwerkingssector er een is waarin veel opportuniteit ligt voor starters. Hiermee wordt de regeling (m.i.) geacht in substantiële mate afbreuk te doen aan de vrijheid van mededinging (als element van de vrijheid van ondernemen).

Tot slot valt te vermelden dat met het Comité uit artikel 68 AVG een opvolger van WP29 als forum ter bespreking van de conflicten en spanningsvelden inzake de verwerking van persoonsgegevens, wordt tot stand gebracht.

VIII.4. Conclusie

In het kader van de moderne communicatie en andere relevante technologie is het nodig dat de bescherming zo uniform mogelijk is, daar persoonsgegevens in de eerste plaats niet door en voor lokale spelers worden verwerkt. In die zin is het in het voordeel van zowel de betrokkenen als van de gehele digitale markt dat de regeling doorzichtig en consistent is. Op het niveau van de Unie is dit in toenemende mate het geval. Op het internationale toneel zijn er echter nog wat haperingen vast te stellen, bijvoorbeeld inzake de Privacy-Shield regeling met de Verenigde Staten.

In toenemende mate lijkt de regeling tevens te varen van een repressieve bescherming en aansprakelijkheden, naar een bescherming door ontwerp en voorafgaande safeguards, zoals nieuwe informatieplichten, aanspreekpunten, toezichthoudende organen, waarborgen… In het kader van de snel evoluerende technologie, meer bepaald met het oog op de kolossale -en nog steeds exponentieel toenemende- volumes gegevens die vandaag worden verwerkt, is het dan

ook meer dan logisch dat wordt bewogen naar een voorkomen eerder dan genezen. Ook het reactieve luik is echter het voorwerp van een toenemend beschermende aard (collectieve actie, bevoegdheden van autoriteiten…). De totale schade die vandaag bijvoorbeeld uit een datalek voortvloeit, is dan ook in veelvouden van deze van decennia geleden te berekenen, zowel in schaal als in intensiteit (volume gegevens, persoonlijk karakter ervan…). Het is vanuit eenzelfde optiek te verklaren dat het belang van de gegevensbescherming steeds meer wordt onderstreept (Handvest, rechtspraak, verordening…), waar de schade van een inbreuk hierop steeds meer verderstrekkende gevolgen kan hebben. Anderzijds is de toenemende intensiteit van de regulering ter zake erg drukkend op de vrijheid van ondernemen binnen de data-sector, bijvoorbeeld met betrekking tot geautomatiseerde besluitvorming of nog waar weinig rekening wordt gehouden met de flexibiliteit die wordt geboden aan kleine ondernemingen binnen de sector.

Op het Belgische niveau zitten we voorlopig in een tussenfase. De omschrijving van de rechten en plichten in nationale wetgeving zal vervallen nu de AVG zonder omzetting van toepassing is (noteer dat dit niet in alle lidstaten is doorgedrongen).[246] Waar echter een belangrijke speelruimte zich voordoet is in de regeling van de gerechtelijke aspecten alsook de technische invulling van de beveiligingssystemen, meer in het bijzonder inzake de nieuwe nadruk op bescherming door ontwerp. Het lijkt zeer waarschijnlijk dat het eerste aspect analoog aan de Privacywet aan de rechtbank van eerste aanleg zoals in kortgeding wordt overgelaten, daar het doorsnee conflict omtrent persoonsgegevens een dringende en permanente uitspraak vereist. Wat de technische voorschriften betreft, daartegen, is moeilijk in te schatten waar we naartoe gaan. Hierbinnen moet nog eens worden afgewogen tussen de flexibiliteit van de regeling in het licht van de snel evoluerende verwerkingstechnieken en de daadwerkelijk beschermende impact van de voorschriften.

Al bij al kan de nieuwe regeling geacht worden wat laat aangekomen te zijn in het licht van het reeds universele karakter van de gegevensverwerking, de volumes die vandaag reeds verwerkt worden en de complexiteit van de verwerkingstechnieken, maar de progressieve en flexibele aard van de laatste legislatieve stukken zouden wel eens kunnen compenseren voor deze achterstand. Uiteindelijk is vanwege deze soepelheid omtrent een aantal zaken dringend een invulling of afbakening van rechten nodig, al zeker waar het continentale stelsel voorspelbaarheid preekt.

Tot slot wordt (weinig verrassend) geconcludeerd dat de nieuwe gegevensbeschermingsregeling -al zeker waar deze wordt voorgehouden als bestaande ter bevordering van de digitale economie en de interne markt- sterk drukt de ondernemingsvrijheid, voornamelijk door het toenemende aantal plichten voor de relevante ondernemingen; verplichte gegevenseffectbeoordeling, eisen inzake transparantie (informatieplichten en communicatie op maat, al zeker waar het om ingewikkelde informatie naar een leek toe gaat), eisen van bescherming door ontwerp (weliswaar

[246] Zie bijvoorbeeld de situatie in Duitsland: http://privacylawblog.fieldfisher.com/2017/data-protection-does-the-german-implementation-act-bdsg-e-undermine-the-gdpr/.

in het licht van beschikbare middelen en techniek, niettemin bijkomende kosten), verplichte functionaris, kosteloze toegang en uiteindelijk onduidelijke termen en toepassingsgebied.