UHASSELT
KNOWLEDGE IN ACTION

KU LEUVEN

Maastricht University

Faculteit Rechten

master in de rechten

Masterthesis

De samenwerkingsband tussen de Algemene Verordening Gegevensbescherming en het voorstel voor een Verordening betreffende Artificiële Intelligentie

Alexander Broux

Scriptie ingediend tot het behalen van de graad van master in de rechten, afstudeerrichting rechten

PROMOTOR :

Prof. dr. Ken ANDRIES

2021
2022

UHASSELT
KNOWLEDGE IN ACTION

KU LEUVEN

Maastricht University

Faculteit Rechten

master in de rechten

Masterthesis

De samenwerkingsband tussen de Algemene Verordening Gegevensbescherming en het voorstel voor een Verordening betreffende Artificiële Intelligentie

Alexander Broux

Scriptie ingediend tot het behalen van de graad van master in de rechten, afstudeerrichting rechten

PROMOTOR :

Prof. dr. Ken ANDRIES

Samenvatting

Artificiële intelligentie is de dag van vandaag overal om ons heen te vinden. Het heeft, gelet op de graad van integratie in onze samenleving, bijzonder lang op zich laten wachten alvorens de wetgever deze familie van technologieën van een regelgevend kader probeerde te voorzien. Hierin wordt verandering gebracht met het voorstel van AI-verordening dat op 21 april 2021 werd ingediend.

Deze masterscriptie onderzoekt of dit Voorstel, in samenwerking met het reeds bestaande gegevensbeschermingsregime onder de GDPR voldoende performant zal zijn om tegemoet te komen aan enkele van de meest pertinente risico's voor het recht op bescherming van persoonsgegevens en dit ook zal blijven voor ten minste de voorzienbare toekomst.

Om hierop een antwoord te bieden wordt in het eerste deel gekeken naar wat artificiële intelligentie nu net is. Hoewel de existentiële vraag naar: "Wat is intelligentie?" - zeer interessant is, wordt in deze scriptie enkel ingegaan op de invulling ervan in het kader van het Voorstel. In een tweede hoofdstuk onder dit deel wordt gekeken naar allerhande voor- en nadelen die AI-toepassingen met zich meebrengen en hoe de EU-wetgever aangeeft met deze risicoanalyses te zijn omgegaan.

Hoofdstuk 3 bespreekt de vrucht van hun werk: de krachtlijnen van het voorstel van AI-verordening, dat gekenmerkt wordt door haar risicogebaseerde aanpak, waarbij enkele AI-systemen worden verboden, enkelen worden gecategoriseerd als hoog-risico systemen en de rest wordt gelaten in een restcategorie van niet tot laag risico AI-toepassingen. Het gros van het Voorstel is enkel van toepassing op de categorie met hoog risico.

Het tweede deel bespreekt in hetzelfde stramien enkele kernbegrippen in het privacyrecht en in het gegevensbeschermingsrecht alvorens over te gaan tot de krachtlijnen van de GDPR, die zich voornamelijk kenmerken door de in artikel 5 vervatte beginselen inzake verwerking van persoonsgegevens.

Alvorens een conclusie te formuleren over de elementen die in het corpus van deze scriptie worden besproken, wordt in het derde deel gekeken naar de verhouding tussen de twee (toekomstige) verordeningen; De verantwoordelijke personen worden geïdentificeerd en de toepassingsgebieden worden naast elkaar gelegd. Verder gaat het derde deel ook in op de manier waarop het pasgeboren AI-recht omgaat met de uitdagingen op het vlak van bescherming van persoonsgegevens en wordt een opmerking geformuleerd bij de definiëring van AI.

Dankwoord

Na jaren van bloed, zweet en koffie kan ik met enige trots de u vandaag voorliggende scriptie tot behalen van de graad van master in de rechten aan de Universiteit Hasselt presenteren. Omdat ik doorheen dit hele traject niet alleen heb moeten staan, zijn enkele woorden van dank zeker op hun plaats.

In de eerste plaats zou ik graag mijn promotor, Prof. Dr. Ken Andries bedanken om mijn hoofd bij de zaak te houden en mij mezelf niet te laten verliezen in de eindeloze zeeën aan interessante literatuur die mijn onderwerp rijk is.

Vervolgens gaat mijn dank uit naar mijn vrienden en familie, die tijdens het schrijfproces geduldig mijn monologen hebben aanhoord en soms kritische vragen stelden waardoor dit werk zonder twijfel naar een hoger niveau getild kon worden. Ook is het een vermelding waard dat ze mij doorheen mijn hele opleidingstraject steeds hebben gesteund en voor off-campus ontspanning en plezier hebben gezorgd.

Een bijzonder dankwoord mag ook worden gericht aan mijn vriendin. Alles wat mijn vrienden hebben moeten verduren, heeft zij in een veelvoud over zich heen gekregen. Uren heeft ze geduldig geluisterd naar woordenregens over een onderwerp dat haar maar weinig zegt, en als klap op de vuurpijl heeft ze ook nog dit werk nagelezen.

De laatste en voornaamste "dankuwel" is gericht aan mijn ouders, en in het bijzonder aan mijn moeder. Deze laatste "merci" telt dan ook voor veel meer dan enkel de ondersteuning tijdens het schrijven van deze scriptie. Zij hebben er steeds voor gezorgd dat ik alle kansen die mij geboden werden met twee handen kon aangrijpen.

Inhoudsopgave

Lijst van afkortingen

(voorstel van) AI-verordening	Voorstel (Comm.) voor een verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van bepaalde wetgevingshandelingen van de Unie, 21 april 2021, 2021/0106 [COD].
AGI	Artificial General Intelligence / Algemene Artificiële Intelligentie.
AI	Artificiële Intelligentie / Kunstmatige intelligentie.
AI HLEG	High-Level Expert Group on Artificial Intelligence / Deskundigengroep op Hoog Niveau inzake Kunstmatige Intelligentie.
ANI	Artificial Narrow Intelligence / Beperkte Artificiële Intelligentie / Tweede generatie Artificiële Intelligentie.
ASI	Artificial Super Intelligence.
BUPO / IVBPR	Internationaal Verdrag inzake Burgerrechten en Politieke Rechten van 16 december 1966.
CAO	Collectieve Arbeidsovereenkomst.
DPIA	Data Protection Impact Assessment / Gegevensbeschermingseffectenbeoordeling.
DPO	Data Protection Officer / Functionaris voor gegevensbescherming.
EU	Europese Unie.
EVRM	Europees Verdrag voor de Rechten van de Mens van 4 november 1950.
GDPR	Algemene Verordening Gegevensbescherming / AVG / Verordening (EU), 2016/679 van het Europees Parlement en de Raad tot 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.
HvJ-EU	Hof van Justitie van de Europese Unie.
IoT	Internet of Things.
RvE	Raad van Europa.

VR	Virtual Reality.
White Paper / Witboek	White Paper (Comm.) on Artificial Intelligence – A European approach to excellence and trust, 19 February 2020, COM (2020) 65 final. / Witboek (Comm.) over kunstmatige intelligentie – Een Europese benadering op basis van excellentie en vertrouwen, 19 februari 2020, COM (2020) 65 final.
Handvest Grondrechten	Handvest van de Grondrechten van de Europese Unie, van 14 december 2007, (2007/C 303/01).
GBA	Gegevensbeschermingsautoriteit.
Rechtshandhavingsrichtlijn	Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

Lijst van figuren

Inleiding

1. Situering van het onderzoek

1. **OPZET.** Op 21 april 2021 werd door de Europese Commissie een voorstel ingediend bij het Europees Parlement om een verordening tot stand te brengen met betrekking tot artificiële intelligentie. Tot op heden bestaat hierover nog geen juridisch bindend kader.

Op 25 mei 2018 trad de Algemene Verordening Gegevensbescherming (AVG / GDPR)[1] in werking waarmee de persoonsgegevens van EU-burgers in belangrijke mate worden beschermd in het kader van de verwerkingen ervan. De GDPR geeft datasubjecten inzage in en controle over wie er op welk moment en voor welke doeleinden toegang krijgt tot hun persoonsgegevens.

Deze scriptie zal, rekening houdend met deze twee instrumenten, onderzoeken hoe ze op elkaar inspelen en hoe de regelgeving met betrekking tot de verwerking van persoonsgegevens door en voor Artificiële Intelligent (AI)[2] zal evolueren.

2. **ARTIFICIËLE INTELLIGENTIE.** Artificiële intelligentie is een nieuwe en spannende, maar ook onvoorstelbaar gevaarlijke technologie, die een enorm hoeveelheid kansen met zich meebrengt voor de toekomst maar ook het einde van de mensheid kan betekenen wanneer we niet goed opletten… Of dat is toch de denkpiste die wordt bewandeld in verschillende (post-) apocalyptische films en boeken in het *Science Fiction* genre.[3]

Het onderzoeksveld dat werkzaam is in deze sector tracht niets minder te bereiken dat het evenaren van het menselijke brein in een machine.[4] Heiligschennis voor sommigen, de laatste stap in onze evolutie voor anderen, maar op dit moment vooral nog een droom. Hoewel AI reeds aanwezig is in veel aspecten van ons dagelijks leven,[5] is er nog geen concreet zicht op de ontwikkeling van een algemene artificiële intelligentie. Zelfrijdende auto's[6] zijn echter niet langer een onbereikbare fantasie, virtuele assistenten

---

[1] Hoewel de officiële afkorting van de Algemene Verordening Gegevensbescherming in Nederlandstalige landen eigenlijk "AVG" is, volgt de praktijk in België dit voorschrift eigenlijk niet. Nagenoeg elke keer dat deze Verordening ter sprake komt, wordt ernaar verwezen met de Engelstalige afkorting "GDPR". Deze scriptie zal zich bedienen van deze laatste, in België meer courante afkorting.

[2] Artificiële intelligentie wordt in Nederlandstalige lectuur ook regelmatig aangeduid als "Kunstmatige Intelligentie". Dit zijn inhoudelijk exact dezelfde concepten.

[3] De voorbeelden van AI in science fiction zijn eindeloos. Daarom worden *ad random* enkele van de bekendste werken genoemd: *Metropolis* (Film, 1927); A.C. CLARKE, *2001: A Space Odyssey* (Boek, 1968); D. ADAMS, *The Hitch Hiker's Guide to the Galaxy* (Boek, 1978); I. ASIMOV, *I, Robot* (Boek, 1940-1950; Film, 2004); *Ex Machina* (Film, 2014); …
Als interessante bijkomende lectuur wordt verwezen naar: S. CAVE, K. DIHAL & S. DILLON (eds.), *AI Narratives: A History of Imaginative Thinking about Intelligent Machines*, Oxford, Oxford University Press, 2020, 448p, https://doi.org/10.1093/oso/9780198846666.001.0001.

[4] F. ABBASI, "The pursuit to creating the most human-like AI", *Technative* 10 december 2020, https://technative.io/the-pursuit-to-creating-the-most-human-like-ai/; L. PERSONA, "AI still needs humans to stay intelligent—here's why", *Technative*, 27 april 2022, https://technative.io/ai-still-needs-humans-to-stay-intelligent-heres-why/; L. CLARKE, "Forget the hype, we have no idea how to reach human-like artificial intelligence", *Techmonitor* 13 mei 2021, https://techmonitor.ai/technology/we-have-no-idea-how-to-reach-human-like-artificial-intelligence; …

[5] X, "AI in Daily Life", *Exponenta.io* 23 februari 2021, https://exponenta.io/ai-in-daily-life/; C.A. PICKOVER, *Kunstmatige Intelligentie – Van middeleeuwse robots tot neurale netwerken: Een chronologisch overzicht*, Kerkdriel (Nederland), Librero, 2021, p. VIII-XI; WITBOEK (Comm.) over kunstmatige intelligentie – een Europese benadering op basis van excellentie en vertrouwen, 19 februari 2020, COM (2020) 65 final, p. 1; …

[6] R. ZALLONE, "Artificial Intelligence vs Autonomous Cars vs General Data Protection Regulation", *AEIT International Conference of Electrical Technologies for Automotive* 2020, p. 1-6, https://doi.org/10.23919/AEITAUTOMOTIVE50086.2020.9307410.

zoals Bixby,[7] Samantha,[8] Alexa[9] en Mycroft[10] helpen vandaag al duizenden mensen wereldwijd en sinds 1997 winnen computers matchen schaak tegen menselijke Grootmeesters.[11]

Ook minder opvallende of impressionante technologieën kunnen onder de verzamelterm AI worden geplaatst: denk hierbij aan oa. Zoekmachines,[12] suggesties op Netflix en geautomatiseerde fabrieken in de assemblage-industrie.[13]

Het einde van de mensheid is op dit moment nog niet in zicht, maar dat wilt niet zeggen dat AI niet hoognodig gereguleerd moet worden. Het is namelijk een veel te nuttige groep technologieën om niet te gebruiken en stof te laten vangen. Dit gebruik brengt onvermijdelijk enkele risico's met zich mee, waarvan niet het minste voor het recht op privacy. Het favoriete voedsel van deze machines is namelijk data. AI biedt de mogelijkheid aan machtigere, kapitaalkrachtigere partijen om persoonsgegevens makkelijker, sneller en in veel grotere hoeveelheden te verwerken. Uit de definitie die door Andreas Kaplan en Michael Haenlein werd verwoord,[14] kan worden afgeleid dat dataverwerking een zeer belangrijk aspect van AI is.

De Europese wetgever kwam aan de vraag om duidelijkheid omtrent AI tegemoet op 21 april 2021 met het "*Voorstel van Verordening tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van bepaalde wetgevingshandelingen van de Unie*" (Verder voorstel AI-verordening). In tegenstelling tot de GDPR, heeft de toekomstige AI-verordening geen voorloper. Ze is dus de eerste wetgevende tekst op EU-niveau die zich specifiek op AI richt. Daarom is het dus niet zo moeilijk om hier enkele vraagtekens bij te plaatsen en dat is wat deze masterscriptie ook zal doen.

3. PRIVACY & VERWERKING VAN PERSOONSGEGEVENS. Het recht op eerbiediging van het privéleven, het recht op eerbiediging van het gezinsleven, de onschendbaarheid van de gezinswoning, het briefgeheim, "*the right to be let alone*", "*data protection*", … Allen worden in één adem uitgesproken wanneer het gaat over het recht op privacy. Iedereen wilt zijn privacy behouden en velen onder ons zullen op de muur gaan staan om dit fundamenteel grondrecht te verdedigen wanneer het al te veel wordt bedreigd.

Mensen zijn zich zeer bewust van hun recht op privacy, mede omdat het door verschillende prominente figuren wereldwijd regelmatig in de reguliere media wordt aangehaald.[15] Toch is er sinds de introductie van sociale media begin/halverwege de jaren 2000 een trend waar te nemen waarin mensen op een

[7] SAMSUNG, "What is bixby?", *Samsung.com*, https://www.samsung.com/global/galaxy/what-is/bixby/.
[8] SAMSUNG, "Vraag het Sam!", *Samsung.com*, https://www.samsung.com/be/chatbot-sam/.
[9] AMAZON, "Top 10 Alexa features for spring", *Amazon.com*, https://www.amazon.com/b?node=21576558011.
[10] MYCROFT, "The Private and Open Voice Assistant", *Mycroft.ai*, https://mycroft.ai/.
[11] IBM, "Deep Blue", *IBM.com*, https://www.ibm.com/ibm/history/ibm100/us/en/icons/deepblue/; → Dit werd ondertussen ook al verbeterd door een andere AI-toepassing: O. VAN MILTENBURG, "Zelflerende AI wint van 's werelds bekendste schaakengine", *Tweakers* 19 april 2019, https://tweakers.net/nieuws/151828/zelflerende-ai-wint-van-s-werelds-bekendste-schaakengine.html.
[12] Google.com; Yahoo.com; DuckDuckGo.com,
[13] X, "Smart factories: dé slimme fabrieken van de toekomst", *Mecalux.be* 1 maart 2022, https://www.mecalux.be/blog/smart-factories-slimme-fabrieken-toekomst; …
[14] "H*et vermogen van een systeem om externe gegevens correct te interpreteren, om te leren van deze gegevens, en om deze lessen te gebruiken om specifieke doelen en taken te verwezenlijken via flexibele aanpassing.*" in: A. KAPLAN & M. HAENLEIN, "Siri, Siri in my Hand, who's the Fairest in the Land? On the Interpretations, Illustrations and Implications of Artificial Intelligence", *Business Horizons 2018*, vol. 62(1), 15-25.
[15] Denk aan Edward Snowden, Maximilian Schrems, Hoorzitting Marc Zuckerberg, onrust omtrent de covid safe app, …

bijna systematische manier alles wat ze doen en meemaken op een dag, online zetten.[16] Dit fenomeen beperkt zich niet tot de zogenaamde "*influencers*" maar ook jij, ik en Jan met de pet delen ons leven met bijna letterlijk iedereen ter wereld met een internetconnectie. Het feit dat we ons bewust zijn van het belang van privacy en het tegenstrijdige feit dat we ons hiernaar niet gedragen online, wordt de "*Privacy paradox*" genoemd.[17]

Platformen zoals Facebook (Meta), Instagram (Meta), LinkedIn, Twitter, Google, maar ook Apple en Samsung hebben onze data tot één hun belangrijkste handelsgoederen gemaakt.[18] Elektriciteitsleveranciers weten wat, wanneer, hoeveel en op welke plek in onze huizen stroom verbruikt via het *Internet of Things*[19] en met de opkomst van *Smart-Devices* en zelfs *Smart-Homes* delen we nu uit eigen vrije wil elke stap die we binnen of buiten de geborgenheid van onze woning zetten.[20]

Dit kan al tellen als schets van de huidige stand van zaken betreffende ons recht op privacy. Gelukkig moet dit, zoals bijna alles in deze wereld genuanceerd worden. Privacy is wel degelijk van groot belang en het feit dat de bezorgdheid hieromtrent zo wijdverspreid en actueel is, toont duidelijk aan dat het onderwerp leeft[21]. Verschillende privacy activisten zoals oa. Maximilian Schrems (NOYB)[22] en in eigen land het Ministry of Privacy[23], zetten zich dagelijks in om ons grondrecht te beschermen. Ook bij de verschillende instanties die zich aan de wetgeving dienen te houden is men permanent op zijn hoede om geen al te grote inbreuken te maken.[24]

---

[16] C. RIDINGS, D. GEFEN & B. ARINZE, "Psychological Barriers: Lurker and Poster Motivation and Behavior in Online Communities", *Communications of the Association for Information Systems* (vol. 18, article 16) 10 juni 2006, p. 329-354, https://doi.org/10.17705/1CAIS.01816.

[17] M. TADDICKEN, "The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure", *Journal of Computer-Mediated Communication* (vol. 19, issue 2) 1 januari 2014, p. 248-273, https://doi.org/10.1111/jcc4.12052; C. POITRAS, "The Privacy Paradox", *UConn Today* 18 augustus 2016, https://today.uconn.edu/2016/08/privacy-paradox/#; N. PELUSI, "The Privacy Paradox", *Psychology Today* November 2007 (laatst herzien 9 juni 2016, https://www.psychologytoday.com/us/articles/200711/the-privacy-paradox; S. BARTH & M.D.T. DE JONG, "The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review", *Telematics and Informatics* (vol. 34, issue 7) November 2017, p. 1038-1058, https://doi.org/10.1016/j.tele.2017.04.013; O. KERR, "The Privacy Paradox", *The Washington Post* 21 mei 2015, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/05/21/the-privacy-paradox/; B. WITTES & J.C. LIU, "The privacy paradox: The privacy benefits of privacy threats", *Centre for Technology Innovation at Brookings* mei 2015, 21p, https://www.brookings.edu/wp-content/uploads/2016/06/Wittes-and-Liu_Privacy-paradox_v10.pdf; …

[18] Y. ZHAO, Y. YU, Y. LI, H. HAN & X. DU, "Machine learning based privacy-preserving fair data trading in big data market", *Information Sciences* (vol. 478) april 2019, p. 449-460, https://doi.org/10.1016/j.ins.2018.11.028; S. DELGADO-SEGURA, C. PÉREZ-SOLÀ, G. NAVARRO-ARRIBAS, J. HERRERA-JOANCOMARTÍ, "A fair protocol for data trading based on Bitcoin transactions", *Future Generation Computer Systems* (vol. 107) juni 2020, p. 832-840, https://doi.org/10.1016/j.future.2017.08.021; …

[19] C. BEKARA, "Security Issues and Challenges for the IoT-based Smart Grid", *Procedia Computer Science* (vol 34) 2014, p. 532-537, https://doi.org/10.1016/j.procs.2014.07.064; …

[20] B.L. RISTESKA STOJKOSKA, K.V. TRIVODALIEV, "A review of Internet of Things for smart home: Challenges and solutions", *Journal of Cleaner Production* (vol. 140, part 3) 1 januari 2017, p. 1454-1464, https://doi.org/10.1016/j.jclepro.2016.10.006; A. SAAD AL-SUMAITI, M.H. AHMED & M.M.A. SALAMA, "Smart Home Activities: A Literature Review", *Electric Power Components and Systems* 5 februari 2014, p. 294-305, https://doi.org/10.1080/15325008.2013.832439; …

[21] S. BARTH & M.D.T. DE JONG, "The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review", *Telematics and Informatics* (vol. 34, issue 7) November 2017, p. 1038-1058, https://doi.org/10.1016/j.tele.2017.04.013; A. GOLDFARB & C. TUCKER, "Shifts in Privacy Concerns." *American Economic Review* (vol. 103, nummer 3) mei 2012, p. 349-53, http://dx.doi.org/10.1257/aer.102.3.349; …

[22] https://noyb.eu/en.

[23] https://ministryofprivacy.eu/.

[24] Verordeningen zijn rechtstreeks toepasbare wetgevingsinitiatieven die uitgaan van het supranationaal niveau, *in casu* de Europese Unie. In de hiërarchie der normen moet deze dus worden geplaatst boven de gewone wetten van lidstaten. Instanties die zich aan de Algemene Verordening Gegevensbescherming dienen te houden zijn dus niet enkel private rechtspersonen, maar kunnen zeker ook overheden zijn. Kort samengevat: quasi iedere persoon, onderneming of overheidsinstantie, die ook maar enige verwerking van persoonsgegevens uitvoert of doet uitvoeren, moet ten minste eens een grondige blik werpen op de GDPR. Dit met uitzondering van de instanties die onder het toepassingsgebied van andere gegevensbeschermingsregulering zouden vallen.

Het belang van privacy, en meer bepaald één aspect ervan: de verwerking van persoonsgegevens, werd op 25 mei 2018 in belangrijke mate in de verf gezet door de inwerkingtreding van de "*Verordening 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*" (AVG/GDPR).[25] Sindsdien hebben datasubjecten zelf controlemogelijkheden om te bepalen wie er op welk moment en voor welke doeleinden toegang krijgt tot hun persoonsgegevens.

[25] VERORDENING (EU), 2016/679 van het Europees Parlement en de Raad tot 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.

2. Onderzoeksvragen en -methodologie

4. CENTRALE ONDERZOEKSVRAAG. Als centrale onderzoeksvraag, waarop op het einde van dit onderzoek een antwoord geformuleerd zal worden, geldt:

Hoe verhouden de Algemene Verordening Gegevensbescherming en het voorstel van Artificiële Intelligentie-Verordening zich tot elkaar met betrekking tot het recht op privacy als een fundamenteel mensenrecht?

5. SUBONDERZOEKSVRAGEN. Om een goed onderbouwde conclusie te formuleren, moeten eerst verschillende subonderzoeksvragen worden beantwoord, zoals in eerste instantie:

- *Wat is "artificiële intelligentie"?*
- *Wat houdt het "recht op privacy" in?*
- *Wat houdt het "recht op bescherming van persoonsgegevens" in?*

De antwoorden op deze definiërende en beschrijvende vragen werden via rechtsdogmatisch onderzoek en een literatuurstudie gevonden. Artificiële intelligentie is een onderzoeksveld dat totaal los staat van de juridische sferen waarin een rechtenopleiding vertoeft. Daarom was het voor deze masterscriptie niet voldoende om enkel een rechts-dogmatisch onderzoek te voeren. Om het technische aspect van AI toe te lichten werd een intensieve literatuurstudie in deze sector verricht.

Een volgend soort vragen dat gesteld moet worden zijn de juridisch inhoudelijke vragen. Er worden twee EU-rechtelijke instrumenten besproken en dus moet er logischerwijze ook naar hun inhoud en implementering worden gekeken.

- *Wat zijn de krachtlijnen van het voorstel van AI-verordening?*
- *Wat zijn de krachtlijnen van de GDPR?*
- *Welke bepalingen uit elk van deze instrumenten is relevant voor respectievelijk AI-toepassingen en gegevensbescherming?*

Ook deze beschrijvende vragen werden aan de hand van rechtsdogmatisch onderzoek en een literatuurstudie beantwoord. Hier is op sommige momenten de technische informatie die bekomen is uit de vorige vragen van belang.

De laatste onderzoek-gerichte vragen zijn van beschrijvende en evaluerende aard. Er wordt een waardeoordeel: "schadelijk", "niet-schadelijk" of "voordelig" gegeven aan verschillende AI toepassingen die onderscheiden kunnen worden. Het is belangrijk om voor deze vragen niet te veel het voorstel van AI-verordening en haar voorbereidende werken bij de hand te houden, zodat ze niet te sturend werken.

- *Welke zijn de meest schadelijke AI-toepassingen voor het recht op privacy?*
- *Welke zijn de meest voordelige AI-toepassingen voor het recht op privacy?*

Om deze scriptie af te ronden en alvorens terug te koppelen naar de centrale onderzoeksvraag moet nog één laatste, vergelijkende en evaluerende vraag worden gesteld:

- *Moet, en zo ja hoe, de GDPR of het voorstel van AI-verordening aangepast worden om te voldoen aan de huidige en toekomstige uitdagingen?*

Hiermee is het de bedoeling om tot een afweging te komen van al hetgeen besproken werd en om aan de hand van eigen inbreng en literatuurstudie van ethische en filosofische bronnen te komen tot "*the law as it should be*". Is de regelgeving bestand tegen redelijk voorzienbare technologische ontwikkelingen?

3. Opbouw en structuur

6. **DELEN.** Deze masterscriptie is opgedeeld in drie grote delen: (1) Artificiële intelligentie; (2) Bescherming van persoonsgegevens; en (3) Het samenspel van AI en privacy.

7. **HOOFDSTUKKEN.** Deel 1 is op zijn beurt opgedeeld in 6 hoofdstukken die achtereenvolgend AI zullen bespreken qua terminologie en technische mogelijkheden; de voor- en nadelen van verschillende AI-toepassingen; de krachtlijnen van het voorstel van AI-verordening; de relevante bepalingen met betrekking tot privacy en meer bepaald met betrekking tot de bescherming van persoonsgegevens; en ten slotte een eerste, tussentijdse conclusie bij, en overzicht van deel 1.

Deel 2, dat handelt over de bescherming van persoonsgegevens, telt 5 hoofdstukken met een gelijkaardige opbouw als die van deel 1. Zo zal dit deel het hebben over de begrippen: "privacy" en "bescherming van persoonsgegevens", de toepasselijke wetgeving (naast GDPR); hun onderlinge verhouding; de krachtlijnen van de GDPR; de relevante bepalingen met betrekking tot AI; en wederom, om het deel af te sluiten, een tussentijdse conclusie van deel 2.

Het derde en laatste deel van deze scriptie zal de voorgaande twee samenbrengen. Als eerste is er een bespreking van de huidige situatie, welk recht op dit moment limieten stelt aan de dataverwerking voor en door AI, als die er zijn. Vervolgens worden de toekomstige veranderingen besproken. Op welke vlakken zal de opmars van AI moeten inboeten, en waar wordt ze net vrij gelaten?

De conclusie bij dit laatste deel vormt tevens de conclusie van het gehele onderzoek.

1. Deel 1: Artificiële intelligentie (AI)[26]

8. **KORTE GESCHIEDENIS**.[27] Artificiële intelligentie houdt de mensheid al in haar ban sinds het spreekwoordelijke begin der tijden.[28] Reeds in de klassieke oudheid besprak de Griekse filosoof Aristoteles in zijn *Politika* de mogelijkheid van robots die menselijke slaven zouden vervangen. Hij noemde hen toen nog '*automata'*.[29] Ergens rond 1940 bedacht de auteur Isaac Asimov zijn drie wetten van robotica[30] die hij verder uitdiepte in verschillende sci-fi-boeken tussen 1941 en 1950. Tot op de dag van vandaag vormen ze nog steeds belangrijke richtlijnen bij de ontwikkeling van ethische AI. Enkele jaren later stelde één van de grondleggers van de moderne computertechnologie in zijn artikel: "*Computing Machinery and Intelligence*"[31], een test voor waarmee de intelligentie van een computer geëvalueerd zou kunnen worden, een imitatiespel, of zoals het beter gekend is: de '*Turingtest'*. In 1956 werd voor het eerst de term "Artificial Intelligence" gebruikt tijdens het '*Dartmouth Summer Research Project on Artificial Intelligence'*.[32] Er wordt voor geopteerd deze workshop aan te duiden als het begin van AI zoals we het vandaag kennen, omdat op dit moment de geboorte van de terminologie plaatsvond en de eerste stappen werden gezet om de menselijke intelligentie machinaal te reproduceren.[33]

Eerst waren er fantasieën en dromen, vervolgens computers om de gelimiteerde mogelijkheid van mensen voor wiskundige taken en geheugen aan te vullen en ondertussen zijn we aanbeland in het tijdperk waarin de computerwetenschap zich volop stort op de ontwikkeling van AI. Talloze blockbusters, boeken, podcasts en wetenschappelijke artikels proberen ons een beeld te geven van een wereld waarin de mensheid samen zal leven met AI. Velen verbinden hier absolute rampscenario's aan. De realiteit is echter, zoals bijna altijd, iets genuanceerder. De enorme vooruitgang die AI ons biedt gaat uiteraard hand in hand met enkele risico's, net zoals die er zijn bij elke ontwikkeling van nieuwe technologie, maar het einde van de mensheid door een kwaadaardige superintelligentie is (nog) niet aan de orde. Er zijn wereldwijd verschillende instanties die hun bezorgdheden uiten en op een heldere manier de potentiële

[26] Wanneer in dit deel naar artikelen of overwegingen wordt verwezen, zonder specifieke benoeming, wordt het voorstel van AI-verordening bedoeld. Het gaat ook over datzelfde voorstel wanneer in dit deel wordt verwezen naar het "Voorstel", de "toekomstige Verordening", of eender welke andere benaming die duidelijk naar het voorstel van AI verordening verwijst.
[27] S. CAVE, K. DIHAL & S. DILLON (eds.), AI Narratives: A History of Imaginative Thinking about Intelligent Machines, Oxford, Oxford University Press, 2020, 448p, https://doi.org/10.1093/oso/9780198846666.001.0001.
[28] C.A. PICKOVER, *Kunstmatige Intelligentie – Van middeleeuwse robots tot neurale netwerken: Een chronologisch overzicht*, Kerkdriel (Nederland), Librero, 2021, p. VIII.
[29] C.A. PICKOVER, *Kunstmatige Intelligentie – Van middeleeuwse robots tot neurale netwerken: Een chronologisch overzicht,* Kerkdriel (Nederland), Librero, 2021, p. 5.
[30] **Eerste Wet**: "Een robot mag een mens geen letsel toebrengen of door niet te handelen toestaan dat een mens letsel oploopt."; **Tweede Wet**: "Een robot moet de bevelen uitvoeren die hem door mensen gegeven worden, behalve als die opdrachten in strijd zijn met de Eerste Wet."; **Derde Wet**: "Een robot moet zijn eigen bestaan beschermen, voor zover die bescherming niet in strijd is met de Eerste of Tweede Wet."; Later werden deze wetten nog aangevuld met een Nulde wet: **Wet 0**: "Een robot mag de mensheid geen kwaad doen, of door niets te doen, de mensheid schade toebrengen." → I. ASIMOV, *I, Robot*, New York, Bantam Books, 1950, p. 44.
[31] A.M. TURING, "Computing Machinery and Intelligence", *Mind* 1950, 59, p. 433-460, https://www.cs.mcgill.ca/~dprecup/courses/AI/Materials/turing1950.pdf.
[32] Dartmouth Summer Research Project: The Birth of Artificial Intelligence, https://www.historyofdatascience.com/dartmouth-summer-research-project-the-birth-of-artificial-intelligence/. → J. MC CARTHY, M.L. MINSKY, N. ROCHESTER & C.E. SHANNON, *A proposal for the Dartmouth summer research project On artificial intelligence*, 31 augustus 1955, http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf.
[33] K. GABRIELS, *Conscientious AI – Machine Learning Morals*, Brussel, VUBPRESS, 2020, p. 11; R.A. BROOKS, *Cambrian Intelligence. The Early History of the New AI*, Cambridge, (MA), MIT Press, p. 80.

risico's van AI aankaarten[34] met als vrucht het voorstel van AI-verordening[35] dat het onderwerp van deze tekst uitmaakt.

9. WERKWIJZE EN OPBOUW. In dit deel zal achtereenvolgens gekeken worden naar wat AI is, wat er de potentiële voor- en nadelen van zijn, hoe de AI-verordening hieraan tegemoet zal komen en op welke manier dit relevant is voor het recht op privacy en meer bepaald op het recht op bescherming van persoonsgegevens.

Hoofdstuk 1 zal trachten een inleiding tot artificiële intelligentie te geven. Omdat dit een masterscriptie ter behalen van een graad in de rechten is, is het niet de bedoeling om de details omtrent de werking van AI te beschrijven. Het is slechts de bedoeling om een beter begrip te krijgen van wat het nu net is, hoe het in grote lijnen werkt, in welke vormen het zich manifesteert en waarom het allemaal misschien toch niet zo eng is als het op het eerste gezicht lijkt. Angsten en bezorgdheden komen namelijk heel vaak voort uit onwetendheid.
Om te beginnen bij het begin is het dus zeer belangrijk om in eerste instantie het concept: "*artificiële intelligentie*", toe te lichten. Duidelijk mag zijn dat dit op zich al geen gemakkelijk vraagstuk is aangezien er verschillende definities de ronde doen omtrent gewone "intelligentie". Een veelvoud daarvan is dus te verwachten voor "artificiële intelligentie".

Vervolgens zal hoofdstuk 2 worden gewijd aan een bespreking van de mogelijkheden en risico's die met AI gepaard gaan. Het is ijdele hoop om op één academiejaar en zonder noemenswaardige middelen een volledig nieuwe risicoanalyse uit te voeren, maar gelukkig is dit ook niet nodig aangezien de Europese Commissie die taak reeds met vrucht heeft volbracht. Na een korte blik op wat "het internet" en de andere klassieke mediakanalen over AI te zeggen hebben, zal er dus voornamelijk worden gekeken naar het Witboek betreffende Kunstmatige Intelligentie[36] en de Ethische Richtsnoeren voor Betrouwbare Kunstmatige Intelligentie.[37] De risico's die deze bronnen naar voor brengen zullen absoluut noodzakelijk zijn om in verdere hoofdstukken de toereikendheid van de beoogde maatregelen te beoordelen in het licht van het recht op privacy en het recht op bescherming van persoonsgegevens.[38]

Na deze eerste twee hoofdstukken, die ertoe dienen om een rudimentair begrip van AI – wat het inhoudt en wat de risico's en voordelen zijn - te schetsen, zal iets gedetailleerder worden gekeken naar het Voorstel van AI-Verordening in hoofdstuk 3. Het voorstel van AI-verordening zal in grote lijnen worden

[34] ETHISCHE RICHTSNOEREN (Comm.) van het Directoraat-Generaal Communicatienetwerken, Inhoud en Technologie, voor betrouwbare KI, Publications Office, 8 april 2019, https://data.europa.eu/doi/10.2759/924378; WITBOEK (Comm.) over kunstmatige intelligentie – een Europese benadering op basis van excellentie en vertrouwen, 19 februari 2020, COM (2020) 65 final, https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_nl.pdf; …
[35] VOORSTEL (Comm.) voor een verordening van het Europees Parlement en de Raad tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van bepaalde wetgevingshandelingen van de Unie, 21 april 2021, 2021/0106 [COD], https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52021PC0206.
[36] WITBOEK (Comm.) over kunstmatige intelligentie – een Europese benadering op basis van excellentie en vertrouwen, 19 februari 2020, COM (2020) 65 final.
[37] ETHISCHE RICHTSNOEREN (Comm.) van het Directoraat-Generaal Communicatienetwerken, Inhoud en Technologie, voor betrouwbare KI, Publications Office, 8 april 2019.
[38] De GDPR gaat namelijk niet over het gehele recht op privacy. Deze verordening handelt enkel over de bescherming van persoonsgegevens van EU-inwoners.

geanalyseerd om de meest relevante bepalingen voor deze scriptie te identificeren, namelijk diegene die handelen over het recht op privacy en het recht op bescherming van persoonsgegevens.

Het laatste hoofdstuk van dit eerste deel zal de relevante artikelen voor privacy en voor de bescherming van persoonsgegevens in de kijker zetten.

1.1. Hoofdstuk 1. Artificiële Intelligentie

1.1.1. De terminologie

10. DEFINITIE VAN INTELLIGENTIE. Zoals voorheen reeds aangehaald is het bijzonder moeilijk om een sluitende definitie over AI te formuleren aangezien er tot nu toe ook nog niet echt een sluitende definitie bestaat omtrent gewone intelligentie. Toch moeten er bepaalde knopen worden doorgehakt en daarom zal er geen verder onderzoek naar de etymologie of mogelijke inhoud van "intelligentie" worden gedaan dan de volgende definitie die in 1999 door de psycholoog, Howard E. Gardner werd gegeven:

> *"I now conceptualize an intelligence as a biopsychological potential to process information that can be activated in a cultural setting to solve problems or to create products that are of value in a culture"*[39]

Opvallend in deze definitie is dat Gardner intelligentie onlosmakelijk koppelt aan een biologisch aspect. Hoewel er op het moment van schrijven nog geen algemene AI bekend is, kan toch al worden gesteld dat deze voorwaarde inmiddels achterhaald is.

11. ALGEMENE DEFINITIE VAN ARTIFICIËLE INTELLIGENTIE. Dit gezegd zijnde, werden er sinds haar eerste vermelding in 1955 over "artificiële intelligentie" tonnen papier en terabytes aan harde schijven vol geschreven. Omdat elke afzonderlijke auteur natuurlijk zijn of haar bijdrage tracht te leveren aan het besproken onderwerp, zijn er verschillende definities in de omloop. Hiervan worden er hieronder drie besproken die mijns inziens samen een redelijk verstaanbare en op dit moment zo volledig mogelijke invulling geven aan het begrip:

> *"Making a machine behave in ways that would be called intelligent if a human were so behaving."*[40]

> *"We define AI as a system's ability to interpret external data correctly, to learn from such data, and to use those learnings to achieve specific goals and tasks through flexible adaptation."*[41]

> *"Simply put, AI is a collection of technologies that combine data, algorithms and computing power"*[42]

AI is dus per definitie gedrag dat door een machine of toepassing tentoon wordt gespreid.

Het gedrag in kwestie is het gevolg van een combinatie van technologieën die data verwerken op basis van algoritmen die zo zijn opgesteld dat ze de data correct interpreteren, eruit leren en specifieke doelen en taken kunnen uitvoeren met betrekking tot deze data.

---

[39] H.E. GARDNER, *Intelligence reframed: Multiple intelligences for the 21st century*, New York, Basic Books, 1999, p. 33-34.
[40] J. MC CARTHY, M.L. MINSKY, N. ROCHESTER & C.E. SHANNON, *A proposal for the Dartmouth summer research project On artificial intelligence*, 31 augustus 1955, p. 11.
[41] A. KAPLAN, & M. HAENLEIN, "Siri, Siri in my Hand, who's the Fairest in the Land - On the Interpretations, Illustrations and Implications of Artificial Intelligence", *Business Horizons* 2019, vol. 62, p. 17, https://www.sciencedirect.com/science/article/pii/S0007681318301393.
[42] WITBOEK (Comm.) over kunstmatige intelligentie – een Europese benadering op basis van excellentie en vertrouwen, 19 februari 2020, COM (2020) 65 final, p. 2.

Ten slotte is het ook van belang dat wij – de mens als zijnde het voorbeeld waar naartoe gewerkt wordt – dit gedrag zouden bestempelen als intelligent als het door een andere telg van onze soort werd gesteld.

Dit laatste criterium is terug te vinden in de Turingtest[43], waarbij een computer/AI, naar zijn beste vermogen, het geprogrammeerde gedrag op dat van een mens doet lijken. Wanneer iets intelligent lijkt, en de mens het niet kan onderscheiden van haar eigen intelligentie, dan moet dit toch ook *as such* worden erkend.

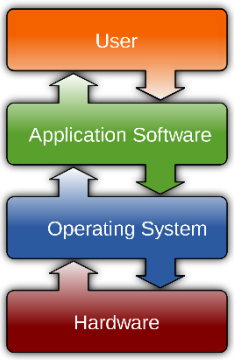
12. **JURIDISCHE DEFINITIE.** Om een iets juridischere noot in deze definiëring te introduceren kan worden gekeken naar het voorstel van AI-verordening. Wetgeving zou geen wetgeving zijn als het geen eigen gooi naar definiëring deed. Het is namelijk van uitzonderlijk groot belang om goed te kaderen wat nu net onder de regelgeving moet vallen. De toelichting bij het voorstel[44] vermeldt dat het gaat om één enkel, toekomstbestendige definitie, die als volgt klinkt.

> *"'Artificiële-intelligentiesysteem" (AI-systeem): software die is ontwikkeld aan de hand van een of meer van de technieken en benaderingen die zijn opgenomen in de lijst van bijlage I en die voor een bepaalde reeks door mensen gedefinieerde doelstellingen output kan genereren, zoals inhoud, voorspellingen, aanbevelingen of beslissingen die van invloed zijn op de omgeving waarmee wordt geïnterageerd."*[45]

Hieruit zijn vier belangrijke elementen te onderscheiden:

1. Het moet gaan om software;
2. Die minimum één techniek of benadering uit bijlage I bij het Voorstel tot AI-verordening toepast;
3. Die voor door mensen gedefinieerde doelstellingen, output kan genereren;
4. Die invloed hebben op de omgeving waarmee de AI een interactie heeft.

13. **SOFTWARE.**[46] Software is de verzameling van in computertaal geschreven instructies die de brug vormen tussen de gebruiker en de hardware. Het gaat om alle functionele aspecten van een computer, die geen betrekking hebben tot fysieke onderdelen. Daarom is het voor de hand liggend om eerst kort hardware te omschrijven om vervolgens de link te leggen met software en waarom de twee elkaar nodig hebben.



Figuur 1. Samenwerking tussen soft- en hardware. → Golftheman, CC BY-SA 3.0<https://creativecommons.org/licenses/by-sa/3.0>,

[43] A.M. TURING, "Computing Machinery and Intelligence", *Mind* 1950, 59, p. 433-434.
[44] Zie 1.1. Motivering en doel van het voorstel, in de Toelichting bij het voorstel van AI-verordening. → Voorstel (Comm.) voor een verordening van het Europees Parlement en de raad van 21 april 2021 tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (wet op de artificiële intelligentie) en tot wijziging van bepaalde wetgevingshandelingen van de unie, COM(2021) 206 final - 2021/0106[COD].
[45] Zie artikel 3(1) voorstel AI-verordening.
[46] IBM, "What is Software Development? – Learn the essentials of software development and how it helps businesses innovate and compete.", *ibm.com/topics*, https://www.ibm.com/topics/software-development; D. JOHNSON, "What is software? A guide to all of the different types of programs and applications that tell computers what to do", *Business Insider* 26 maart 2021, https://www.businessinsider.com/what-is-software?r=US&IR=T; TECHOPEDIA, "Software", *techopedia.com*, https://www.techopedia.com/definition/4356/software.

Hardware zijn letterlijk alle lichamelijke, tastbare goederen waaruit een computer is opgebouwd. Denk hierbij aan CPU's, moederborden, grafische kaarten, schermen, toetsenborden, … ; Alles wat fysiek werk zal leveren bij het gebruik van een computer.

Software zijn de onlichamelijke aspecten van een systeem waarmee hardware kan worden aangestuurd. In eerste instantie is het dus het communicatiemiddel tussen mens en machine. Zoals het diagram hiernaast weergeeft zijn er minstens twee vormen van software. De applicatiesoftware vertaalt mensentaal naar computertaal en voert zodanig taken uit die niet rechtstreeks met de hardware te maken hebben. Systeemsoftware sturen de hardware aan zodat deze kan doen waarvoor hij is gemaakt. Naast deze twee vormen zijn er ook nog (1) programmeer-software, die software developers ondersteunt; en (2) *malicious software*, die computers of andere software probeert te beschadigen of te ontregelen.

14. **BIJLAGE I.** In de eerste bijlage bij het voorstel van AI-verordening zijn drie technieken en benaderingen op het gebied van AI benoemd, waarvan er minimum één aanwezig moet zijn in de software als de AI in kwestie binnen de definitie van de verordening en dus binnen haar toepassingsgebied wilt vallen. De technieken en benaderingen in kwestie zullen in de volgende titel onder dit hoofdstuk besproken worden.

BIJLAGE I **TECHNIEKEN EN BENADERINGEN OP HET GEBIED VAN ARTIFICIËLE INTELLIGENTIE** **als bedoeld in artikel 3(1)**
(a) Benaderingen voor machinaal leren, waaronder gecontroleerd, ongecontroleerd en versterkend leren, met behulp van een brede waaier aan methoden, waaronder diep leren ("deep learning").
(b) Op logica en op kennis gebaseerde benaderingen, waaronder kennisrepresentatie, inductief (logisch) programmeren, kennisbanken, inferentie- en deductiemachines, (symbolisch) redeneren en expertsystemen.
(c) Statistische benaderingen, Bayesiaanse schattings-, zoek- en optimalisatiemethoden.

Figuur 2. Bijlage I bij voorstel AI-verordening

De verwoordingen in deze bijlage zijn zeer breed gehouden, waardoor er op dit moment geen AI-toepassingen bekend zijn die hierbuiten vallen. Belangrijk om op te merken is dus wel dat wanneer er een AI ontwikkeld zou worden die niet onder één van deze technieken of benaderingen te plaatsen valt, deze niet onder het toepassingsgebied van de verordening zal kunnen worden geplaatst, en er dus – ten minste in theorie – het risico bestaat dat AI-ontwikkelaars op zoek zullen gaan naar mogelijkheden om aan deze wetgeving te ontsnappen. Hieraan wordt door de wetgever tegemoet gekomen door nu al aan te geven dat het de bedoeling is om deze bijlage aan te vullen naargelang de technologie avanceert.[47]

Het limitatief opsommen van technieken en benaderingen die de software moet gebruiken om van AI te spreken in de zin van deze verordening vereist van de wetgever dat deze te allen tijde zeer goed op de hoogte blijft en vlot kan inpikken op nieuwe ontwikkelingen. Het feit dat wetgeving bijna per definitie achterloopt op de realiteit, doet hieromtrent toch wel enkele zorgen de kop opsteken.

[47] Artikel 4 voorstel tot AI-verordening; & 5.2.1. Toepassingsgebied en Definities (Titel I), in de Toelichting bij het voorstel van AI-verordening.

15. **OUTPUT A.D.H.V. GEDEFINIEERDE DOELSTELLING.**[48] Dit is mijns inziens een zeer breed te interpreteren criterium. Namelijk alles wat de mens als opdracht geeft aan de op de bepaalde technieken en benaderingen gebaseerde software kan worden beschouwd als een "door de mens gedefinieerde doelstelling". Handelingen van de mens zijn in deze ook gewoon gelimiteerd door al het geldend recht dat in werking is. Het opdracht geven tot moord is en blijft strafbaar, of de opdracht nu wordt gegeven aan een menselijke huurmoordenaar of aan een AI-toepassing.

De limieten waaraan AI zich te houden heeft, zullen door de AI-verordening worden vastgelegd. Deze zal zich dus voornamelijk bezighouden met welke output voor AI-toepassingen beoogd mag worden. Foutieve, gebrekkige of totaal van de pot gerukte uitkomsten zijn echter een reëel probleem in een vakgebied dat nog volop in ontwikkeling is.

Samen met de volgende vereiste van beïnvloeding van de omgeving door de AI, is de stap naar sciencefiction heel klein. Dit omdat we in het achterhoofd kunnen – en misschien zelfs moeten – houden dat draadloze telefonie, touchscreens en VR in de Star Trek-afleveringen van 50 jaar geleden gewoonweg fantasie waren.[49]

16. **OMGEVING BEÏNVLOEDEN.** Wat precies valt onder het "*van invloed zijn op de omgeving waarmee geïnterageerd wordt*", kan op verschillende manieren worden ingevuld. Vereist dit een rechtstreekse fysieke uiting van wat door de AI wordt verwezenlijkt?; of worden de toezichthoudende mensen aanzien als "omgeving" en is het simpelweg aanbrengen van een idee bij deze personen genoeg om van een beïnvloeding te spreken?

Hoewel enkele bekende AI-toepassingen een robotlichaam hebben gekregen en daardoor dus zelf tot fysieke uitvoering kunnen overgaan, hebben de belangrijkste toepassingen helemaal geen fysieke vorm. Mijns inziens kan dus bijna alles als "beïnvloeding" worden bestempeld, vanaf het moment dat de output – in welke vorm dan ook – een serieuze aanzet geeft tot nadenken. Omdat tot op heden nog niet in de gedachten van mensen kan worden gekeken, is het onmogelijk om te weten wanneer dit theoretisch criterium is voldaan. Rechtspraak zal in deze met een waarneembaar criterium moeten komen om zo duidelijk af te lijnen wat wel en niet onder deze definitie van AI valt.

17. **CUMULATIEF EN *SENSU LATO* INTERPRETATIE.** Bovenstaande elementen uit artikel 3(1) AI-verordening dienen cumulatief voldaan te zijn om van een artificieel intelligentie-systeem in de zin van deze verordening te spreken, wat de drempel toch op een bepaald niveau zet.

---

[48] Zoals in dit randnummer zelf wordt aangehaald gaat het om een begrip waarover mijns inziens in de toekomst nog discussies gevoerd zullen worden. Vanaf wanneer is er een gedefinieerde doelstelling? Op welk moment moet worden vastgesteld of die er is? Er wordt geargumenteerd dat dit zo breed mogelijk ingevuld moet worden, zonder hierbij de redelijkheid uit het oog te verliezen. In grote lijnen kan dus gesteld worden dat er een gedefinieerde doelstelling zal bestaan vanaf het moment dat een welbewuste keuze wordt gemaakt, met de bedoeling bepaalde gevolgen van de AI te bekomen, om een bepaalde input aan de AI-toepassing te geven. Dit moet worden ingevuld naargelang de soort en het doel van de desbetreffende AI. Rechtspraak en rechtsleer zullen hier in de toekomst ongetwijfeld verdere invulling aan geven.

[49] Wanneer het gedachtenexperiment wordt verdergezet naar de eerder onwaarschijnlijke situatie waarin de "door de mens gedefinieerde doelstellingen" geen gebrek vertonen en de AI-toepassing naar alle standaarden ook in orde is, – en er dus niet van een voorzienbare of aantoonbare menselijke fout kan worden gesproken – komt er een zeer interessant juridisch probleem aan het licht: Waar ligt de aansprakelijkheid? Hierover hebben reeds verschillende auteurs zich het hoofd gebroken, maar deze scriptie zal hier niet verder op in gaan.

Uiteraard zal niet elke software er één zijn die als AI kan worden bestempeld. Deze moet namelijk werken op of met een techniek of benadering uit bijlage I. Vervolgens moet deze toepassing tot een output komen op basis van een door de mens gedefinieerde doelstelling en ten slotte moet de output in de vorm van "inhoud, voorspellingen, aanbevelingen of beslissingen" de omgeving waarmee geïnterageerd wordt beïnvloeden.

Wat betreft de interpretatie van de voor interpretatie vatbaar zijnde componenten, moet mijns inziens de meest brede invulling worden geaccepteerd. Het te limitatief inkleuren van deze definitie zal anders voornamelijk tot gevolg hebben dat de praktijk op zoek zal gaan naar manieren om onder de restricties van deze verordening uit te komen. Met het oog op de toekomst en met de constante technologische vooruitgang in dit veld in het achterhoofd, zou de verordening zeer snel irrelevant worden indien de definitie te strikt wordt geïnterpreteerd. Enkel bijlage I is op dit moment al voorzien als veranderlijk element in de definitie, terwijl dit niet het enige is dat verduidelijking vereist.[50]

1.1.2. Een onderverdeling naar werking en aard[51]

18. KADERING.[52] Gelet op de zonet besproken definiëring kan worden geconcludeerd dat AI een zeer brede waaier aan systemen, algoritmes en robots kan zijn, zolang het maar gaat om een software die met bepaalde input, aan de hand van een aantal limitatief genoemde technieken en benaderingen een output kan genereren die een invloed kan hebben op de omgeving van het systeem in kwestie.

Onder deze titel zal kort worden gekeken naar de verschillende technieken en benaderingen, hoe ze werken en wat ze precies beogen te doen. Het kan op dit punt in deze scriptie niet genoeg benadrukt worden dat het geenszins de bedoeling is om een volledige, gedetailleerde beschrijving te geven van dit immens brede onderzoeks-en werkveld. Hetgeen u voorligt is tenslotte een scriptie tot behalen van een diploma in de rechten, niet in de informatica- en communicatietechnologie.

19. BIG DATA, ALGORITMEN EN AI. Big data is een overkoepelende term die gebruikt wordt om te verwijzen naar zowel enorme hoeveelheden data, het verzamelen en de verwerking, alsook naar de analyse van deze data en de visualiseringen ervan.[53] Het is voor deze term van geen belang om wat voor soort data het gaat of waar deze vandaan komt, wat dus wilt zeggen dat zowel persoonsgegevens – al dan niet een bijzondere categorie – als productiegegevens van fabrieken hieronder kunnen vallen.

---

[50] Zie artikel 4 van het voorstel van AI-verordening.

[51] X, "Welke soorten kunstmatige intelligentie (AI) ken jij?", *vboxxcloud.nl* 2021, https://vboxxcloud.nl/blog/soorten-kunstmatige-intelligentie/; M. DE KETELAERE, "Wat is artificiële intelligentie en wat ben ik ermee?", *imec.be* 19 mei 2020, https://www.imec.be/nl/artikelen/wat-is-artificiele-intelligentie-en-wat-ben-ik-ermee; …

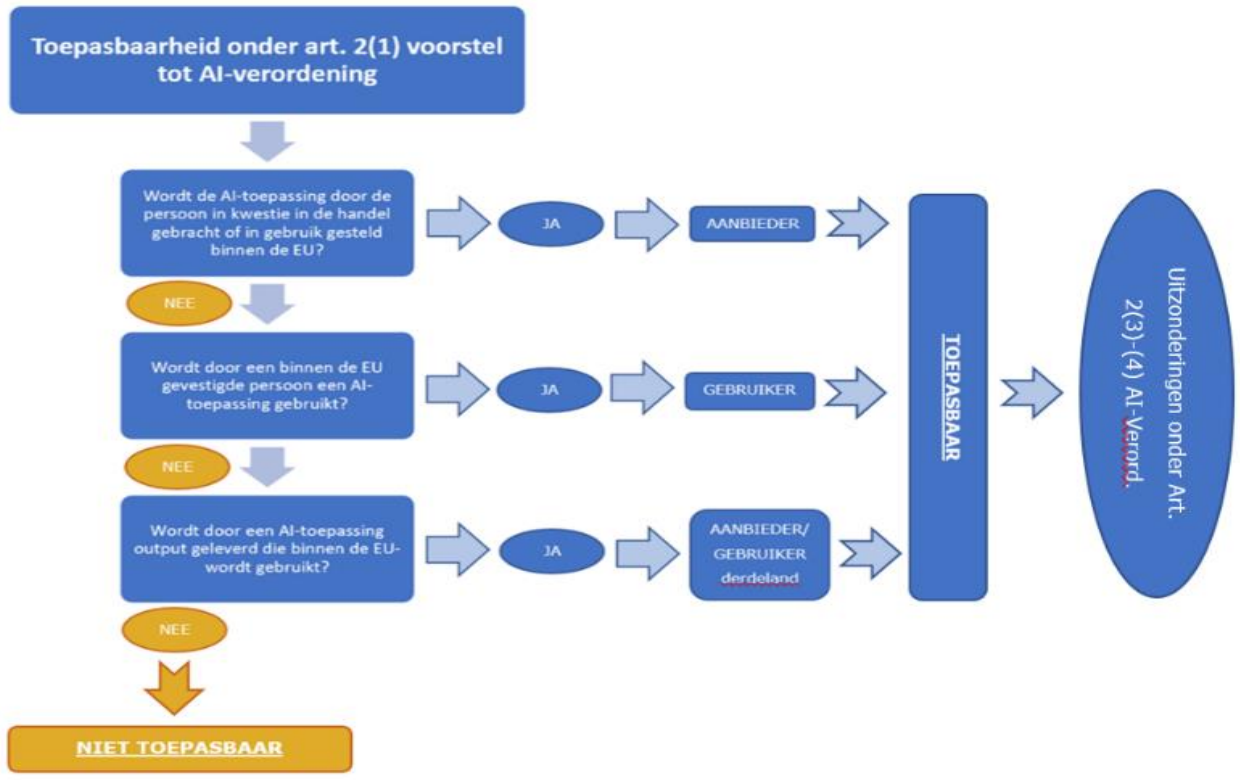
[52] Omwille van de enorme waaier aan concepten en begrippen die bestaan in het veld van de computertechnologie en ook gewoon alleen al in het onderzoeks- en werkveld van AI, zal hier niet worden ingegaan op alle mogelijk relevante aspecten. Deep learning, neurale netwerken, Internet of Things (IoT), Theory of Mind, het onderscheid tussen belichaamde AI en software, … gaan te ver voor deze tekst.

[53] Raad van Europa, Consultative Committee of Convention 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23 januari 2017, p. 2; Europese Commissie, Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's - Naar een bloeiende data-economie, COM(2014) 442 final, Brussel, 2 juli 2014, p. 5; International Telecommunication Union, *Big data - Cloud computing based requirements and capabilities*, November 2015, p. 2; FRA, *Handbook on European data protection law – 2018 edition*, Luxemburg, Publications Office of the European Union, 2018, p. 350 (Council of Europe, European Court of Human Rights, European Data Protection Supervisor, European Union Agency for Fundamental Rights, *Handbook on European data protection law : 2018 edition*, Publications Office, 2019, https://data.europa.eu/doi/10.2811/343461).

Het belangrijkste wat onthouden moet worden over Big Data is dat het door het hoeveelheidsaspect de mogelijkheid biedt om voor andere doeleinden te worden gebruikt in het verwerkingsaspect. Data die op het eerste zicht niet direct te maken heeft met een bepaald onderwerp, kan door combinatie met andere gegevens toch leiden tot conclusies over dat onderwerp.

Een algoritme is als het ware een recept om in geval van een bepaald probleem tot een oplossing te komen. Het is de taak van een programmeur om bij een bepaald probleem een stapsgewijs draaiboek uit te schrijven over hoe het opgelost moet worden en dit te vertalen in een programmeertaal zodat het algoritme ook kan worden uitgevoerd door de computer. Deze vertaalde versie van het algoritme is een programma wat op zijn beurt onder de verzamelterm "software" valt.[54]

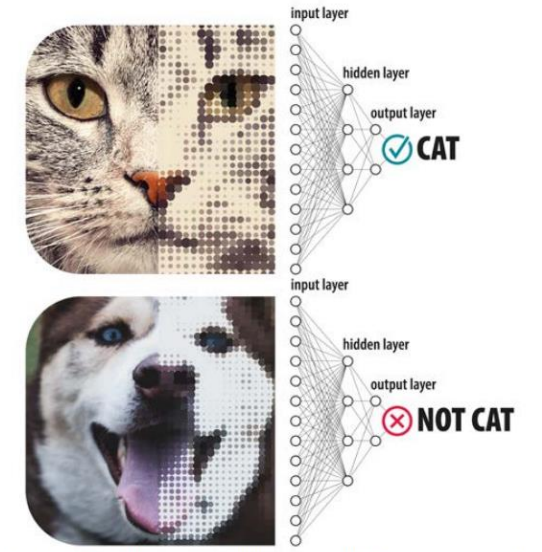
Artificiële intelligentie steunt zowel op algoritmes als op grote hoeveelheden data om tot de geautomatiseerde beslissingen te komen die haar kenmerken.



Figuur 3. Toepasbaarheid van de AI-verordening onder art. 2(1) AI-verordening vertaald naar een algoritme, ter illustratie van wat een algoritme nu net is.

[54] Zie supra, Randnr. 13 – Software.

20. ARTIFICIAL NARROW INTELLIGENCE[55], ARTIFICIAL GENERAL INTELLIGENCE[56] & ARTIFICIAL SUPER INTELLIGENCE.[57] De eerste generatie AI-toepassingen werken volledig op de programmering van algoritmes, waarvan een simpel schematisch voorbeeld hieronder te zien is. Mensen met veel expertise in een bepaald vakgebied gieten hun kennis in algoritmes die vervolgens worden vertaald naar programma's waardoor een systeem deze kan toepassen. Omdat dit niet echt als "intelligent" kan worden bestempeld aangezien de oplossing en de strategie om daartoe te komen letterlijk worden aangereikt, wordt deze generatie ook wel "symbolische AI"[58] genoemd.



Graphic by EPRS, produced by Samy Chahri; picture credits: @bedneyimages (freepik.com) and C. Brear (Unsplash).

Figuur 4. Schema van een artificieel neuraal netwerk ter herkenning van katten.

De volgende stap in de evolutie, bestaande uit de zogenaamde tweede generatie of zwakke, beperkte AI heeft door middel van geüpdatete algoritmes de mogelijkheid om zelf de oplossing voor een probleem te zoeken.[59] Het algoritme is nu dus zo opgebouwd dat de mens niet meer stap voor stap moet voorkauwen hoe de oplossing moet worden bereikt, maar enkel nog moet aangeven op welke manier de AI-toepassing tot een oplossing voor een gegeven probleem kan komen. Dit concept heet "machinaal leren". De limieten van deze zwakke, "*Artificial Narrow Intelligence*" (ANI) laten zich op dit moment nog gelden doordat deze "intelligentie" zich enkel manifesteert in zeer beperkte, sterk afgelijnde niches, zoals bijvoorbeeld schaken[60] of het herkennen van bepaalde objecten.

In de toekomst willen AI-onderzoekers hun AI doen evolueren naar sterke, algemene AI waarbij het systeem zich in meerdere gebieden comfortabel kan bewegen. Deze "*Artificial General Intelligence*" (AGI), zou zich in principe dus laten kenmerken door een op die van de mens gelijkende intelligentie die, net zoals bij mensen, over verschillende gebieden kan strekken. Nadat deze mijlpaal is bereikt is de laatste stap, die volgens sommigen ook de laatste uitvinding van de mens zal zijn,[61] deze naar een

[55] P. BOUCHER, *Artificial intelligence: How does it work, why does it matter, and what can we do about it?*, Brussel, Scientific Foresight Unit (STOA), within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament, juni 2020, p. 3-13. → (ISBN: 978-92-846-6770-3; doi: 10.2861/44572)
[56] P. BOUCHER, *Artificial intelligence: How does it work, why does it matter, and what can we do about it?*, Brussel, Scientific Foresight Unit (STOA), within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament, juni 2020, p. 13-17.
[57] P. BOUCHER, *Artificial intelligence: How does it work, why does it matter, and what can we do about it?*, Brussel, Scientific Foresight Unit (STOA), within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament, juni 2020, p. 13-17.)
[58] P. BOUCHER, *Artificial intelligence: How does it work, why does it matter, and what can we do about it?*, Brussel, Scientific Foresight Unit (STOA), within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament, juni 2020, p. 2-3.
[59] Zie infra, Randnr. 21 – Bijlage I & Figuur 5.
[60] Zie supra, Randnr. 2 – Inleiding – Artificiële intelligentie.
[61] J. BARRAT, *Our Final Invention: Artificial Intelligence and the End of the Human Era*, New York, Thomas Dunne Books/St Martin's Press, p. 336, ISBN13: 9780312622374; & G. MICHAEL, "The Future of Artificial Intelligence: Benevolent or Malevolent?", *Skeptic Magazine* (vol. 20, nummer 1) 2015, p. 57-60, https://www.researchgate.net/profile/George-Michael-8/publication/294876416_The_Future_of_Artificial_Intelligence_Benevolent_or_Malevolent_Book_Reviews_of_Michio_Kaku_The_Future_of_the_Mind_The_Scientific_Quest_to_Understand_Enhance_and_Empower_the_Mind_and_James_Barrat_Our_F/links/56c5207e08aea564e304dcab/The-Future-of-Artificial-Intelligence-Benevolent-or-Malevolent-Book-Reviews-of-Michio-Kaku-The-Future-of-the-Mind-The-Scientific-Quest-to-Understand-Enhance-and-Empower-the-Mind-and-James-Barrat-O.pdf.

"*Artificial Super Intelligence*" (ASI), waarbij het AI-systeem de menselijke – en dus ook de algemene artificiële – intelligentie overstijgt Dit is voornamelijk het speelveld van verschillende *science fiction*-films en daarom zal er op dit moment nog niet al te veel aandacht aan worden geschonken. Het is wel belangrijk om in het achterhoofd te houden dat dit een scenario is dat ook geregeld zal moeten worden wanneer het zich voordoet. Op dit moment is het daarvoor echter nog iets te vroeg.

21. **BIJLAGE I.** Als belangrijkste document voor dit deel – en bij uitbreiding deze scriptie –, krijgt het voorstel van AI-verordening hier het laatste woord om te bepalen waarop de nadruk moet worden gelegd. Bijlage I zal daarom als leidraad dienen en enkel de drie daarin vermelde technieken en benaderingen worden kort, schematisch toegelicht.

Technieken en benaderingen van AI onder Bijlage I[62]	
Machinaal leren = tweede generatie-AI waarbij het algoritme zodanig is ontworpen dat het zelf de oplossing tot een probleem kan vinden, zonder dat het daarvoor door mensen opgestelde regels moet volgen. [63]	
Gecontroleerd leren (*supervised learning*)	Het zelf vinden van oplossingen kan gebeuren nadat de AI-toepassing werd getraind met gelabelde data, wat wilt zeggen dat de data in kwestie vergezeld wordt door informatie over die data.
Ongecontroleerd leren (*unsupervised learning*)	Wanneer de trainingsdata niet gelabeld is, wordt gesproken van ongecontroleerd leren. Het is in deze situatie ook de bedoeling dat er zo min mogelijk menselijke inmenging is in het leerproces.
Versterkend leren (*Reinforcement learning)*	Versterkend leren is een vorm van machinaal leren waarbij de toepassing zelf, op basis van een zeer beperkte hoeveelheid feedback opeenvolgende beslissingen moet maken die tot een optimum in een bepaalde situatie moeten leiden.[64]
Op logica en kennis gebaseerde benaderingen = voornamelijk eerste generatie-AI, soms in combinatie met zwakke AI-systemen. De mens moet het spreekwoordelijk handje van de AI vaak nog vasthouden en begeleiden.	
Kennisrepresentatie	In dit geval spreekt het woord redelijk voor zich. De systemen die onder deze noemer vallen staan in voor de representatie van kennis. Ze groeperen en ordenen data volgens een bepaalde logica.
Inductief programmeren	Dit is een vorm van automatisch programmeren waarbij de AI-toepassing input krijgt, samen met een beschrijving van de beoogde output die het programma dat de AI moet schrijven zal moeten genereren.
Kennisbanken	Een kennisbank is een gespecialiseerde databank waarin kennis over een bepaald onderwerp op een gestructureerde manier op één plaats wordt opgeslagen.
Inferentie- en deductiemachines[65]	Deze machines hebben als taak om uit een poel van kennis nieuwe kennis af te leiden.
Symbolisch redeneren	Symbolisch redeneren werd voordien reeds kort aangehaald als eerste generatie AI, die nog niet echt zelf redeneert, maar dit wel doet uitschijnen.[66]
Expertsystemen	"Expertsystemen" is een synoniem voor diezelfde eerste generatie AI, waarbij een expert zijn of haar kennis in algoritmes giet en een programmeur deze omzet naar een computertaal zodat de toepassing deze expertise vervolgens kan reproduceren.[64]
Statische benaderingen, Bayesiaanse schattings-, zoek- en optimalisatiemethoden	
	Een statistische benadering, zoals bv. een Bayesiaans netwerk, is bedoeld om voor een bepaalde gebeurtenis te bepalen in welke mate van waarschijnlijkheid, elk van de factoren die ertoe aanleiding gaven hebben bijgedragen. M.a.w. de procentuele bijdrage van elke conditio sine qua non bij een bepaald feit.

Figuur 5. Verklarend overzicht van technieken en benaderingen onder Bijlage I bij voorstel AI-verordening

[62] Interessante bijkomende lectuur betreffende soorten, technieken en benaderingen waarmee AI wordt ontwikkeld is de volgende: K.H. BLÄSIUS, U. HEDTSTÜCK & C.-R. ROLLINGER, "Sorts and types in Artificial Intelligence" in J. SIEKMANN, *Lecture notes in Artificial Intelligence*, Berlijn, Springer Verlag, 1989, ISBN 3-540-52337-5; A. AGRAWAL, J. GANS & A. GOLDFARB, *The economics of Artificial Intelligence*, Chicago, University of Chicago Press, 2019, https://doi.org/10.7208/9780226613475; D. FLOREANO & C. MATTIUSSI, *Bio-Inspired Artificial Intelligence: Theories, Methods, and Technologies*, Cambridge (Massachusetts) & Londen (Engeland), The MIT Press, 2008, 674 p., ISBN 9780262303910; …

[63] IBM, "What is deep learning?", *IBM* 1 mei 2020, https://www.ibm.com/cloud/learn/deep-learning.

[64] M. VAN OTTERLO & M. WIERING, "Reinforcement Learning and Markov Decision Processes", in M. VAN OTTERLO & M. WIERING, *Reinforcement Learning*, onderdeel van boekenreeks: Adaptation, Learning, and Optimization, Vol. 12. p. 3–42, doi:10.1007/978-3-642-27645-3_1. ISBN 978-3-642-27644-6. (https://link.springer.com/chapter/10.1007/978-3-642-27645-3_1)

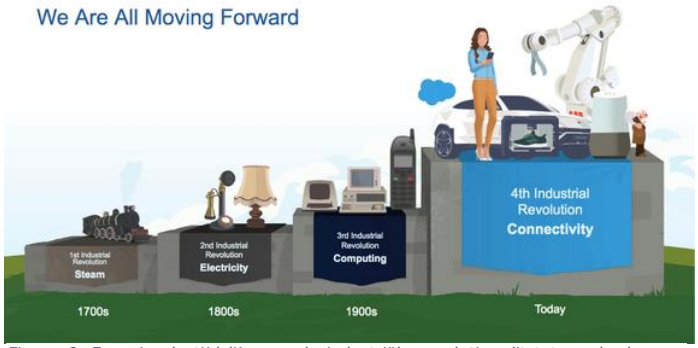
[65] F. HAYES-ROTH, D. WATERMAN; D. LENAT, *Building Expert Systems*, San Francisco, Addison-Wesley Pub. Co., 1983, 472 p., ISBN 0-201-10686-8.

[66] Zie Supra: Randnummer 20 - Artificial Narrow Intelligence , Artificial General Intelligence & Artificial Super Intelligence.

1.2. Hoofdstuk 2. De voor- en nadelen van AI

1.2.1. Op het internet en andere populaire kanalen.

22. EMANCIPATIE VAN DE ROBOT.[67] In het kader van alle ontwikkelingen omtrent AI, IoT, Blockchain, Virtual Reality (VR), … wordt steeds vaker gesproken van een vierde industriële revolutie, wat toch wel een beeld geeft van het belang van deze wetgeving in het licht van de wereldwijde bewegingen die door deze technologie worden gepusht.



Figuur 6. Een visuele tijdslijn van de industriële revoluties dit tot op de dag van vandaag hebben plaatsgevonden.https://www.salesforce.com/nl/blog/2017/05/wat-is-industrie-4-0.html.

Industriële revoluties hebben steeds zeer verregaande gevolgen gehad voor de samenlevingen waarin ze zich ontplooiden. De eerste revolutie zorgde als het ware voor een plattelandsvlucht door de enorme vraag naar arbeidskrachten in het recent ontwikkelde fabriekssysteem met alle gevolgen vandien. De tweede, ook wel technologische revolutie genoemd, werd gekenmerkt door de introductie van elektriciteit en de massaproductie die hierdoor mogelijk werd. Deze ontwikkelingen hebben het in zeker zin mogelijk gemaakt om op wereldschaal oorlogen te voeren (WO I & II). Deze revolutie ligt ook aan de grondslag van het grote economische ongelijkheid tussen verschillende delen van de wereld. De derde industriële revolutie, zoals deze wordt beschreven door Jeremy Rifkin[68], wordt gekenmerkt door de introductie van computers en internettechnologie die het mogelijk maakt om data binnen enkele seconden naar de andere kant van de wereld te transporteren.

De derde revolutie is op dit moment nog bezig omdat de manier waarop onze huidige samenleving draait constant aan verandering onderhavig is door de snelle ontwikkeling van technologieën. Duidelijk is wel dat de zogenaamde vierde industriële revolutie is begonnen en de derde overlapt. Deze meest recente revolutie kenmerkt zich door de afnemende nood aan menselijke arbeid omdat deze taken hoe langer hoe meer door robots en AI zullen worden overgenomen.

23. OVERZICHT VAN ENKELE VOORDELEN. Nieuwe technologieën worden over het algemeen met de nodige argwaan ontvangen. Dit was zo met elektriciteit, computers en nu ook met AI. Het is echter belangrijk om te beseffen dat AI niet zo nieuw is als het klinkt. De ontwikkeling ervan is echter nog bijlange niet voltooid. Siri en Alexa bijvoorbeeld zijn al verschillende jaren bij veel mensen thuis geïntegreerd en het eerste contact met talloze bedrijven verloopt via hun chatbots. Lang hiervoor waren er al assemblage robots die duizenden mensen vervangen in fabrieken, wat ervoor zorgt dat deze

[67] C. KRAAIJVANGER, "De Vierde Industriële Revolutie is begonnen: Zijn we straks allemaal overbodig?", *scientas.nl* 21 oktober 2018, https://scientias.nl/de-vierde-industriele-revolutie-is-begonnen-zijn-we-straks-allemaal-overbodig/; X, "De vierde industriële revolutie.", *rixels.com* 3 november 2020, https://rixels.com/nl/blog/de-vierde-industriele-revolutie/; S. PAUW, "Wat is industrie 4.0?", *Salesforce.com* 12 augustus 2020, https://www.salesforce.com/nl/blog/2017/05/wat-is-industrie-4-0.html; …

[68] J. RIFKIN, *The Third Industrial Revolution – How lateral power is transforming energy, the economy, and the world*, New York, Palgrave Macmillan, 2015, 304 p.

mensen ander, minder fysiek zwaar werk kunnen doen. Enkele voordelen die steevast worden herhaald in verschillende artikels zijn de volgende:[69]

- Automatisering ontlast menselijke arbeiders;
- Machines kunnen quasi non-stop werken;
- Virtuele assistenten vergemakkelijken het dagelijks leven;
- AI is veel nauwkeuriger dan de gemiddelde mens kan zijn;
- AI kan de gezondheidszorg verbeteren;
- AI kan de bescherming van data verbeteren.

24. 24/7 WERKENDE AUTOMATISERING, CONSTANTE ASSISTENTIE. Eén van de belangrijkste en oudste toepassingen van robots is in fabrieken, waar ze het zware, repetitieve werk van arbeiders vergemakkelijken. Hoewel dit hen in het begin niet in dank werd afgenomen, is het op dit moment een realiteit waaraan werknemers voornamelijk voordelen ondervinden. De vooruitgang is echter bijlange nog niet tot een einde gekomen, waardoor er een zekere haat-liefdeverhouding blijft bestaan tussen robots en mensen op de werkvloer, zoals bij de nadelen iets meer zal worden besproken. Niet te ontkennen is echter dat werk op verschillende vlakken een pak lichter is geworden, terwijl de productiecapaciteit van ondernemingen enorm is toegenomen. Win-win dus!

Bijna elke smartphone die er vandaag over de toonbanken schuift is uitgerust met software die de eigenaar van de gloednieuwe minicomputer kan bijstaan bij zijn dagdagelijkse taken: "Siri, hoe is het weer vandaag in Brussel?"; "Alexa, plan een meeting in met Sam op 18 juni 2022"; "Sam, voeg wortels toe aan het winkellijstje"; … Hoewel onze virtuele assistenten ons soms verkeerd begrijpen, maakt AI het mogelijk om met simpele commando's kleine, maar vaak tijdrovende taken uit te voeren waardoor we zelf meer tijd over hebben voor belangrijkere zaken.

25. NAUWKEURIG. Vergissen is menselijk. AI maakt zich hier veel minder schuldig aan. Het kan goed zijn dat de toepassing niet het gewenste gedrag vertoont, maar dat ligt aan een menselijke fout. Op dit moment zijn er namelijk enkel nog maar beperkte AI's, die nagenoeg volledig en alleen maar doen waarvoor ze geprogrammeerd en getraind zijn. Als een algoritme perfect is geschreven, dan maakt het geen fouten.

[69] X, "5 belangrijke voordelen van kunstmatige intelligentie", *uniquenewsonline.com* 5 oktober 2020, https://www.uniquenewsonline.com/nl/5-belangrijke-voordelen-van-kunstmatige-intelligentie/; X, "De voordelen van het gebruik van AI om jouw bedrijfsbezittingen te beveiligen", *stanleysecurity.com* 1 juli 2021, https://www.stanleysecurity.com/nl/blog/de-voordelen-van-het-gebruik-van-ai-om-jouw-bedrijfsbezittingen-te-beveiligen; A. AGRAWAL, "De risico's en voordelen van AI-ondersteunde intelligente automatisering beheren", *CISIN.com* , https://www.cisin.com/coffee-break/nl/technology/managing-the-risks-and-benefits-of-ai-assisted-intelligent-automation.html; R. VANHOOIJDONCK, "Top 20 AI-trends om in de gaten te houden in 2021 en daarna" , *blog.richardvanhooijdonk.com* 16 december 2020, https://blog.richardvanhooijdonk.com/nl/top-20-ai-trends-om-in-de-gaten-te-houden-in-2021-en-daarna/; S. BOONSTRA, "Inzicht in data als eerste stap naar effectieve privacy en security", *outvie.nl* 17 december 2021, https://outvie.nl/kennisbank/effectieve-privacy-security/; X, "89% van de organisaties schiet dramatisch tekort met data protectie", *ictmagazine.nl* 23 februari 2022, https://www.ictmagazine.nl/bedrijfsnieuws/89-van-de-organisaties-schiet-dramatisch-tekort-met-dataprotectie/; F. PETITJEAN, "België in Europese kop van AI-onderzoek", *computable.be* 31 oktober 2018, https://www.computable.be/artikel/nieuws/big-data/6504435/5440850/belgie-in-europese-kop-van-ai-onderzoek.html; …

26. **MEDTECH.**[70] *Medical tech* biedt hulp aan menselijke zorgverstrekkers. Zo zijn er AI-systemen die beter en sneller diagnoses kunnen stellen dan bijna elke dokter met jaren en jaren ervaring. In de operatiezaal kan geen enkele hand van vlees en bloed de precisie van een robotarm evenaren voor bepaalde operaties en bij mensen thuis kan een robot gespecialiseerde hulpverlening alarmeren wanneer er zich een situatie voordoet waarin dit noodzakelijk is.

27. **BETERE BESCHERMING VAN DATA.** AI kan een belangrijke partner zijn bij het beschermen van data om verschillende redenen. Ten eerste zijn algoritmen eindeloos veel beter in snel en correct grote hoeveelheden data verwerken dan mensen. Hierdoor heeft de gebruiker van deze toepassing een heel duidelijk overzicht van welke data er zich binnen de organisatie bevindt, welke er toe komt en welke er buiten gaat. Kennis over deze datastromen is absoluut noodzakelijk om aan effectieve bescherming te doen.

Vervolgens is het toezicht dat AI houdt geen momentopname. Een DPO of een andere daarvoor aangestelde natuurlijke persoon heeft een leven naast zijn of haar taak en kan niet constant op elke verwerking toezien. AI kan dit wel. Door 24/7 surveillance, kunnen niet-conforme verwerkingen, cyberaanvallen of toevallige datalekken veel sneller worden vastgesteld en in een volgende stap worden vermeden. Met dit constant toezicht kan ook elke onregelmatigheid in het gebruik van een systeem worden opgepikt, waardoor de kansen van malware significant worden beperkt.

Ten slotte kan AI ook beoordelingen van bestaande beveiliging uitvoeren om zo tot mogelijke verbeteringen te komen.

28. **OVERZICHT VAN ENKELE NADELEN.** Wanneer aan artificiële intelligentie wordt gedacht is het niet moeilijk om verschillende risico's op te noemen, wat verschillende populaire media dus ook reeds hebben gedaan[71]:

- Verlies van jobs door automatisatie;
- Vooroordelen door verkeerde input;
- Socio-economische ongelijkheid;
- Marktinstabiliteit door algoritmen die super snel handelen;
- Autonome wapens;
- "*Deepfakes*"; en
- Inbreuken op het recht op privacy.

[70] S.K. SHARMA, B. BHUSHAN & N.C. DEBNATH (eds.), *Advances in ubiquitous sensing applications for healthcare, Security and Privacy Issues in IoT Devices and Sensor Networks*, Oxford, Academic Press, 2021, 318p, https://www.sciencedirect.com/book/9780128212554/security-and-privacy-issues-in-iot-devices-and-sensor-networks#book-info.
[71] M. THOMAS, "7 Dangerous Risks of Artificial Intelligence", *builtin.com* 6 juli 2021 (laatste update: 28 juli 2021), https://builtin.com/artificial-intelligence/risks-of-artificial-intelligence.

29. **JOBVERLIES & SOCIO-ECONOMISCHE ONGELIJKHEID.** De eerste toepassing van robots in fabrieken ging nog niet om AI – ze waren namelijk van begin tot eind geprogrammeerd om één taak uit te voeren - maar wel om de automatisatie van taken die saai, vuil of gevaarlijk waren mogelijk te maken. Robots zijn namelijk perfect geschikt om langdurig repetitieve handelingen uit te voeren. In de jaren 1960 zorgde dit ervoor dat grote delen van het assemblageproces van onder andere wagens geautomatiseerd konden worden, wat dus zijn gevolgen had voor de menselijke arbeiders op de werkvloer. AI kan de volgende stap in het automatiseringsproces zijn en is dit ook, zoals duidelijk blijkt uit het feit dat verschillende websites als eerste informatieverstrekker een chatbot paraat hebben staan. Het is zeker niet te vergezocht om te stellen dat niet enkel "*blue collar*"-jobs in het gedrang komen want er zijn reeds verschillende initiatieven volop werkzaam binnen *MedTech*[72], *FinTech*[73], *LegalTech*[74], … .

Het jobverlies dat hand in hand gaat met automatisering, zorgt hoe langer hoe meer ook voor ongelijkheid. Zo is het bijna onvermijdelijk dat bepaalde groepen in de bevolking zwaarder getroffen (zullen) worden dan anderen. Hiernaast is er reeds bij de ontwikkeling van AI een duidelijke ongelijkheid op te merken. Het merendeel van AI-onderzoekers is namelijk blank, mannelijk, groeide op in "de gegoede klassen" van de bevolking en heeft meestal geen handicap. Deze redelijk homogene groep zorgt onbedoeld voor het volgende probleem waarmee AI kampt.[75]

30. **VOOROORDELEN.** Er zijn verschillende AI-toepassingen bekend die discriminerend zijn of waren[76]. De algoritmes maken/maakten een onderscheid op basis van huidskleur, geslacht, leeftijd, … Verschillende AI's, ontwikkeld door even veel verschillende bedrijven, hebben – per ongeluk – geleerd om een onderscheid te maken op basis van kenmerken die hiertoe niet zouden mogen dienen wanneer onze universele normen en waarden in acht worden genomen.[77] Microsoft[78], Amazon[79], Google[80],

[72] **Medical technology**: houdt zich bezig met alle soorten technologieën die medisch opgeleid personeel kunnen bijstaan in hun werkzaamheden. Ondertussen zijn er robots die beter kunnen diagnosticeren dan mensen met jarenlange ervaring en die operaties met meer succes kunnen uitvoeren dan chirurgen omdat ze simpelweg veel gecontroleerder kunnen bewegen dan menselijke ledematen. Zie hiervoor onder andere: https://www.medtecheurope.org/.

[73] **Financial technology**: zet in op de verbetering of automatisering van financiële diensten. Zo worden de financiële beurzen heden ten dage niet meer gerund door effectenmakelaars, maar wel door hun computers die in een fractie van de tijd veel meer deals kunnen sluiten waardoor de koersen voor normale mensen niet meer bij te houden zijn. Ook op het niveau van boekhouding en accountancy steken algoritmes de kop op. Zie hiervoor onder andere: https://builtin.com/fintech.

[74] **Legal technology**: focust zich op de juridische wereld en wordt momenteel gedomineerd door geavanceerde zoekmachines en programma's die het mogelijk maken om relatief gemakkelijk een standaardcontract op te stellen voor minder complexe zaken. Ook zijn er chatbots die op veel vragen een simpel antwoord kunnen formuleren waardoor enkel nog de complexere/interessante vraagstukken tot bij een menselijke collega geraken. Zie hiervoor onder andere: https://lawren.io/nl/; M. CORREA, "What is Legal Technology and how is it Changing our Industry?", *The Lawyer Portal* 29 januari 2019, https://www.thelawyerportal.com/blog/what-is-legal-tech-and-how-is-it-changing-industry/.

[75] Olga Russakovsky …

[76] F. DIETZ, "Why your AI might be racist and what to do about it", *Towardsdatascience.com* 9 november 2019, https://towardsdatascience.com/why-your-ai-might-be-racist-and-what-to-do-about-it-c081288f600a.

[77] Denk hierbij onder andere aan het UVRM, EVRM, de Grondwetten, …

[78] A. KRAFT, "Microsoft shuts down AI chatbot after it turned into a Nazi", *CBS News* 25 maart 2016, https://www.cbsnews.com/news/microsoft-shuts-down-ai-chatbot-after-it-turned-into-racist-nazi/; A. TENNERY & G. CHERELUS, "Microsoft's AI Twitter bot goes dark after racist, sexist tweets", *Reuters* 24 maart 2016, https://www.reuters.com/article/us-microsoft-twitter-bot-idUSKCN0WQ2LA.

[79] J. BUOLAMWINI, "Artificial Intelligence Has a Problem With Gender and Racial Bias. Here's How to Solve It", *Time* 7 februari 2019, https://time.com/5520558/artificial-intelligence-racial-gender-bias/.

[80] N. KAYSER-BRIL, "Google apologizes after its Vision AI produced racist results", *Algorithm Watch* 7 april 2020, https://algorithmwatch.org/en/google-vision-racism/.

Facebook[81], IBM[82], en verschillende anderen[83] hebben aan den lijve moeten ondervinden dat AI enorm afhankelijk is van de data waarmee ze gevoed wordt. Meestal waren het namelijk niet de algoritmen die voor de vooroordelen zorgden, maar wel de data waarmee ze werden getraind.

31. **AUTONOME WAPENS.** AI kan voor verschillende militaire doeleinden worden ingezet. Niet ten minste om wapens nog nauwkeuriger te maken dan ze nu al zijn. Het meest sci-fi-geïnspireerde aspect van alle risico's is er één waarin AI zelf beslissingen gaat nemen over het gebruik van nucleaire of biologische wapens. Uit de open brief die meer dan 30.000 mensen, wetenschappers en particulieren, ondertekenden blijkt dat autonome wapens een grote vrees zijn, waar dus niet aan voorbij kan worden gegaan.[84] België is een drijvende kracht om de productie van "*Lethal Autonomous Weapon Systems*" (LAWS), *killer robots* of de in het Nederlands minder welluidend "*dodelijke autonome wapensystemen"* te verbieden.[85]

32. **DEEPFAKES & PRIVACY.** "Deepfakes" zijn beeld- en audiomaterialen die zodanig verregaand samengevoegd en gemanipuleerd zijn dat ze door het menselijke oog en oor niet meer te onderscheiden zijn van het echte. Vals beeldmateriaal is op zich niets nieuws, maar deze technologie maakt het mogelijk om volledig computer-gegenereerde gezichten van onbestaande mensen te vormen maar ook om met buitengewone precisie bestaande gezichten te reproduceren.[86] De "eigenaars" van deze gezichten kunnen dus geconfronteerd worden met uitspraken die ogenschijnlijk door hen werden gedaan, zonder dat dit ooit effectief het geval was.[87] Hoewel deze technologie op het eerste zicht veel leuke, grappige en nuttige toepassingen kan hebben, is op dit moment vooral het negatieve aspect zeer prominent.

---

[81] E. RIOS, "Facbook's AI Seems to Have a Racism Problem", *Mojo Wire* 5 september 2021, https://www.motherjones.com/mojo-wire/2021/09/facebooks-ai-seems-to-have-a-racism-problem/.
[82] M. ENGELHARDT & J. ECKES, "From BLM to IBM: Racism and Bias in AI", *MTS.mediencampus.h-da.de* 10 november 2020, https://mts.mediencampus.h-da.de/blog/from-blm-to-ibm-racism-and-bias-in-ai/.
[83] T. TRAN, "Scientists Built an AI to Give Ethical Advice, But It Turned Out Super Racist", *Futurism* 22 oktober 2021, https://futurism.com/delphi-ai-ethics-racist; X, "Artificial intelligence: Algorithms face scrutiny over potential bias", *BBC News* 20 maart 2019, https://www.bbc.com/news/technology-47638916; N. SARWAR, "AI Created To Give Ethical Advice Is Being Racist And Murderous", *ScreenRant* 25 oktober 2021, https://screenrant.com/ai-ethical-advice-racist-murderous/.
[84] X, "Autonomous Weapons: An Open Letter From AI & Robotics Researchers", https://futureoflife.org/2016/02/09/open-letter-autonomous-weapons-ai-robotics/.
[85] Voorstel van Resolutie, 23 juni 2021, betreffende een internationaal verbodsverdrag op dodelijke autonome wapensystemen, (DOC 55 2087/001), https://www.dekamer.be/FLWB/PDF/55/2087/55K2087001.pdf.
[86] Hierbij kan de vraag gesteld worden welke andere specifieke rechten hier een bepaalde invloed op kunnen hebben. Het portretrecht, een onderdeel van het recht op afbeelding, dat op zijn beurt een recht is dat zeer nauw gelinkt is aan het overkoepelende recht dat in deze thesis in het tweede deel zal worden besproken: het recht op bescherming van persoonsgegevens; dat natuurlijk onder het recht op privacy te categoriseren valt.
[87] J. KIETZMANN, L.W. LEE, I.P. MCCARTHY & T.C. KIETZMANN, "Deepfakes: Trick or treat?", *Business Horizons* 2020, 63(2), p. 135–146, https://www.sciencedirect.com/science/article/pii/S0007681319301600?via%3Dihub; J. BRANDON, "Terrifying high-tech porn: Creepy 'deepfake'videos are on the rise", *Foxnews* 20 februari 2020, https://www.foxnews.com/tech/terrifying-high-tech-porn-creepy-deepfake-videos-are-on-the-rise.

Zo wordt ze onder andere ingezet om "fake news"[88], "revengeporn"[89] en frauduleuze documenten[90] te fabriceren.[91]

Deze scriptie zal verder niet ingaan op de discussie of het privacy- en/of AI-recht de meest opportune rechtstakken zijn om deze problematiek aan te pakken, maar het is wel duidelijk dat er een belangrijk risico voor persoonsgegevens schuilt in het bedrieglijk gebruik van gezichten.

Deepfakes vormen ook niet het enige risico voor privacy. Zoals op dit punt reeds zeer duidelijk is, werken AI-toepassingen voornamelijk op en met data. Ze worden gebruikt om enorme hoeveelheden data overzichtelijk te maken en ze worden getraind om andere taken uit te voeren met specifiek daarvoor bedoelde data. De manier waarop de algoritmes beveiligd zijn, hangt onlosmakelijk vast aan hoe goed de data zelf is beveiligd. De manier waarop beslissingen worden gemaakt, bepaalt op welke manier de data worden gebruikt, … [92] [93]

[88] O. SCHWARTZ, "You thought fake news was bad? Deep fakes are where truth goes to die", *The Guardian* 12 november 2018, https://www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth.

[89] A. GHOSHAL, "Twitter, Pornhub and other platforms ban AI-generated celebrity porn", *TNW* 7 februari 2018, https://thenextweb.com/news/twitter-pornhub-and-other-platforms-ban-ai-generated-celebrity-porn.

[90] M. SCHREYER, T. SATTAROV, B. REIMER & D. BORTH, "Adversarial Learning of Deepfakes in Accounting", *onuitgegeven*, https://doi.org/10.48550/arXiv.1910.03810.

[91] Duidelijk is dat het gebruik van andermans gezicht uitermate problematisch is. Hoewel het niet gezegd is welk recht dit precies dient op te lossen – portretrecht, privacy-recht, of het toekomstig AI-recht – kan niet worden geaccepteerd dat het onherkenbaar copy-pasten van een gezicht kan vallen onder de uitzondering voor satire en parodie (in het geval van fake-news) of dat er geen inbreuk op het privéleven zou bestaan wanneer je het slachtoffer bent van revengeporn. Zie oa. A. BANKS, "Deepfakes & Why the future of porn is terrifying", *Highsnobiety* 2018, https://thenextweb.com/news/twitter-pornhub-and-other-platforms-ban-ai-generated-celebrity-porn.

[92] Zie infra: vanaf Randnummer 56 – Context van het voorstel tot en met Randnummer 71 – AI en voorstel van AI-verordening in een notendop.

[93] Slotbedenking bij deze titel: De enorme expansie in de hoeveelheid data die tegenwoordig bestaat en op dagelijkse basis wordt gegenereerd en verwerkt brengt uiteraard ook evenredige risico's met zich mee betreffende de bescherming ervan. AI is heden ten dage gewoonweg noodzakelijk om de verwerking van dergelijke hoeveelheden data mogelijk te maken omdat het voor mensen gewoon niet meer te overzien is. De moeilijkheid ligt er in deze in dat het probleem onlosmakelijk verbonden is met de oplossing. AI heeft data nodig om te bestaan, te leren en een nut te hebben. Langs de andere kant is het momenteel ook zo dat de mens AI nodig heeft om de gegenereerde hoeveelheden data verwerkt te krijgen. Er valt dus een soort kip-ei-cirkelredenering te herkennen. Beide elementen hebben elkaar zodanig versterkt dat het moeilijk wordt om een definitief antwoord te bieden op wie eerst was: De enorme hoeveelheid data, die enkel door AI nog verwerkt kan worden; of de AI, die gevoed, getraind en bedoeld is om data te verwerken en deze dus nodig heeft.

1.2.2. In het Voorstel van AI-Verordening

33. JURIDISCH RELEVANTE RISICOANALYSE. Na het voorgaande overzicht van enkele voor- en nadelen die door de klassieke mediakanalen worden opgemerkt in de randnummers 22 tot 32, zal vanaf nu gekeken worden naar de meer juridisch relevante risicoanalyse waarop de wetgever zich bij het voorstel van AI-verordening heeft gebaseerd. Uit de toelichting bij dit voorstel zal blijken dat voor de identificatie van de impact van AI in de hoofdzaak naar twee belangrijke teksten wordt verwezen: het "Witboek betreffende Kunstmatige Intelligentie"[94] dat de Europese Commissie hierover heeft uitgebracht; en de "Ethische Richtsnoeren voor Betrouwbare Kunstmatige Intelligentie"[95], opgesteld door de Deskundigengroep op Hoog Niveau inzake Kunstmatige Intelligentie (AI HLEG)[96]. Beide documenten kunnen als invloedrijke voorbereidende werken worden gezien voor het Voorstel van AI-Verordening dat op 21 april 2021 aan het Europees Parlement en de Raad van de Europese Unie werd voorgelegd, en zullen de belangrijkste bronnen zijn voor dit hoofdstuk.

In de toelichting bij het voorstel wordt duidelijk gemaakt dat er gekozen is voor een "*horizontaal EU-wetgevingsinstrument volgens een evenredige, risico-gebaseerde aanpak + gedragscodes voor AI-systemen zonder hoog risico*"[97]. Er wordt dus een onderscheid gemaakt tussen:

- Verboden systemen;
- Hoog risico systemen; en
- Laag of minimaal risico systemen.

Een verdere bespreking van de risicogebaseerde aanpak die het voorstel typeert, zal in hoofdstuk 3[98] worden uitgewerkt. Onder deze titel zal eerst verder worden besproken wat deze risico's volgens het voorstel, het Witboek en de Ethische richtsnoeren nu net inhouden en hoe deze door middel van raadplegingen[99] van belanghebbenden[100] in kaart werden gebracht.

34. RISICO'S GEÏDENTIFICEERD IN HET VOORSTEL. In de toelichting bij het voorstel wordt maar weinig expliciete melding gemaakt van belangrijke risico's. Wel wordt ons op het hart gedrukt dat de wetgever zich bewust is van de gevaren. De tekst echter, focust duidelijk op alle mogelijke voordelen.[101] Het is in deze namelijk ook niet meer echt nodig om alle nadelen te gaan opsommen, aangezien deze taak reeds ter harte werd genomen in het Witboek en de Ethische Richtsnoeren. Deze positieve kijk wordt verdergezet in de overwegingen waar enkel nog overwegingen 4 en 5 kort erkennen dat er risico's

[94] Europese Commissie, Witboek over kunstmatige intelligentie – een Europese benadering op basis van excellentie en vertrouwen, 19 februari 2020, COM (2020) 65 final.
[95] Europese Commissie - Directoraat-Generaal Communicatienetwerken, Inhoud en Technologie, Ethische richtsnoeren voor betrouwbare KI, Publications Office, 8 april 2019.
[96] "*High-Level Expert Group on Artificial Intelligence*".
[97] 3.3 effectenbeoordeling, in de Toelichting bij het voorstel van AI-verordening.
[98] Zie infra: Vanaf Randnummer XXX.
[99] 3.1. Raadpleging van belanghebbenden & 3.2. Bijeenbrengen en gebruik van expertise, in de Toelichting bij het voorstel van AI-verordening.
[100] Burgers, academici, praktijkdeskundigen, commerciële en niet-commerciële organisaties en overheden.
[101] 1.1. Motivering en doel van het voorstel; 3.1. Raadpleging van belanghebbenden; 3.2. Bijeenbrengen en gebruik van expertise; en 3.5. Grondrechten, in de Toelichting bij het voorstel van AI-verordening.

mogelijk zijn en dat er daarom moet worden ingezet op goede, geharmoniseerde wetgeving binnen de EU.

De effectieve tekst van het voorstel van AI-verordening is opgebouwd volgens een model dat zich volledig baseert op het risiconiveau van verschillende toepassingen, waarover later meer.[102]

1.2.3. Ethische Richtsnoeren voor betrouwbare Kunstmatige Intelligentie

35. INTRODUCTIE BIJ DE "ETHISCHE RICHTSNOEREN". De zoektocht naar een manier om artificiële intelligentie en haar ontwikkeling een duidelijke richting te geven is al geruime tijd aan de gang. Het was natuurlijk geen optie om een dergelijk interessante en lucratieve technologie een stille dood te doen sterven door haar te streng aan banden proberen te leggen. Daarom moest er dus een afweging worden gemaakt.

In 2018 bracht de AI HLEG hiertoe een eerste versie van "Ethische Richtsnoeren" uit. In deze uitgave werd een openbare raadpleging georganiseerd waarop meer dan vijfhonderd belanghebbende partijen, verspreid over de EU, zijn ingegaan. In de volgende versie van 18 december 2019, waarop deze scriptie gebaseerd is, zijn alle opmerkingen en feedback opgenomen om zo te komen tot de conclusie dat betrouwbare AI moet bestaan uit drie componenten:

- De AI moet **wettig** zijn;
- De AI moet **ethisch** zijn; en
- De AI moet **robuust** zijn.

De wettigheid van AI zal in de toekomst worden geregeld door de toekomstige AI-verordening. Omdat er in 2019 nog geen voorstel was, behandelen de Richtsnoeren de vereiste van wettigheid verder niet.[103] Wat voor de onderzoekers betrokken bij de richtsnoeren interessanter en relevanter was, is de "*lex ferenda*"; de "*law as it should be*". Wat moet AI-wetgeving helpen realiseren en waarom is dat het doel? Het ethische en robuuste aspect van AI wordt daarom wel uitvoerig behandeld in de drie hoofdstukken die in steeds hogere graad van praktische toepasselijkheid zijn geschreven. Het is voornamelijk het laatste deel (C)[104] dat relevant is voor deze scriptie. De titel van dit deel spreekt voor zich:

> "Voorbeelden van de mogelijkheden en punten van zorg die KI met zich meebrengt"[105]

[102] Zie infra: Randnummer 61 – Risicogebaseerde aanpak.
[103] Zie hiervoor Randnummer 2 van de Richtsnoeren.
[104] Europese Commissie - Directoraat-Generaal Communicatienetwerken, Inhoud en Technologie, Ethische richtsnoeren voor betrouwbare KI, Publications Office, 8 april 2019, p. 41-45, Randnummer 121-135.
[105] Zoal eerder reeds kort vermeld staat KI voor Kunstmatige Intelligentie, hetgeen exact hetzelfde is als Artificiële Intelligentie.

Voordelen

36. **DRIE GROTE VOORDELEN.**[106] De AI HLEG identificeert drie grote groepen van voordelen die AI kan bewerkstelligen voor enkele urgente uitdagingen waarmee de wereld kampt:

1. Klimaatactie en duurzame infrastructuur;
2. Gezondheid en welzijn; en
3. Goed onderwijs en digitale transformatie.

Klimaatactie en duurzame infrastructuur[107]

37. **GRONDSTOFFEN, ENERGIE & INFRASTRUCTUUR.** De belangrijkste aspecten waarin computers eindeloos veel beter zijn dan mensen zijn: geheugen en wiskunde. Het is dus ook op deze vlakken dat ze een belangrijk verschil kunnen maken. Door bijvoorbeeld AI-toepassingen te koppelen aan big data[108] zou het mogelijk zijn om energie en grondstoffen veel efficiënter te benutten door onze behoeften nauwkeuriger vast te stellen en de infrastructuur daarop af te stellen.

38. **MOBILITEIT.** De motoren waarop onze vervoersmiddelen bewegen zijn een belangrijk aspect in de klimaatcrisis. Ook hier kan AI helpen om koolstof achter ons te laten en energie nuttiger te gebruiken. Ook files zouden opgelost kunnen worden door routes te optimaliseren en alle vervoersmiddelen in "real-time" met elkaar in contact te brengen zodat ze zich op elkaar kunnen afstemmen.

Gezondheid en welzijn[109]

39. **MEDTECH.**[110] AI kan en wordt al gebruikt om behandelingen slimmer en gerichter te maken. Dokters worden voorbijgestoken op het vlak van diagnostisering en AI-systemen kunnen soms lang voor hun menselijke collega's ziektes vaststellen waardoor een anticipatieve en preventieve aanpak mogelijk is. In de ouderenzorg is AI een waardevol hulpmiddel dat bijvoorbeeld ten alle tijde voor toezicht kan zorgen.

Goed onderwijs en digitale transformatie[111]

40. **JOBS & ONDERWIJS.** Naast haar destructieve aspect op de werkvloer zoals we dat vandaag voornamelijk kennen, kan AI ook ineens een oplossing bieden voor deze veranderende jobnoden door zo nauwkeurig mogelijk te voorspellen welke jobs en beroepen door de technologie zullen worden verstoord, te identificeren waar zich nieuwe mogelijkheden zullen voordoen en op beiden te anticiperen door het onderwijs op de toekomstige noden af te stellen.

---

[106] Europese Commissie - Directoraat-Generaal Communicatienetwerken, Inhoud en Technologie, Ethische richtsnoeren voor betrouwbare KI, Publications Office, 8 april 2019, p. 41-43.
[107] Europese Commissie - Directoraat-Generaal Communicatienetwerken, Inhoud en Technologie, Ethische richtsnoeren voor betrouwbare KI, Publications Office, 8 april 2019, p. 42.
[108] In de zin van de hoeveelheid aan data. → Zie supra: Randnummer 19.
[109] Europese Commissie - Directoraat-Generaal Communicatienetwerken, Inhoud en Technologie, Ethische richtsnoeren voor betrouwbare KI, Publications Office, 8 april 2019, p. 42-43.
[110] Zie supra: Randnummer 29 – Jobverlies & Socio-economische ongelijkheid.
[111] Europese Commissie - Directoraat-Generaal Communicatienetwerken, Inhoud en Technologie, Ethische richtsnoeren voor betrouwbare KI, Publications Office, 8 april 2019, p. 43.

Binnen het onderwijs zelf biedt AI de mogelijkheid om voor iedereen een aangepast, gepersonaliseerd programma samen te stellen waardoor de kwaliteit van onderwijs in het algemeen significant kan worden verhoogd.

Nadelen

41. **ZWARTE ZWANEN.** De Ethische Richtsnoeren vermelden vier grote groepen van potentiële risico's en waarschuwen voor de onzekerheid die gepaard gaat met technologie die elke dag vorderingen maakt. Er wordt stilgestaan bij de mogelijkheid dat niet alle factoren gekend zullen en kunnen zijn en de zogenaamde "zwarte zwanen".[112] Daarom zal het absoluut noodzakelijk zijn om regelmatig risicoanalyses te blijven uitvoeren. Het moet dus ook vanzelfsprekend zijn dat onderstaande lijst niet limitatief is.[113]

Naast alle onzekerheden die er bij elke nieuwe stap vooruit zullen ontstaan was het in 2019 wel al duidelijk dat AI op vier aspecten extra goed in de gaten gehouden moet worden:

1. AI die personen kan herkennen en volgen;
2. AI die verborgen is;
3. AI die burgers kan beoordelen; en
4. Dodelijke autonome wapensystemen.

AI die personen kan herkennen en volgen[114]

42. **BIG BROTHER.** ANPR-camera's zijn al lang geen nieuw fenomeen meer, in onder andere het Verenigd Koninkrijk en China kan je geen stap zetten zonder dat CCTV[115] of de iets geavanceerdere Chinese gezichtsherkennende, slimme camera's het hebben gezien. Het constant monitoren en volgen van personen, zonder enige rechtmatige reden gaat in tegen het principe van onschuld tot het tegendeel is bewezen. Elke persoon die zich in de openbare ruimte begeeft wordt namelijk gezien als een potentieel crimineel. Het is daarom van groot belang dat de wetgeving deze toepassingen duidelijk reguleert.

Het is uiteraard wel een zeer handig middel in de strijd tegen criminaliteit, zolang hiervoor geen buitenproportionele surveillance van de gewone burger moet worden getolereerd. De AI-verordening komt hieraan expliciet tegemoet in artikel 5.2, waarover later meer.[116]

AI die verborgen is[117]

43. **TURING TEST.** Het is vooral op ethisch vlak van belang dat mensen weten met wie of wat ze te maken hebben. Het is namelijk niet ondenkbaar dat mensen zich door AI zouden laten beïnvloeden of eraan gehecht raken, zoals dat ook vaak genoeg voorkomt met menselijke oplichters online.[118] Ook stelt

[112] Een zwarte zwaan is een zeer zeldzame gebeurtenis met grote gevolgen – zo zeldzaam dat deze mogelijk nog nooit is voorgekomen. Daarom kan gewoonlijk slechts met zeer weinig zekerheid worden vastgesteld hoe groot de kans erop is.
[113] Europese Commissie - Directoraat-Generaal Communicatienetwerken, Inhoud en Technologie, Ethische richtsnoeren voor betrouwbare KI, Publications Office, 8 april 2019, p. 45, randnummer 135.
[114] Europese Commissie - Directoraat-Generaal Communicatienetwerken, Inhoud en Technologie, Ethische richtsnoeren voor betrouwbare KI, Publications Office, 8 april 2019, p. 44, randnummer 130.
[115] "*Closed-Circuit Television*".
[116] Zie infra, Randnummer 61 – Risicogebaseerde aanpak.
[117] Europese Commissie - Directoraat-Generaal Communicatienetwerken, Inhoud en Technologie, Ethische richtsnoeren voor betrouwbare KI, Publications Office, 8 april 2019, p. 44, randnr. 131.
[118] Denk hierbij maar aan de problematiek omtrent "phishing", "catfishen", …

de AI HLEG dat de ontwikkeling van op mensen gelijkende robots de "waarde van het mens-zijn" zou kunnen verminderen, waardoor zorgvuldige ethische controle dus echt wel op zijn plaats is.

***AI die burgers kan beoordelen*[119]**

44. **THOUGHT POLICE.**[120] Omdat onze samenleving ernaar streeft om de vrijheid en autonomie van alle burgers te verzekeren, is het zeer zorgwekkend wanneer op basis van AI een beoordeling van het (verwachte) gedrag kan worden gemaakt en hieraan dus ook implicaties worden verbonden. Het is belangrijk dat een dergelijke beoordeling enkel mogelijk mag zijn wanneer ze duidelijk gerechtvaardigd is en de maatregel in kwestie ook evenredig en rechtvaardig is. Ook hier heeft het voorstel van AI-verordening dit punt meegenomen en artikel 5.1.c verbiedt dit soort toepassingen in de regel met slechts enkele strikt afgelijnde uitzonderingen.[121]

***Dodelijke autonome wapensystemen*[122]**

45. **"LAWS".** Het is geweten dat "men" zich momenteel bezighoudt met onderzoek naar, en de ontwikkeling van de eerder reeds aangehaalde "LAWS"[123]. Wat niet geweten is, is om welke landen en sectoren het precies gaat en hoe ver deze ontwikkelingen staan. Het kan *in casu* gaan om raketten voor selectieve aanvallen tot lerende machines die zonder menselijke interventie zouden kunnen gaan beslissen waar, wanneer en met wie ze gaan vechten.

[119] Europese Commissie - Directoraat-Generaal Communicatienetwerken, Inhoud en Technologie, Ethische richtsnoeren voor betrouwbare KI, Publications Office, 8 april 2019, p. 44-45, randnr. 132.
[120] G. ORWELL, *Nineteen Eighty-Four*, Londen, Secker & Warburg, 1949, 328p.
[121] Zie uitgebreider infra: Randnummer 61 – Risicogebaseerde aanpak.
[122] M. GUETLEIN, "Lethal autonomous weapons — Ethical and doctrinal implications", Naval War College Newport 14 februari 2005, onuitg., https://apps.dtic.mil/sti/pdfs/ADA464896.pdf; H.M. ROFF, "The Strategic Robot Problem: Lethal Autonomous Weapons in War", Journal of Military Ethics (vol. 13, issue 3) 2013, https://doi.org/10.1080/15027570.2014.975010; E. BARBÉ & D. BADELL, "The European Union and Lethal Autonomous Weapons Systems: United in Diversity?", in E. JOHANSSON-NOGUÉS, M.C. VLASKAMP & E.BARBÉ (eds.), European Union Contested – Foreign policy in a New Global Context, Cham, Springer, 2020, 219 p., https://doi.org/10.1007/978-3-030-33238-9.
[123] Zie supra: Randnummer 31 – Autonome wapens.

1.2.4. Witboek over Kunstmatige Intelligentie – Een Europese benadering op basis van excellentie en vertrouwen

46. INTRODUCTIE BIJ HET WITBOEK OVER KUNSTMATIGE INTELLIGENTIE.

"Kunstmatige intelligentie ontwikkelt zich snel. Ze zal onze levens veranderen door de gezondheidszorg te verbeteren (bv. door nauwkeuriger diagnoses, waardoor betere preventie van ziekten mogelijk wordt), de landbouw efficiënter te maken, bij te dragen tot de bestrijding van en aanpassing aan de klimaatverandering, de efficiëntie van productiesystemen te verbeteren via voorspellend onderhoud, de beveiliging van de Europese burgers te versterken, en op veel andere manieren die we ons nu nog amper kunnen inbeelden. Tegelijkertijd brengt kunstmatige intelligentie (KI) een aantal potentiële risico's met zich mee, zoals een gebrek aan transparantie bij de besluitvorming, gender- of andere vormen van discriminatie, schending van de privacy of gebruik voor criminele doeleinden."[124]

Met deze woorden start de Europese Commissie haar "Witboek over Kunstmatige Intelligentie". Het mag voor alle betrokkenen duidelijk zijn dat er in de toekomst alleen maar een toename zal zijn van digitale technologie en de Commissie erkent daarom dus ook dat het absoluut noodzakelijk is dat mensen er vertrouwen in kunnen hebben.[125] Hiertoe stelt de Commissie dat de AI van de toekomst excellentie en vertrouwen moet nastreven.

47. EXCELLENTIE. Het Witboek is als het ware een draaiboek van de Commissie waarin wordt opgesomd wat nodig is om te komen tot deze beoogde "Europese benadering van Excellentie en Vertrouwen". Hiertoe wordt eerst vastgesteld wat nodig is om tot excellentie te komen: hoe kan ervoor gezorgd worden dat de EU één van de sterkste, zo niet de sterkste positie behoudt op vlak van AI, in welke ondersteunende technologieën moet worden geïnvesteerd, welke infrastructuur is daarvoor nodig, hoe zal voor optimale samenwerking tussen lidstaten onderling en de particuliere sectoren worden gezorgd, … Allemaal vragen waarop door het Witboek een antwoord wordt gegeven.

48. VERTROUWEN. Het volgende onderdeel van het Witboek gaat over vertrouwen. Het is hier dat de voorwaarden waaraan een wettelijk kader moet voldoen worden besproken: in welk regelgevingskader het – toen nog onbestaande – voorstel van AI-verordening zou moeten werken, welke aanpassingen

[124] Europese Commissie, Witboek over kunstmatige intelligentie – een Europese benadering op basis van excellentie en vertrouwen, 19 februari 2020, COM (2020) 65 final, p. 1.
[125] Europese Commissie, Witboek over kunstmatige intelligentie – een Europese benadering op basis van excellentie en vertrouwen, 19 februari 2020, COM (2020) 65 final, p. 1.

nodig zouden zijn aan reeds bestaande wetgeving en welke zeven types van wetgeving de AI-verordening zou moeten bevatten.[126] [127]

Voorafgaand hieraan is er een korte probleemanalyse verwoord, wat op dit punt in deze scriptie het meest relevante stuk is, en waarop in de volgende randnummers dieper zal worden ingegaan.

Voordelen

49. **HERHALING.** Net zoals Ethische Richtsnoeren die het Witboek zijn voorafgegaan en het voorstel van AI-verordening dat eerder reeds werd besproken, identificeert het Witboek zelf niet echt nieuwe, belangrijke voordelen. Het mag ondertussen duidelijk zijn dat deze significant zijn en alleen maar zullen toenemen in aantal en impact naargelang de ontwikkeling verder gaat.

Nadelen

50. **TWEE SOORTEN RISICO'S.** De opdeling van de risico's, hoewel ook deze in dezelfde lijn verder gaat als de voorgaande risicoanalyses,[128] is significant verschillend. De commissie onderscheidt in deze twee categorieën:

1. Risico's voor de grondrechten, met inbegrip van de bescherming van persoonsgegevens en privacy en non-discriminatie; en
2. Risico's voor de veiligheid en de doeltreffende werking van de aansprakelijkheidsregeling.

Risico's voor de grondrechten, met inbegrip van de bescherming van persoonsgegevens en privacy en non-discriminatie[129]

51. **FUNDAMENTELE RECHTEN.** Het Witboek zet haar roze bril even af om enkele verregaande potentiële gevaren te beschrijven waaraan AI gevoelig is, en zeer waarschijnlijk gevoelig aan zal blijven. Zo lopen verscheidene fundamentele rechten het risico te worden geschonden, zelfs buiten het kwaadwillig en dus gewoonweg illegaal gebruik van AI-toepassingen om. Het recht op vrijheid van meningsuiting, vrijheid van vergadering, de menselijke waardigheid, het beginsel van non-discriminatie op basis van geslacht, ras, etnische afkomst, religie of overtuiging, handicap, leeftijd of seksuele geaardheid, het recht op een

[126] **Trainingsdata**: zonder data, geen AI. Daarom is het van groot belang dat de data waarmee AI getraind wordt ook voldoet aan de normen en waarden van de EU; **data en registers**: één van de grote problemen rond AI is dat het niet duidelijk is hoe het tot zijn output komt. Om dit tegen te gaan moeten er registers worden bijgehouden van de algoritmes en de data waarmee het werkt. Zo kan – ten minste in theorie – worden nagekeken hoe tot conclusies wordt gekomen en kunnen aanpassingen gericht worden doorgevoerd; **te verstrekken informatie**: Zowel voor de gebruikers als voor datasubjecten (meestal burgers), is het belangrijk voor het vertrouwen in AI, dat ze degelijke informatie over het systeem ontvangen over de mogelijkheden en de gebreken; **robuustheid en nauwkeurigheid**: teneinde een eindproduct te bekomen dat betrouwbaar een nauwkeurig is, moet doorheen het volledige productieproces van AI de technische robuustheid in het achterhoofd worden gehouden. d.w.z. dat vanaf het begin rekening moet worden gehouden met de mogelijke risico's en dat alle redelijke maatregelen moeten worden genomen om eventuele schade tot een minimum te beperken; **menselijk toezicht**: zoals reeds meermaals is vermeld bestaat er op dit moment nog geen algemene AI en één van de zwakheden van de systemen zal altijd het gebrek gevoelens het intuïtie zijn, dat inherent is aan de mensheid. Daarom is het van buitengewoon groot belang dat er te allen tijde een menselijke evaluatie van AI-output is, hetzij voorafgaand aan de implementering van een beslissing, hetzij erna; **specifieke voorschriften voor welbepaalde KI-toepassingen, bijvoorbeeld voor biometrische identificatie op afstand**: Het verwerken van biometrische data brengt zeer specifieke risico's met zich mee en vereist dus ook een specifieke regelgeving die hieraan tegemoet kan komen.

[127] Europese Commissie, Witboek over kunstmatige intelligentie – een Europese benadering op basis van excellentie en vertrouwen, 19 februari 2020, COM (2020) 65 final, p. 10-25.

[128] Zie supra: Randnummers 22-32 (Risico's opgeworpen in klassieke mediakanalen) & 35-45 (Risico's opgeworpen in de Ethische richtsnoeren).

[129] Europese Commissie, Witboek over kunstmatige intelligentie – een Europese benadering op basis van excellentie en vertrouwen, 19 februari 2020, COM (2020) 65 final, p. 12-13.

doeltreffende voorziening in rechten en een eerlijk proces, consumentenbescherming en ten slotte het recht op bescherming van persoonsgegevens en privacy worden allemaal bedreigd door AI die met goede bedoelingen wordt ontwikkeld. Dit komt omdat het risico op vooroordelen en discriminatie inherent is aan elke maatschappij of economische activiteit en het uiteraard deze setting is waarin AI wordt ontwikkeld.

Het probleem met dergelijke – per ongeluk – ingebouwde vooroordelen, is dat deze voor een veel grotere groep mensen serieuze gevolgen kunnen hebben wanneer deze consequent door AI zouden worden toegepast. Het is namelijk een gekend probleem dat er maar weinig echt inzicht is in hoe een systeem nu exact tot conclusies komt.

Met de toenemende mogelijkheden van AI, zullen veel meer beslissingen, waarvoor voordien mensen nodig waren, worden genomen door, of met inmenging van, AI-systemen. Rekening houdend met vorige alinea is het niet meer dan logisch dat dit een problematische ontwikkeling kan zijn. Hier bovenop komt nog eens dat de gegevensbeschermingswetgeving sterk onder druk kan worden gezet door AI-toepassingen omdat de mogelijkheid om immense hoeveelheden data tegen ongeziene snelheden te verwerken en verbanden te leggen, het ook mogelijk maakt om data te de-anonimiseren en dit zelfs uit datasets die op zich geen persoonsgegevens bevatten …

Risico's voor de veiligheid en de doeltreffende werking van de aansprakelijkheidsregeling[130]

52. **MATERIËLE SCHADE EN PRODUCTAANSPRAKELIJKHEID.** Na de Sci-Fi-scenario's zijn er ook de meer concrete schadegevallen die uit tekortkomingen in het ontwerp van de technologie of uit problemen met de beschikbaarheid en kwaliteit van data voor machinaal leren voortvloeien. Het kan hier bijvoorbeeld gaan om het foutief identificeren door een autonome wagen van een voorwerp op de weg met gewonden en/of materiële schade tot gevolg.

Een gebrek aan duidelijk omschreven eisen waaraan AI-producten die op de EU-markt worden gebracht, kan leiden tot onzekerheid met betrekking tot de aansprakelijkheid voor gebrekkige producten. Ook de onmogelijkheid om na te gaan wat nu net aan de grondslag lag van een problematische output, doet onzekerheid ontstaan omtrent bevoegdheden, aansprakelijkheid en handhavingsmechanismen.

[130] Europese Commissie, Witboek over kunstmatige intelligentie – een Europese benadering op basis van excellentie en vertrouwen, 19 februari 2020, COM (2020) 65 final, p. 13-14.

1.2.5. Toegepast of het recht op privacy en het recht op bescherming van persoonsgegevens

53. **TERUGBLIK.** Elk document of artikel dat in het kader van dit eerste deel, handelend over artificiële intelligentie, werd bestudeerd maakt op een bepaald moment melding van de risico's ervan. AI heeft naast haar – op dit moment nog niet limitatief vast te stellen – voordelen namelijk bijna even veel struikelblokken. Waarvan niet het minste voor het recht op privacy en het recht op bescherming van persoonsgegevens dat meestal in éénzelfde adem wordt uitgesproken. Het onderscheid zal in het volgende deel van deze scriptie in detail worden uit de doeken gedaan maar op dit moment bestaat er geen enkele twijfel meer over het feit dat de ongerustheden terecht zijn: AI heeft veel risico's die goed doordachte regelgeving vereisen en de opsomming van de risico's voor grondrechten eindigt steevast met een meer *in concreto* beschrijving van problemen aangaande de bescherming van persoonsgegevens.

54. **DE CONCRETE RISICO'S.** De verschillende besproken teksten identificeren als belangrijkste problemen voor het recht op privacy de volgende:

- Het risico op de-anonimiseren;
- Het risico op real-time monitoring d.m.v. biometrische gegevens;
- Het risico op geautomatiseerde beslissingen op basis van persoonsgegevens; en
- Het risico op discriminatie op basis van bijzondere categorieën van persoonsgegevens;[131]

1.2.6. Tussentijdse terugblik[132]

55. **TERUGBLIK.** In de twee voorgaande hoofdstukken werden het begrip "artificiële intelligentie" en enkele voor- en nadelen van deze technologie besproken. Deze hoofdstukken boden daarmee dus een antwoord op de subonderzoeksvragen: "Wat is AI?" en "Welke zijn haar meest schadelijke en voordelige toepassingen?".

Wat betreft definiëring kan heel kort worden gezegd dat artificiële intelligentie door het voorstel van AI-verordening – ondanks een zekere moeilijkheid hieromtrent – een juridische definitie krijgt in artikel 3(1).
Met betrekking tot de voor- en nadelen is het belangrijk te onthouden dat de Commissie bij de afweging

[131] Zie artikel 9 GDPR.
[132] Omdat het onmogelijk is om alle informatie die te vinden is over de voor- en nadelen en hoe deze op een verantwoorde manier tegenover elkaar afgewogen zouden moeten worden om tot "goede" regelgeving te komen, is het aangewezen naar enkele niet-besproken bronnen te verwijzen die dieper ingaan op de onderwerpen die in de voorgaande delen werden besproken. Deze hebben geen noemenswaardige rechtstreekse invloed gehad op deze scriptie.
- F. DOSHI-VELEZ, et all, "Accountability of AI Under the Law: The Role of Explanation", onuitgegeven, via https://papers.ssrn.com//sol3/Papers.cfm?abstract_id=3064761;
- J.A. KROLL, S. BAROCAS, E.W. FELTEN, J.R. REIDENBERG, D.G. ROBINSON, & H. YU, *Accountable Algorithms*, Princeton University, ProQuest Dissertation Publishing, Doctoraatsthesis met betrekking tot Computerwetenschappen, ISBN:1-339-15703-9, 978-1-339-15703-0;
- S. WACHTER, B. MITTELSTADT, & L. FLORIDI, "Transparent, Explainable, and Accountable AI for Robotics", *SCIENCE ROBOTICS* (vol. 2, issue 6) 31 mei 2017, available at DOI: 10.1126/scirobotics.aan6080;
- B. GOODMAN & S. FLAXMAN, "EU Regulations on Algorithmic Decision-Making and a 'Right to Explanation'", *AI MAGAZI*NE (vol.38, no. 3) oktober 2017, https://doi.org/10.1609/aimag.v38i3.2741; …

van de immense voordelen tegenover de potentieel zeer verregaande nadelen niet over één nacht ijs is gegaan. De voorbereidende werken dateren jaren terug en alle betrokken partijen werden gehoord of werd ten minste de kans gegeven gehoord te worden.

De belangrijkste nadelen in het relevante gebied voor deze scriptie zijn: het risico op de-anonimiseren, real time monitoring, het nemen van geautomatiseerde beslissingen en het risico op discriminatie op basis van persoonsgegevens. Dit zijn dus ook de nadelen die doorheen de verdere hoofdstukken in het achterhoofd gehouden moeten worden.

Met betrekking tot de definiëring zullen in Deel III de in hoofdstuk 1 aangehaalde bedenkingen verder worden uitgewerkt. Ook zullen de belangrijkste risico's terugkomen om kort af te toetsen of de voorgestelde verordening hieraan tegemoet komt.

1.3. Hoofdstuk 3. De krachtlijnen van het voorstel van AI-Verordening

56. CONTEXT VAN HET VOORSTEL.[133] Uit de toelichting bij het voorstel komt zeer duidelijk het enthousiasme en optimisme naar voren dat onlosmakelijk gepaard gaat met de snelle technologische vooruitgang die in het veld van AI wordt geboekt. Deze positieve zienswijze is niet zomaar een roze bril, maar het gevolg van een onderbouwde visie op de voor- en nadelen. Het voorstel van AI-verordening is het resultaat van jaren voorbereidend werk waarin men getracht heeft om aan één van de grootste uitdagingen van ons tijdperk tegemoet te komen.

AI is een familie van technologieën wiens snelle evolutie niet te stoppen is. Ze biedt op bijna alle vlakken van de samenleving een waaier aan nieuwe opportuniteiten. Voor de Europese Unie was het dus ook van groot belang om in het kader van haar technologische machtspositie op het wereldtoneel, een onuitwisbare stempel te drukken op hoe deze technologie in de toekomst zal worden ontwikkeld en toegepast. De titel van het Witboek spreekt voor zich: "*Een Europese benadering op basis van excellentie en vertrouwen"*. Het is de *ratio* van deze wetgeving om een kader te voorzien waarin het potentieel van AI ten volle wordt benut, zonder dat het volk het gevoel heeft in de kou gelaten te worden. Dit kader moet daarom de Europese fundamentele rechten, normen en waarden respecteren. Bovendien is het belangrijk op te merken dat AI die in de EU werkzaam is, ten alle tijde moet dienen ter bevordering van de mensheid. Het moet mensgericht zijn en blijven, zodat het vertrouwen in deze technologie kan groeien en ze omarmd kan worden.

Om tegemoet te komen aan de zorgen van burgers en ondernemingen met betrekking tot artificiële intelligentie heeft de Europese Commissie ervoor geopteerd om op basis van haar bevoegdheid onder artikel 114 VWEU[134] een harmonisatie van AI-wetgeving te verzekeren in de gehele EU door middel van een verordening. De eerste initiatieven tot (vrijwillig) reguleren doken namelijk al op in enkele lidstaten terwijl een fragmentering van wetgeving over dit onderwerp niet wenselijk zou zijn.[135] Als tweede

---

[133] 1.1. Motivering en doel van het voorstel, in de Toelichting bij het voorstel van AI-verordening.

[134] **Artikel 114 (1)VWEU.** *Tenzij in de Verdragen anders is bepaald, zijn de volgende bepalingen van toepassing voor de verwezenlijking van de doeleinden van artikel 26. Het Europees Parlement en de Raad stellen volgens de gewone wetgevingsprocedure en na raadpleging van het Economisch en Sociaal Comité de maatregelen vast inzake de onderlinge aanpassing van de wettelijke en bestuursrechtelijke bepalingen van de lidstaten die de instelling en de werking van de interne markt betreffen. 2. Lid 1 is niet van toepassing op de fiscale bepalingen, op de bepalingen inzake het vrije verkeer van personen en op de bepalingen inzake de rechten en belangen van werknemers. 3. De Commissie zal bij haar in lid 1 bedoelde voorstellen op het gebied van de volksgezondheid, de veiligheid, de milieubescherming en de consumentenbescherming uitgaan van een hoog beschermingsniveau, daarbij in het bijzonder rekening houdend met alle nieuwe ontwikkelingen die op wetenschappelijke gegevens zijn gebaseerd. Ook het Europees Parlement en de Raad zullen binnen hun respectieve bevoegdheden deze doelstelling trachten te verwezenlijken. 4. Wanneer een lidstaat het, nadat door het Europees Parlement en de Raad, door de Raad of door de Commissie een harmonisatiemaatregel is genomen, noodzakelijk acht nationale bepalingen te handhaven die hun rechtvaardiging vinden in gewichtige eisen als bedoeld in artikel 36 of verband houdend met de bescherming van het milieu of het arbeidsmilieu, geeft hij zowel van die bepalingen als van de redenen voor het handhaven ervan, kennis aan de Commissie. 5. Wanneer een lidstaat het, nadat door het Europees Parlement en de Raad, door de Raad of door de Commissie een harmonisatiemaatregel is genomen, noodzakelijk acht, nationale bepalingen te treffen die gebaseerd zijn op nieuwe wetenschappelijke gegevens die verband houden met de bescherming van het milieu of het arbeidsmilieu vanwege een specifiek probleem dat zich in die lidstaat heeft aangediend nadat de harmonisatiemaatregel is genomen, stelt hij de Commissie voorts, onverminderd lid 4, in kennis van de voorgenomen bepalingen en de redenen voor het vaststellen ervan*.

[135] A. JOBIN, M. LENCA & E. VAYENA, "The global landscape of AI ethics guidelines", *Nature Machine Intelligence* 2 september 2019, p. 389-399, https://www.nature.com/articles/s42256-019-0088-2; & 1.1. Motivering en doel van het voorstel, laatste doelstelling genoemd in alinea 5, in de Toelichting bij het voorstel van AI-verordening; Zie infra: Randnummer 57 – 4 pijlers.

belangrijke rechtsgrond wordt artikel 16 VWEU[136] aangehaald, dat later in deze scriptie[137] nog zal worden aangehaald aangezien het handelt over de bescherming van persoonsgegevens.

57. **4 PIJLERS.** Het voorstel van AI-verordening is gebaseerd op vier specifieke pijlers:

1. "*Ervoor zorgen dat AI-systemen die in de Unie in de handel worden gebracht en gebruikt, veilig zijn en de bestaande wetgeving inzake* ***grondrechten en waarden van de Unie eerbiedigen****;*
2. ***Rechtszekerheid garanderen*** *om investeringen en innovatie in AI te vergemakkelijken en aan te moedigen;*
3. *Het* ***beheer en de doeltreffende handhaving van de bestaande wetgeving*** *inzake grondrechten en veiligheidsvoorschriften die van toepassing zijn op AI-systemen, verbeteren;*
4. *De ontwikkeling van een* ***eengemaakte markt voor wettige, veilige en betrouwbare AI-toepassingen*** *vergemakkelijken en marktversnippering voorkomen*."[138]

58. **VEILIGHEID EN FUNDAMENTELE RECHTEN.** Enkele van de belangrijkste bedenkingen van belanghebbende partijen hadden te maken met wantrouwen in het correct en veilig gebruik van AI met respect voor de fundamentele rechten van de mens. Deze angsten zijn zeer goed te verstaan aangezien bijna elke vermelding van AI in het nieuws, op het internet of in films een wrange nasmaak achterlaat. Zo gaat het bijna altijd om slimme camera's die Orwelliaanse scenario's mogelijk maken, robots die arbeidsintensieve jobs innemen of supercomputers die wereldoverheersing nastreven. Wie tot hier heeft gelezen weet ondertussen dat er regelmatig te veel nadruk gelegd wordt op de gevaren en dat de voordelen ruimschoots opwegen tegen de nadelen, op voorwaarde dat de nadelen uiteraard niet zomaar worden genegeerd. Deze boodschap moet het brede publiek echter ook kunnen bereiken. Daartoe kan een duidelijk wetgevend kader, dat de belangen van de potentieel gedupeerden beschermt, natuurlijk bijdragen.

59. **TOEPASSINGSGEBIED.** Artikel 2(1) van het voorstel maakt dat de toekomstige verordening dient te worden nageleefd door zowel (a) aanbieders die AI in de EU in de handel brengen, (b) gebruikers van AI-toepassingen binnen de Unie en (c) aanbieders en gebruikers van AI die zich in een derde land bevinden, maar waarvan de output in de EU wordt gebruikt.

[136] **Artikel 16(1) VWEU***: Eenieder heeft recht op bescherming van zijn persoonsgegevens. 2. Het Europees Parlement en de Raad stellen volgens de gewone wetgevingsprocedure de voorschriften vast betreffende de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie, alsook door de lidstaten, bij de uitoefening van activiteiten die binnen het toepassingsgebied van het recht van de Unie vallen, alsmede de voorschriften betreffende het vrij verkeer van die gegevens. Op de naleving van deze voorschriften wordt toezicht uitgeoefend door onafhankelijke autoriteiten.*
De op basis van dit artikel vastgestelde voorschriften doen geen afbreuk aan de in artikel 39 van het Verdrag betreffende de Europese Unie bedoelde specifieke voorschriften.
[137] Zie supra: Randnummer 86 – Europese Unie.
[138] 1.1. Motivering en doel van het voorstel, in de Toelichting bij het voorstel van AI-verordening.

Dit zorgt dus voor een breed toepassingsgebied:

Ratione loci strekt het toepassingsgebied zich uiteraard uit over alle lidstaten van de Europese Unie. Elke AI die binnen de EU in gebruik wordt gesteld of waarvan de output hier uitwerking krijgt[139], moet voldoen aan de regels die in de artikelen 9 tot 14 van het voorstel worden uiteengezet.

Ratione personae spreken we over zowel **aanbieders** als **gebruikers[140]** van AI die zich binnen de EU bevinden of waarvan de output van hun AI haar invloed doet gelden binnen de EU.[141]

Ratione materiae is het voorstel – niet zo verbazingwekkend – van toepassing op artificiële-intelligentiesystemen.[142]

60. **RECHTSZEKERHEID.** Een belangrijke vraag vanuit de praktijk was om zekerheid te scheppen omtrent de terminologie en om een duidelijk kader op te stellen zodat in ieder geval binnen de EU het investeringsmilieu optimaal wordt gehouden om de technologische vooruitgang niet in het gedrang te brengen.

Als belangrijkste term was het uiteraard noodzakelijk om "artificiële intelligentie" te definiëren.[143] Hiernaast stelde het werkveld zich ook vragen bij wat precies als risicovol zou worden gezien, hoe dit moest worden beoordeeld en wat er bedoeld werd met "biometrische identificatie op afstand" en "schade". Op al deze vragen en meer wordt een antwoord gegeven in respectievelijk artikel 3, dat een lijst van definities geeft die relevant zijn voor het voorstel, en in de artikelen 5 en 6, dat aangeeft hoe het risicogehalte moet worden geëvalueerd.

[139] En die ook nog wordt bestempeld als hoog-risico onder artikel 6 van het voorstel van AI-verordening.
[140] Zie artikel 3(2) voorstel van AI-verordening. & Zie artikel 3(4) Voorstel van AI-verordening.
[141] Hierbij kan men zich de vraag stellen of dit in de huidige, geglobaliseerde samenleving niet *de facto* gewoon alle AI is die er nu bestaat en ooit zal bestaan. In de hypothese waarin een Amerikaans bedrijf een in de USA geplaatste AI laat werken en de output – die overigens ook nog eens uit een Amerikaanse computer rolt – zijn weg toevallig vindt naar een verkoper in Italië, die ermee zijn bedrijfsvoering denkt te optimaliseren, … in deze – mijns inziens – niet overdreven vergezochte hypothese, zal zowel de Amerikaanse aanbieder van de AI in kwestie, alsook de Amerikaanse gebruiker zich aan de EU AI-verordening moeten houden, of zich zodanig indekken dat de output van zijn AI sowieso nooit de EU bereikt.
[142] Zie artikel 3(1) voorstel van AI-verordening; & Zie supra: Randnummers 12 – Juridische definitie.
[143] Dit werd eerder in deze tekst reeds uitvoerig besproken. Zie hiervoor supra: Randnummers 10-17.

1. **Art. 3*(36): ""biometrisch systeem voor de identificatie op afstand":*** *een AI-systeem dat is bedoeld voor het identificeren van natuurlijke personen op afstand door middel van de vergelijking van de biometrische gegevens van een persoon met de biometrische gegevens die zijn opgenomen in een referentiedatabank en zonder dat de gebruiker van het AI-systeem vooraf weet of de persoon hierin is opgenomen en kan worden geïdentificeerd;"*[144]
2. **Art. 3(44): ""*ernstig incident":*** *elk incident dat direct of indirect leidt, kan hebben geleid of kan leiden tot:(a)het overlijden van een persoon of ernstige schade voor de gezondheid van een persoon, eigendom of het milieu;(b)een ernstige en onomkeerbare verstoring van het beheer en de exploitatie van kritieke infrastructuur."*
3. **Risico** wordt volgens de regels van artikels 5 en 6 beoordeeld hetgeen in onderstaande tabellen zal worden verduidelijkt.

61. **RISICOGEBASEERDE AANPAK.** Het voorstel draagt de veilige implementering van AI in de Europese lidstaten hoog in het vaandel en stelt daarom in artikel 5 vast dat er toepassingen zijn die gewoonweg niet door de beugel kunnen. Deze zouden namelijk een gevaar kunnen vormen voor de fysieke of psychologische gezondheid van burgers of een onevenredige inbreuk op hun recht op privacy zijn. Artikel 6 en Bijlage III bevatten daarenboven de criteria aan de hand waarvan een hoog risico systeem kan worden geïdentificeerd en welke systemen sowieso onder deze noemer zullen vallen.

De systemen die door bijlage III worden benoemd hebben allen betrekking tot fundamentele rechten.[145] Het gevolg hiervan is echter dat enkele andere vrijheden de afweging hebben verloren en dus in deze verhouding ondergeschikt worden geacht aan de bovenstaande. Hierbij gaat het voornamelijk om de vrijheid van kunsten en wetenschappen, de vrijheid van ondernemerschap en het recht op intellectuele eigendom.[146]

[144] Een interessante aanvulling hierop volgt direct in de volgende twee leden door een uitbreiding voor de identificatie op afstand in **real time** en **achteraf**: (37)"*biometrisch systeem voor de identificatie op afstand in real time": een biometrisch systeem voor de identificatie op afstand waarbij het vastleggen van biometrische gegevens, de vergelijking en de identificatie plaatsvinden zonder aanzienlijke vertraging. Dit omvat niet alleen de onmiddellijke identificatie, maar ook beperkte korte vertragingen om omzeiling te voorkomen*; & (38)"*biometrisch systeem voor de identificatie op afstand achteraf": een ander biometrisch systeem voor de identificatie op afstand dan een biometrisch systeem voor de identificatie op afstand in real time.*

[145] Denk hierbij voornamelijk aan het recht op menselijke waardigheid, eerbiediging van het privéleven en bescherming van persoonsgegevens, vrijheid van meningsuiting, vrijheid van vergadering en vereniging, non discriminatie, …

[146] De toelichting bij het voorstel tot AI-verordening noemt als gelimiteerde grondrechten de artikelen 13, 16 en 17(2) van het Handvest van de Grondrechten van de Europese Unie. → 3.5. fundamentele rechten, in de Toelichting bij het voorstel van AI-verordening.

Risicogebaseerde aanpak	
Verboden artificiële intelligentie-systemen	Deze systemen vormen een onaanvaardbaar risico doordat hun toepassing in strijd is met de waarden van de EU. Titel II van het voorstel tot AI-verordening benoemt deze systemen.
Hoog risico artificiële intelligentie-systemen	De hoofdmoot van het voorstel tot AI-verordening gaat over AI-systemen die een hoog risico vormen voor de gezondheid, veiligheid of fundamentele rechten van natuurlijke personen. Deze systemen zijn toegelaten, als en slechts als deze voldoen aan de dwingende voorschriften onder Titel III van het voorstel. Bijlage III bij het voorstel bevat een lijst van toepassingen die geacht worden een hoog risico te vormen.
Laag of minimaal risico artificiële intelligentie-systemen	Alle AI-systemen die niet onder één van de vorige categorieën vallen, zijn in theorie dus vrij te implementeren en te ontwikkelen in de EU. Overeenkomstig Titel IX zal het door de Commissie en de lidstaten wel sterk aangemoedigd worden om op vrijwillige basis gedragscodes aan te nemen en zo *de facto* de voorschriften van het voorstel na te leven.

Figuur 7. Risicogebaseerde aanpak in het voorstel van AI-verordening

<table>
<tr><th colspan="6"><u>Risicobeoordeling in het voorstel van AI-verordening</u></th></tr>
<tr><td rowspan="9">Artikel 5 (1) voorstel AI-verordening</td><td colspan="5">Verboden AI-toepassingen zijn van zodanig hoog risico / strijdig met EU-normen en waarden dat de wetgever simpelweg heeft geoordeeld dat ze niet in de handel mogen worden gebracht, in gebruik worden gesteld of gebruikt worden in de gevallen waarin ze:</td></tr>
<tr><td>(a)</td><td colspan="4">Het gedrag van personen wezenlijk verstoren zodat aan deze of andere personen fysieke of psychologische schade kan worden toegebracht;</td></tr>
<tr><td>(b)</td><td colspan="4">De kwetsbaarheden van een specifieke groep die door hun leeftijd of fysieke of geestelijke handicap bestaan, uitbuiten om hun gedrag te verstoren zodat aan deze of andere personen fysieke of psychologische schade kan worden toegebracht;</td></tr>
<tr><td>(c)</td><td colspan="4">Voor of door overheidsinstanties classificatie- of evaluatiesystemen instellen die natuurlijke personen beoordelen volgens hun bekende of voorspelde gedrag of persoonlijkheidskenmerken en hieraan een sociale score toekennen indien;</td></tr>
<tr><td></td><td colspan="2">(I) Er een nadelige behandeling aan vast hangt buiten de context waarin de data oorspronkelijk werd verzameld;</td><td colspan="2">(II) Er een nadelige behandeling aan vast hangt die ongerechtvaardigd of onevenredig is met hun gedrag of de ernst ervan.</td></tr>
<tr><td colspan="5">Wanneer het gaat om (d) biometrische systemen voor de identificatie op afstand in real time in openbare ruimtes met het oog op rechtshandhaving mag AI niet worden gebruikt tenzij en voor zover het strikt noodzakelijk is voor één van onderstaande doelstellingen:</td></tr>
<tr><td></td><td>(I) Het gericht zoeken naar potentiële slachtoffers;</td><td>(II) Het voorkomen van een specifieke, aanzienlijke en imminente dreiging;</td><td colspan="2">(III) De detectie, opsporing of identificatie van een dader of verdachte van een strafbaar feit dat met minstens drie jaar vrijheidsstraf wordt bestraft.</td></tr>
<tr><td rowspan="3">Artikel 6 voorstel AI-verordening</td><td>(1)</td><td colspan="4">Om te bepalen of een AI-systeem een hoog risico vormt, moeten twee voorwaarden cumulatief worden voldaan:</td></tr>
<tr><td></td><td colspan="2">(a) Het systeem in kwestie is bedoeld om te worden gebruikt als veiligheidscomponent van een product of is zelf een product dat onder de regelgevingen in bijlage II valt;</td><td colspan="2">(b) Er moet een conformiteitsbeoordeling worden uitgevoerd door een onafhankelijke derde met het oog op het in de handel brengen of gebruiken van het product dat onder de regelgevingen in bijlage II valt.</td></tr>
<tr><td>(2)</td><td colspan="4">Als het AI-systeem onder één van de beschrijvingen uit bijlage III valt, is het sowieso ook een hoog risico systeem.</td></tr>
</table>

Figuur 8. Risicobeoordeling in het voorstel van AI-verordening

62. BESTAANDE WETGEVING HANDHAVEN.

"Vanwege het horizontale karakter moet het voorstel volledig verenigbaar zijn met de bestaande uniewetgeving die van toepassing is op sectoren waar reeds gebruik wordt gemaakt of in de nabije toekomst waarschijnlijk gebruik zal worden gemaakt van AI systemen met een hoog risico."[147]

Met deze woorden schetst de toelichting bij het voorstel van AI-verordening duidelijk hoe het voorstel zich verhoudt tot alle andere EU-wetgeving.

Concreet wil dit dus zeggen dat de wetgever de bedoeling heeft om de toekomstige verordening verenigbaar te maken met onder andere het Handvest van de Grondrechten van de Europese Unie[148], de Richtlijn Gegevensbescherming Politie en Justitie (Rechtshandhavingsrichtlijn)[149] en de Algemene Verordening Gegevensbescherming[150], …

Met betrekking tot de GDPR is het belangrijk een opmerking te maken over de verhouding tot het Voorstel.[151] Het is namelijk zo dat de EU-wetgever de toekomstige AI-verordening ziet als *lex specialis* ten aanzien van GDPR, door in het licht van deze regelgevingen ook te voorzien in specifieke, geharmoniseerde regels die beogen de hele levenscyclus van AI-systemen, van design tot gebruik, te regelen.

63. INTERNE MARKT. Zoals eerder reeds werd aangehaald[152] is het volgens de EU-wetgever van groot belang om te voorzien in geharmoniseerde regelgeving voor alle EU-lidstaten teneinde niet met een gefragmenteerd AI-landschap geconfronteerd te worden. Het is namelijk logisch dat de Unie als eenheid, met al haar lidstaten een pak sterker staat om met haar normen en waarden de toekomst van AI-ontwikkeling te beïnvloeden dan als België dit bijvoorbeeld alleen zou proberen te verwezenlijken.

Net zoals de verwerkingsverantwoordelijken en verwerkers van persoonsgegevens onder het GDPR-regime zich in alle landen te houden hebben aan de EU-regels wanneer ze de gegevens van EU-burgers verwerken[153], zullen aanbieders en gebruikers van AI-toepassingen zich moeten schikken naar deze toekomstige verordening als ze hun product op deze markt willen aanbieden of gebruiken.

---

[147] 1.2. Verenigbaarheid met bestaande bepalingen op beleidsterrein, in de Toelichting bij het voorstel van AI-verordening.
[148] Handvest van de Grondrechten van de Europese Unie, van 14 december 2007, (2007/C 303/01). (https://eur-lex.europa.eu/eli/treaty/char_2007/oj).
[149] Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.
[150] 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.
[151] "*Het voorstel doet geen afbreuk aan en vormt een aanvulling op de algemene verordening gegevensbescherming (Verordening (EU) 2016/679) en de Richtlijn rechtshandhaving (Richtlijn (EU) 2016/680) met een reeks geharmoniseerde regels die van toepassing zijn op het ontwerp, de ontwikkeling en het gebruik van bepaalde AI-systemen met een hoog risico, en beperkingen op bepaalde toepassingen van biometrische systemen voor identificatie op afstand.*" → 1.2. Verenigbaarheid met bestaande bepalingen op beleidsterrein, in de Toelichting bij het voorstel van AI-verordening.
[152] Zie supra: Randnummers 56 – Context van het Voorstel & 57 – 4 pijlers.
[153] Zie artikels 2 en 3 GDPR.

Wetend dat AI een product is waarvan haar finale vorm nog lang niet in zicht is, kan een regelgeving zoals diegene die nu wordt besproken, wereldwijd richtinggevend werken omdat de EU nu eenmaal een grote, belangrijke afzetmarkt is.

64. **"*REGULATORY SANDBOXES*".**[154] Om innovatie te ondersteunen en aan te moedigen en toch tegelijkertijd een maximale bescherming te bieden aan EU-burgers heeft de EU-wetgever ervoor geopteerd om een systeem op poten te zetten dat het mogelijk maakt voor de nationale of overkoepelend bevoegde autoriteiten om testomgevingen voor regelgeving op te zetten. Binnen deze in tijd en ruimte beperkte proefomstandigheden krijgen de ontwikkelaars van innovatieve technologieën de kans om hun AI-systeem te laten werken onder het toeziend oog van de autoriteit in kwestie.

Onder Titel V worden specifieke maatregelen voor KMO's, zowel aan de gebruikers- als de aanbiederszijde voorzien om hen ook de mogelijkheid te bieden conformiteitscontroles te laten uitvoeren. Ook met betrekking tot de verwerking van persoonsgegevens zijn er specifieke bepalingen van toepassing wanneer de verwerking in kwestie plaatsvindt in het kader van een AI-testomgeving. Deze bepalingen zullen later uitvoerig worden besproken.[155]

65. **TRANSPARANTIEVERPLICHTING & "HUMAN OVERSIGHT".** Om vorm te geven aan de "benadering op basis van excellentie en vertrouwen" implementeert het Voorstel in artikel 13 de verplichting om gebruikers van AI te informeren over het systeem in kwestie, zodat ze het op passende wijze kunnen gebruiken en interpreteren. Hiertoe moet een gebruiksaanwijzing worden opgesteld.[156]

Artikel 14 waarborgt de mogelijkheid om op een effectieve manier menselijk toezicht te kunnen houden op de werking van een AI-systeem.

66. **EX-ANTE RISICOBEOORDELING & EX-POST HANDHAVINGSMAATREGELEN.** De risicobeoordeling moet gebeuren voordat het AI-systeem in kwestie in werking wordt gebracht. Hiertoe gelden er verschillende verplichtingen met betrekking tot mededeling, conformiteitsvereisten, aanmelding bij de bevoegde autoriteit, certificering, …[157] die voldaan moeten zijn alvorens een hoog-risicosysteem mag worden geïmplementeerd in de EU. De hiertoe opgerichte of aangeduide nationale autoriteit[158] zal hierop toezien en zal in haar taak ook worden bijgestaan door het Europees Comité voor Artificiële Intelligentie[159] dat onder andere hiervoor speciaal zal worden opgericht.

Ook nadat een hoog risico AI-systeem werd losgelaten op de Europese interne markt, is er nog een mogelijkheid voorzien om eventuele problemen hieromtrent aan te pakken. Hiervoor wordt voornamelijk

[154] 1.2. Verenigbaarheid met bestaande bepalingen op beleidsterrein, in de Toelichting bij het voorstel van AI-verordening → Artikelen 53 – 55 voorstel AI-verordening (Titel V)
[155] Zie infra: Randnummer 70 – Artikelen 53 & 54 – Maatregelen ter ondersteuning van innovatie.
[156] Zie artikel 13(2) van het voorstel van AI-verordening.
[157] Zie artikelen 16-52 van het voorstel AI-verordening. → Niet al deze artikelen bevatten specifieke verplichtingen voor de aangewezen verantwoordelijken onder het toekomstig regime van het voorstel.
[158] Zie artikel 30 juncto 59 van het voorstel van AI-verordening.
[159] Zie artikel 56 - 58 van het voorstel van AI-verordening.

gekeken naar de mogelijkheid om administratieve monsterboetes op te leggen zoals we deze ook onder het GDPR-regime kennen.[160]

[160] Zie artikel 71 van het voorstel AI-verordening; maakt het mogelijk om administratieve geldboeten op te leggen tot (3) 30.000.000 euro of 6% van de totale wereldwijde jaaromzet van het voorafgaande boekjaar, (4) 20.000.000 euro of 4% van de totale wereldwijde jaaromzet van het voorafgaande boekjaar of (5) tot 10.000.000 euro of 2% van de totale wereldwijde jaaromzet van het voorafgaande boekjaar, al naargelang wat de aard van de inbreuk precies is.

1.4. Hoofdstuk 4. Relevante bepalingen met betrekking tot privacy en de bescherming van persoonsgegevens

67. INLEIDING & OVERZICHT. Hoewel alle voorschriften voor AI-systemen, verplichtingen voor distributeurs, importeurs, gebruikers en eventuele derden, de verplichtingen omtrent aanmelding, de regels met betrekking tot certificering en beboeting, en alle andere aspecten van het voorstel van AI-verordening uitermate belangrijk zijn om tot het samenhangende geheel te komen dat het kern van het Europees AI-kader zal vormen, is het voor deze scriptie niet opportuun om ze allemaal even gedetailleerd te bespreken. Dit hoofdstuk zal een antwoord bieden op de subonderzoeksvraag die peilt naar de relevante bepalingen in het voorstel met betrekking tot privacy en bijgevolg ook op het recht op bescherming van persoonsgegevens dat er *in casu* toe doet.

Een snelle lezing van het Voorstel trekt de aandacht voornamelijk naar de artikelen 3(29) – (38); 5; 6; 53 en 54, en de samen met hen te lezen overwegingen.[161] Hoewel dit niet de enige bepalingen zijn die een zekere impact zullen hebben op de verwerking van persoonsgegevens, of de handhaving van de toekomstige Verordening met betrekking tot die verwerkingen, zullen de andere niet of slechts kort worden aangehaald.

68. ARTIKEL 3 - DEFINITIES. Dit artikel bevat alle definities die van toepassing zijn op het voorstel van AI-verordening. Naast de definiëring van "AI-systeem" en alle mogelijke hoedanigheden van personen en instellingen waarop de Verordening van toepassing zal zijn en die zullen instaan voor de naleving ervan, worden in de punten 29 tot 38 ook enkele termen verduidelijkt die betrekking hebben op de verschillende soorten data naargelang het moment waarop ze worden gebruikt, waar ze vandaan komen of waarvoor ze moeten dienen.

[161] Naast de artikelen en overwegingen die in de volgende randnummers besproken zullen worden, zijn er ook nog enkele andere bepalingen die een zekere, doch minder verregaande invloed zullen hebben op de verwerking van persoonsgegevens ten behoeve van, of door AI: *Artikel 10*, dat samen gelezen moet worden met *overweging 44*, gaande over de kwaliteitscriteria waaraan trainings-, validatie- en testdata moeten voldoen; *Artikel 29(6),* over de verplichting van de gebruiker van een hoog-risico AI om een gegevensbeschermingseffectenbeoordeling ("*Data Protection Impact Assessment*" = DPIA) overeenkomstig artikel 35 GDPR of artikel 27 Rechtshandhavingsrichtlijn uit te voeren; *Artikel 60*, dat gaat over een EU-databank waarin alle hoog-risico autonome AI-systemen worden opgenomen en dat overeenkomstig (4) enkel persoonsgegevens mag bevatten in zoverre die noodzakelijk zijn; …

Definities in artikel 3 (29) tot (38) van het voorstel van AI-verordening.			
Artikel 3 …	**Tijdstip**		
(29)	"**Trainingsdata**": Trainingsdata is data die voor het op de markt brengen van het AI-systeem wordt gebruikt om het te trainen met alle leerbare parameters.		
(30)	"**Validatiedata**": Deze data zal in de fase die volgt op de training, worden gebruikt om te testen of het getrainde systeem naar behoren werkt en om de niet-leerbare parameters en het leerproces daarvan af te stellen.		
(31)	"**Testdata**": Als laatste controle voordat een systeem op de markt wordt gebracht, wordt het getest met testdata om te controleren of de AI de verwachte prestaties levert.		
(32)	"**Inputdata**": Na implementatie werkt AI nog steeds op data, maar nu niet meer in een gecontroleerde omgeving.[162] Dit is de data die een gebruiker aan zijn kersvers gekochte AI zal voeden en die zal zorgen voor een output.		
		Soort gegevens	
(33)	"**Biometrische gegevens**": zijn persoonsgegevens die betrekking hebben tot de fysieke, fysiologisch of gedragsgerelateerde kenmerken van natuurlijke personen op basis waarvan identificatie mogelijk is. Overweging 7 stelt dat dit begrip dezelfde invulling dient te krijgen als onder artikel 4, 14e lid GDPR.[163]		
			Doeleinde
(34)	"**Systeem voor herkennen van emoties**": Dit soort AI heeft als doel om op basis van biometrische gegevens de emoties of intenties van natuurlijke personen vast te stellen of af te leiden.		
(35)	"**Systeem voor biometrische categorisering**": AI die onder deze noemer valt, is bedoeld om natuurlijke personen in te delen in specifieke categorieën op basis van hun biometrische gegevens.[164]		
(36)	"**Biometrisch systeem voor de identificatie op afstand**": Dit soort systeem heeft als doel het mogelijk te maken om natuurlijke personen, op afstand, door middel van vergelijking van hun biometrische gegevens met een referentiedatabank, te identificeren. Het is hiertoe niet vereist dat de gebruiker van de AI op voorhand weet of de persoon in kwestie in de databank is opgenomen.[165]		
(37)	"**Biometrisch systeem voor de identificatie op afstand in real time**": Wanneer het identificeren op afstand, door middel van biometrische gegevens, plaatsvindt zonder een aanzienlijke vertraging. Dit wil dus ook zeggen dat een vertraging van enkele minuten, bedoeld om beperkende bepalingen te omzeilen, nog steeds onder deze noemer zal vallen.		
(38)	"**Biometrisch systeem voor de identificatie op afstand achteraf**": Elk systeem voor identificatie op afstand op basis van biometrische gegevens dat niet onder de voornoemde definitie valt, en dus pas na een aanzienlijke termijn plaatsvindt, zal onder deze noemer vallen.		

Figuur 9. Definities in artikel 3(29) tot (38) van het voorstel van AI-verordening.

[162] De inputdata zal uiteraard sterk lijken op alle vroegere soorten data omdat de huidige AI-toepassingen nu eenmaal relatief gelimiteerde capaciteiten hebben. Denk aan het systeem dat werd getraind om katten te herkennen. Deze AI zal kunnen zeggen welke afbeeldingen katten zijn, en welke niet onder die noemer kunnen worden geplaatst. Hetzelfde systeem moet je geen beelden van bloemen gaan geven als input want daar kan het systeem natuurlijk niets zinnig mee.

[163] Hierop wordt later concreter nog ingegaan. Zie infra: Randnummers 93 – Biometrische persoonsgegevens & 109 - artikel 4(13), (14) & (15) – Gevoelige persoonsgegevens.

[164] Artikel 3(35) geeft als voorbeelden van categorieën: geslacht, leeftijd, haarkleur, oogkleur, etnische afkomst, seksuele gerichtheid of politieke overtuiging. Het is niet ondenkbaar dat dit soort systemen, indien ze misbruikt worden, zeer zware gevolgen zouden kunnen hebben. Daarom worden ze ook zeer sterk gelimiteerd een verbod in sommige gevallen ten gevolge van artikel 5(1)(b) en (c). Beide hierin verboden toepassingen vereisen namelijk voorafgaand een zekere hoeveelheid categorisering en profilering. (zie hiervoor ook "*profilering*" onder artikel 4(4) GDPR en zie infra: Randnummer 100 – Profilering.) De gevallen die niet verboden zouden worden door artikel 5, vallen per definitie onder artikel 6(2), verwijzend naar Bijlage III, (1).

[165] Artikel 6(2), verwijzend naar Bijlage III, (1)(a) stelt dat al deze systemen per definitie een hoog risico vormen. Voor enkele specifieke gevallen worden ze ook verboden door artikel 5(1)(d) – *in concreto* dus wanneer een politionele dienst in real time, in de openbare ruimte met het oog op de rechtshandhaving een dergelijk biometrisch systeem voor identificatie op afstand gebruikt. – mits enkele uitzonderingen die verder in het artikel worden uiteengezet.

69. ARTIKELEN 5 EN 6 – VERBOD EN HOOG RISICO. De risicogebaseerde aanpak van het Voorstel werd onder randnummer 61 reeds uitvoering uit de doeken gedaan en moet dus niet meer worden herhaald. Wat wel nog kort even dient vermeld te worden, is dat artikel 5 samen gelezen dient te worden met overwegingen 15 tot 26. En dat artikel 6 steunt op de verklaringen in de overwegingen 27 tot 40.

De overwegingen bij artikel 5 verklaren waarom de Commissie ervoor heeft gekozen om bepaalde toepassingen te verbieden en stelt dat de verwerking van biometrische gegevens door AI-systemen bedoeld voor identificatie op afstand in real time van natuurlijke personen in openbare ruimten met het oog op de rechtshandhaving, onderhavig is aan de regels van de Rechtshandhavingsrichtlijn.[166] De verwerking van biometrische en andere persoonsgegevens onder dezelfde voorwaarden en door eenzelfde systeem, maar niet met het oog op rechtshandhaving, moet blijven voldoen aan de vereisten van onder andere artikel 9, 1e lid GDPR.

Wat betreft de hoog-risico AI-toepassingen is naast de verklaringen voor alle specifiek benoemde systemen in Bijlage III, ook belangrijk op te merken dat overweging 41 (net zoals overweging 23) stelt dat deze artikelen van de toekomstige Verordening op geen enkele manier mogen worden uitgelegd als zijnde een rechtsgrondslag voor de verwerking van persoonsgegevens.

70. ARTIKELEN 53 & 54 – MAATREGELEN TER ONDERSTEUNING VAN INNOVATIE. Met betrekking tot de reeds eerder genoemde[167] AI-testomgevingen voor regelgeving zijn er enkele specifieke regels opgenomen met betrekking tot de verwerking van persoonsgegevens. Deze worden hier kort besproken omdat deze in een later stadium vergeleken dienen te worden met de normale regelgeving onder de GDPR.[168]

Wanneer het gaat om innovatieve AI-systemen die betrekking hebben op de verwerking van persoonsgegevens, is het verplicht ervoor te zorgen dat de gegevensbeschermingsautoriteiten van de betrokken lidstaten betrokken worden. → artikel 53(2).

Onder artikel 54 wordt een verdere verwerking van persoonsgegevens toegestaan voor zover die in het algemene belang van de AI-testomgeving zou zijn. Dat wil zeggen dat persoonsgegevens die rechtmatig voor andere doeleinden werden verzameld, ook verwerkt mogen worden ten behoeve van het ontwikkelen en testen van bepaalde AI-systemen binnen de testomgeving. Dit artikel voegt dus *de facto* een extra verwerkingsgrond in[169], zoals ook wordt duidelijk gemaakt door overweging 72 van het Voorstel.

---

[166] Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.
[167] Zie supra: Randnummer 64 – "Regulatory Sandboxes"
[168] Zie infra: Randnummers 102 tot en met 106 → 2.3. Hoofdstuk 3: De krachtlijnen van de GDPR.
[169] Op basis van artikel 6(4) GDPR. Zie infra: Randnummer 104 – Rechtmatigheid van de verwerking.

1.5. Overzicht deel 1

71. AI EN VOORSTEL VAN AI-VERORDENING IN EEN NOTENDOP. In dit eerste deel werd gekeken naar de definiëring van het concept "Artificiële Intelligentie", wat *grosso modo* de inhoud ervan is in de volksmond en hoe de Commissie het omschrijft om te bepalen wanneer er aan het toepassingsgebied *ratione materiae* van de toekomstige AI-verordening is voldaan. Hieromtrent werden enkele opmerkingen kort aangehaald waarop in het laatste deel van deze masterscriptie dieper zal worden ingegaan.

Volgend op de definiëring heeft de auteur getracht om, op een voor leken verstaanbare manier, kort samen te vatten welke generaties, technieken en benaderingen er tot de huidige stand van zaken kunnen worden gerekend in het onderzoeks- en werkveld dat zich bezighoudt met AI. Dit was noodzakelijk om met een zeker begrip te kunnen kijken naar Bijlage I bij het Voorstel.

Na het definiërend en verkennend gedeelte van het begrip en de inhoud van artificiële intelligentie was het tijd om een blik te werpen op welke kansen en risico's er kleven aan deze – relatief – jonge familie van technologieën. Het belangrijkste wat uit dit hoofdstuk moet worden meegenomen is dat er enorme hoeveelheden informatie en desinformatie te vinden zijn met betrekking tot dit onderwerp, maar dat de Europese Commissie zeker niet over één nacht ijs gegaan is wat betreft de afweging van de voor- en nadelen ten opzichte van elkaar. Als belangrijkste nadelen, die zeker ook in het derde deel zullen terugkomen, worden onthouden: (i) het risico op de-anonimiseren, (ii) real time monitoring, (iii) het nemen van geautomatiseerde beslissingen en (iv) het risico op discriminatie op basis van persoonsgegevens.

In het laatste hoofdstuk van dit deel werden de krachtlijnen van het voorstel van AI-verordening uit de doeken gedaan en werden enkele van de meest relevante bepalingen uit dit Voorstel extra in de schijnwerpers gezet omdat deze volgens de auteur de grootste impact zouden kunnen hebben op het recht op de bescherming van persoonsgegevens. Het gaat *in casu* om de bepalingen omtrent de definities van de verschillende soorten data, naargelang de timing, soort gegevens of de doeleinden ervan; de verboden en hoog-risico AI-toepassingen; en de maatregelen ter ondersteuning van innovatie.

2. Deel 2: Bescherming van persoonsgegevens[170]

72. KORTE INLEIDING & GESCHIEDENIS. Na de bespreking van artificiële intelligentie en het voorstel van AI-verordening in het vorige deel, is het nu de beurt aan privacy en bescherming van persoonsgegevens in het kader van de GDPR. Hoewel de officiële Nederlandstalige afgekorte titel van deze verordening leest als: "*Algemene Verordening Gegevensbescherming*", en dus afgekort: "AVG", wordt deze in België amper gebruikt. In Nederlandse publicaties zal bijna altijd de Nederlandstalige titel worden gebruikt, maar in België is de afkorting van het Engelse "*General Data Protection Regulation*" of "GDPR" veel couranter.

Privacy is een relatief oud gegeven dat tot op de dag van vandaag geen echte juridische definitie heeft.[171] Iedereen heeft wel een duidelijk gevoel wat betreft het recht op privacy, maar het is zeer moeilijk om de vinger te leggen op wat privacy nu net is.[172] De moeilijkheid ligt er onder andere in dat privacy doorheen de geschiedenis enorme sprongen heeft gemaakt en ook op dit moment nog afhankelijk is van samenleving tot samenleving.[173] Zo is de Amerikaanse visie op privacy fundamenteel verschillend van de Europese traditie waarop deze scriptie zich in de hoofdzaak zal richten. Zoals James Q. Whitman het benoemt, gaat het *in casu* om een privacy-cultuur gericht op vrijheid versus een privacy-cultuur gericht op waardigheid.[174]

In 1879 werd door de Amerikaan Thomas Cooley, "*The right to be let alone*"[175] beschreven in de relatie tussen overheid en burger. Dit werd in 1890 uitgebreid tot verhoudingen tussen burgers onderling door Louis Brandeis en Samuel Warren.[176] Ze waren ook de eersten die het "*Right to privacy*" als term gebruikten. Sindsdien is in de Verenigde Staten een waaier aan bepalingen ontstaan die betrekking hebben op hun concept van privacy, zonder dat er een concrete, overzichtelijke codificatie is.[177]

In de Europese context is er een minder duidelijk beginpunt te benoemen maar wat betreft codificatie werd het mijns inziens wat duidelijker aangepakt. Er is specifieke wetgeving met het oog op de

[170] Wanneer in dit deel naar artikelen of overwegingen wordt verwezen, zonder specifieke benoeming, wordt de GDPR bedoeld. Het gaat ook over de GDPR wanneer in dit deel wordt verwezen naar de "Verordening" of eender welke andere benaming die duidelijk naar de GDPR verwijst.

[171] Prof. dr. Paul de Hert geeft in zijn bijdrage aan de podcastreeks: "*Universiteit van Vlaanderen*"[171] een zeer overzichtelijke schets van hoe privacy zich doorheen de geschiedenis heeft ontwikkeld. → P. DE HERT, *Is privacy passé?*, Universiteit van Vlaanderen (video), https://www.youtube.com/watch?v=SNGfjU75iCI.

[172] J.J. THOMSON, "The Right to Privacy", in F.D. SCHOEMAN (ed.), *Philosophical Dimensions Of Privacy: An Anthology*, Online, Cambridge University Press, 12 december 2009, p. 272-289, https://doi.org/10.1017/CBO9780511625138.012; J.L. COHEN, *Regulating Intimacy: A New Legal Paradigm*, Princeton and Oxford, Princeton University Press, 2004, 304p, https://doi.org/10.1017/S1743923X05222079.

[173] A. WESTIN, "The origins of modern claims to privacy", p. 62-63, in F.D. SCHOEMAN (ed.), *Philosophical Dimensions of Privacy: An Anthology*, Online, Cambridge University Press, 12 december 2009, p. 56-74, https://doi.org/10.1017/CBO9780511625138.004; B. MOORE Jr., *Privacy: Studies in Social and Cultural History*, Londen, Routledge, p. 59-65, ISBN13: 9780394538198; A. BERTRAND, *Droit a la Vie Privee et Droit à l'image*, Lexis Nexis, 1999, XIII - 222 p., verwijzend naar J.C.BOLOGNE, *Histoire de la Pudeur*, Zaventem, Hachette, 1986, p. 168, ISBN13: 9782012788800; B. BEIGNIER, "La Vie Privée", p. 139-141 in R. CABRILLAC, M.-A. FRISON-ROCHE, T. REVET, C. ALBIGÈS, E. ALFANDARI, B. BERNARD, *Libertés et Droits Fondamentaux*, Parijs, Toulouse Capitole Publications, 2013, ISBN 2-247-05122-7; H.P. DUERR, *Der Mythos vom Zivilisationsprozess*, Frankfurt am Main, Suhrkamp, 1988, p. 59-72.

[174] J.Q. WHITMAN, "The two western cultures of privacy: Dignity versus liberty." *The Yale Law Journal* (nr. 113) 2003, p. 1151-1221, https://doi.org/10.2139/ssrn.476041.

[175] T.M. COOLEY, *A Treatise on the Law of Torts or the Wrongs Which Arise Independ of Contract*, Chicago, Callaghan and Company, 1879, p.29, https://repository.law.umich.edu/books/11/.

[176] L.D. BRANDEIS & S.D. WARREN, "The Right to Privacy", Cambridge (USA), *Harvard Law Review* 1890, p. 193-220.

[177] J.Q. WHITMAN, "The two western cultures of privacy: Dignity versus liberty." *Yale Law Journal* (nr. 113) 2003, p. 1151-1221.

bescherming van privacy terug te vinden op internationaal niveau, EU-niveau en nationaal niveau. Zo werd het recht op respect voor het privéleven in 1948 voor het eerst opgenomen in de Universele Verklaring voor de Rechten van de Mens[178]. In 1950 werd dit recht bevestigd in het Europees Verdrag voor de Rechten van de Mens[179] en in 2000 volgde voor de EU het Handvest van de Grondrechten van de Europese Unie.[180] In nationale wetgeving is het recht op privacy opgenomen in grondwetten en gewone wetten.[181]

In de Europese context is het duidelijk dat privacy te maken heeft met de persoonlijke levenssfeer van mensen en hun gezinnen. Dit is dan ook hoe veel wetgeving dit recht omschrijft.[182] Het gaat echter verder aangezien privacy zich uitstrekt tot alle facetten van het maatschappelijk leven. Werkgevers mogen niet ongelimiteerd hun personeel monitoren[183], ordediensten krijgen niet zonder meer toegang tot eender welke gegevens[184] en het potentieel van ANPR-camera's wordt op dit moment nog niet ten volle benut.[185] [186]

73. WERKWIJZE EN OPBOUW. Dit deel begint in hoofdstuk 1 met een bespreking van het overkoepelende "recht op privacy". Dit zal een relatief kort hoofdstuk zijn waarin via literatuurstudie en begrijpend lezen van wetgeving een overzicht zal worden gegeven van de context waarin de bescherming van persoonsgegevens is ontstaan en waarom het sindsdien is geëvolueerd naar een op zichzelf staand fundamenteel recht.

Hoofdstuk 2 vervolgens, zal gaan over de kern van de zaak: de bescherming van persoonsgegevens. Ten eerste zal het begrip persoonsgegevens onder de loep worden genomen, wat zijn het, hoe moet het worden ingevuld, welke categorieën zijn er, … Vervolgens zal worden gekeken naar de belangrijkste instrumenten die de bescherming van persoonsgegevens nastreven en hoe deze in de praktijk toegepast dienen te worden. Denk hierbij in eerste instantie uiteraard aan de GDPR, maar ook aan de E-Privacy richtlijn, Conventie 108(+) van de Raad van Europa, … interessante leidraden hiervoor zijn te vinden in adviezen en uitspraken van gegevensbeschermingsautoriteiten, nationale rechtbanken en rechtbanken

[178] Universele Verklaring voor de Rechten van de Mens van 10 december 1948, (A/RES/217).
[179] Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden van 4 november 1950.
[180] Handvest van de Grondrechten van de Europese Unie van 14 december 2007, (2007/C 303/01).

[181] Zie artikel 22 Belgische Grondwet; artikel 9, §1 van de Franse Code Civil & loi n° 70-643 du 17 juillet 1970; en artikel 10 van de Nederlandse Grondwet.
[182] Zie artikel 12 UVRM; artikel 8 EVRM; Artikel 17 BUPO-verdrag; artikel 7 Handvest Grondrechten; en artikel 22 Gw; & zie infra: Randnummer 76-78 – Wetgeving betreffende privacy.
[183] Denk hierbij bijvoorbeeld aan CAO nr. 68 betreffende camerabewaking op de werkplek, al dan niet in samenwerking met de Camerawet; CAO nr. 81 betreffende controle op de elektronische netwerkcommunicatie; Het advies van de GBA betreffende de geolocatie van voertuigen van werknemers, https://www.gegevensbeschermingsautoriteit.be/burger/thema-s/privacy-op-de-werkplek/toezicht-van-de-werkgever/geolocalisatie; …
[184] G. VERMEULEN, "Explorerend onderzoek naar de aard van essentiële informatiestromen van de Lokale Politie
Een verkenning van enkele cruciale spanningsvelden", *biblio.ugent.be*, 2009; RICHTLIJN (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.
[185] ANPR-camera's zijn voorbeelden van eerste generatie AI-toepassingen. Zeer simpel uitgelegd werken ze met een vergelijkingssysteem waarbij de volgorden van de tekens die op de nummerplaten geregistreerd worden, worden vergeleken met een databank. Het zou dus een relatief kleine stap zijn om dezelfde camera's toegang te geven tot een databank met biometrische persoonsgegevens.; A. BROUX, "Allemaal lachen naar de slimme camera", *DeJuristen.be* 21 maart 2018, https://dejuristen.be/privacy/allemaal-lachen-naar-de-slimme-camera/.
[186] Voor een uitgebreidere bespreking van het begrip "privacy", voornamelijk gebaseerd op "Seven Types of Privacy", zie infra: Randnummer 75 – Zeven types privacy.

en Hoven op supra- en internationaal niveau. Deze zullen echter niet in detail worden besproken tenzij ze een duidelijk rechtstreeks nut hebben voor deze scriptie.

De GDPR zal in hoofdstuk 3 worden besproken aan de hand van haar belangrijkste principes. De toestemming van datasubjecten als stokpaardje is hierin niet te vergeten, maar ook andere basisbegrippen, zoals de beginselen van verwerking, de rechten van datasubjecten, … zullen uitvoerig bekeken moeten worden om vervolgens in hoofdstuk 4 de relevante bepalingen die van toepassing zouden kunnen zijn op artificiële intelligentie te identificeren en in detail te ontleden.

2.1. Hoofdstuk 1. Het recht op privacy[187]

2.1.1. Het begrip "privacy"[188]

74. **INLEIDING.** Net zoals "artificiële intelligentie" is er een zekere moeilijkheid die al bij de absolute basis begint, namelijk een concrete definiëring. Bij AI heeft de wetgever deze leemte opgevuld door in artikel 3 (1) van het voorstel een wettelijke definitie op te nemen. Dit geluk hebben we niet met betrekking tot "privacy". Zoals eerder reeds aangehaald[189] is dit onder andere te wijten aan het feit dat het gaat om een concept dat zware invloed ondervindt van zowel tijd als ruimte. Het Amerikaans begrip van privacy focust vooreerst op individuele vrijheid, terwijl de Europese context voornamelijk gericht is op het beschermen van de waardigheid van personen.[190]

De problematiek omtrent definiëring is reeds door verschillende auteurs aangekaart[191], maar meestal gaat het eerder om een opsomming van alle mogelijke soorten schade dan om een effectieve definiëring.[192]

75. **ZEVEN TYPES PRIVACY.** Roger Clarke bracht hier in 1997[193] verandering door een opsomming te geven van vier categorieën die hij herkende binnen het geheel van privacy. Deze opsomming werd in 2013[194] aangevuld tot zeven, dewelke in deze thesis kort zullen worden aangehaald: (1) Privacy van de persoon, (2) privacy omtrent gedrag en handelingen, (3) privacy m.b.t. communicatie, (4) privacy m.b.t. data en afbeelding, (5) privacy omtrent gedachten en gevoelens, (6) privacy omtrent locatie en ruimte en (7) privacy met betrekking tot sociaal leven.

---

[187] S. CONIX, L. PEETERS, A. VAN LOOVEREN, & I. VERHELST, *Privacy, 1e editie*, Brussel, Intersentia, 2019, 194p.;A.E. CUDD & M.C. NAVIN (eds.), *Core Concepts and Contemporary Issues in Privacy*, Cham, Springer, 2018, 265p.; D.J. SOLOVE, *Understanding Privacy*. Cambridge MA, Harvard University Press, 2008.

[188] R.L. FINN, D. WRIGHT, M. FRIEDEWALD, "Seven Types of Privacy", p. 3-32 (https://doi.org/10.1007/978-94-007-5170-5_1), in S. GUTWIRTH, R. LEENES, P. DE HERT, Y. POULLET (eds), *European Data Protection: Coming of Age*, Dordrecht, Springer, 2013, XII, 440p., https://doi.org/10.1007/978-94-007-5170-5_1.

[189] Zie supra: Randnummers 74 – Inleiding & 75 – Zeven types privacy.

[190] J.Q. WHITMAN, "The two western cultures of privacy: Dignity versus liberty." *Yale Law Journal* (nr. 113) 2003, p. 1151-1221.

[191] Wat volgt is een opsomming van enkele auteurs en hun werken ter illustratie van de moeilijkheid die zich voordoet omtrent de definiëring van het begrip: "privacy", zonder dat deze volledig werden gelezen of noemenswaardige impact hebben gehad op deze thesis: D. LYON, *Surveillance after September 11*, Cambridge, Polity Press, 26 september 2003, 197p., ISBN: 0745631819, 9780745631813; S. GUTWIRTH, *Privacy and the information age*, Lanham, MD, Rowman & Littlefield, 2002, 152p., ISBN: 0742517462, 9780742517462; C.J. BENNETT, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Ithaca NY, Cornell University Press, 2018, 288p., ISBN: 1501722131, 9781501722134; D.V.S. KASPAR, "The Evolution (or Devolution) of Privacy," *Sociological Forum* (vol. 20, nr. 1) 2005, p. 69-92, https://www.jstor.org/stable/4540882; H. NISSENBAUM, "Privacy as Contextual Integrity", *Washington Law Review* (vol.79, nr.1) 2004, p.119-158, https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10; B.J. GOOLD, "Surveillance and the Political Value of Privacy", *Amsterdam Law Forum* 2009, https://doi.org/10.37974/ALF.80; B.J. GOOLD and L. LAZARUS, *Security and Human Rights*, Bloomsburry Publishing, 2019, 240p., ISBN: 1509917780, 9781509917785; C. FUCHS, "Towards an alternative concept of privacy", *Journal of Information, Communication and Ethics in Society* (vol.9, issue 4) 2011, p.671-687, https://doi.org/10.1108/14779961111191039.

[192] D.J. SOLOVE, *Understanding Privacy,* Cambridge MA, Harvard University Press, 2010, 272p, ISBN: 9780674035072.

[193] R. CLARKE, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms", *Xamax Consultancy*, augustus 1997, http://www.rogerclarke.com/DV/Intro.html; R. CONNOLLY & G. FOX, "Dataveillance and Information Privacy Concerns", p. 391-410, in A. NORMORE, M. JAVADI & L. LONG (eds.), *Handbook of Research on Strategic Communication, Leadership, and Conflict Management in Modern Organizations*, Hershey, PA, IGI Global, 2019, 553p., https://doi.org/10.4018/978-1-5225-8516-9.

[194] R.L. FINN, D. WRIGHT & M. FRIEDEWALD, "Seven Types of Privacy", in S. GUTWIRTH, R. LEENES, P. DE HERT & Y. POULLET (eds.) *European Data Protection: Coming of Age,* Dordrecht, Springer, p. 4-6. https://doi.org/10.1007/978-94-007-5170-5_1.

Zeven types privacy	
Privacy van de persoon.	Hierin gaat het om wat ook als lichamelijke integriteit valt te omschrijven. Eenieder heeft het recht om de karakteristieken en functies omtrent zijn of haar lichaam privé te houden.
Privacy omtrent gedrag en handelingen.	Iemands seksuele voorkeur, religieuze praktijken, maar ook minder gevoelige informatie, zoals hoe men zich gedraagt in publieke, semi-publieke of private ruimtes, is in essentie enkel zijn of haar zaak.
Privacy m.b.t. communicatie.	Het lijkt vanzelfsprekend dat de communicatie tussen mensen tot hun privé behoort, wat ook door veel overheden wordt geaccepteerd. Daarom wordt er streng op toegezien dat communicatie niet onrechtmatig wordt onderschept en ingekeken.
Privacy m.b.t. data en afbeelding.	Persoonsgegevens zijn alle mogelijke data over een geïdentificeerde of identificeerbare persoon, hierbij kan het gaan om biometrische gegevens, zoals vingerafdrukken of gezichten, maar ook om bankrekeningnummers, emailadressen, … het recht van bescherming van deze gegevens kan onder privacy worden gesteld.
Privacy omtrent gedachten en gevoelens.	Gedachten en gevoelens moeten onderscheiden worden van gedrag en handelingen. Het is namelijk zo dat niet elk idee een handeling tot gevolg heeft en soms handelt men ook zonder nadenken. Het zijn verschillende aspecten van privacy die beiden beschermd moeten worden. Iedereen heeft het recht om zijn gedachten en gevoelens niet kenbaar te maken.
Privacy omtrent locatie en ruimte.	Een belangrijk aspect van privacy dat op dit moment wel eens vaker in het gedrang komt, is het recht om zich vrij te bewegen in openbare en semi-openbare ruimtes, zonder geïdentificeerd, gevolgd of gemonitord te worden.
Privacy met betrekking tot sociaal leven.	Het is het recht van eenieder om zelf te kiezen met wie men zich omringt. Dit wilt zeggen dat er in principe geen controle of toezicht mag worden uitgeoefend op het sociale gedrag van mensen en in welke groepen ze zich begeven.

Figuur 10. Zeven types privacy

Het mag opvallen dat de verschillende aspecten van privacy die door Finn *et al.* beschreven worden duidelijk overlappingen vertonen met andere fundamentele rechten zoals het recht op lichamelijk integriteit, de vrijheid van gedachte, geweten en godsdienst, de vrijheid van meningsuiting en de vrijheid van vergadering en vereniging. Dit komt omdat het desbetreffende aspect van privacy een voorwaarde is om het fundamenteel recht in kwestie te kunnen verzekeren.[195] Zo is het bijvoorbeeld quasi onmogelijk om de vrijheid van meningsuiting te garanderen – een handeling –, zonder dat er eerst een recht is om een mening te vormen – in gedachten – en dit natuurlijk zonder inmenging van een overheid of derde.

[195] FRA, *Handbook on European data protection law – 2018 edition*, Luxemburg, Publications Office of the European Union, 2018, p. 19.

2.1.2. Wetgeving

76. **INLEIDING.** Het recht op privacy en het recht op bescherming van persoonsgegevens is, op alle niveaus waarop wetgeving bestaat, verzekerd. Internationaal, supranationaal en nationaal. In deze titel zullen alle in de Europese context relevante wetgevende teksten worden besproken. Met hun toepassingsgebied en afdwingbaarheid. Laat duidelijk zijn dat voor de Europese Unie, als rechtstreeks werkende, door haar uitgevaardigde tekst, enkel het Handvest van de Grondrechten van de Europese Unie geldt, maar dat er ook andere artikelen ten minste een zeker gewicht geven aan de fundamentele rechten op privacy en gegevensbescherming.

77. **DRAAGWIJDTE.** Het is belangrijk om in het achterhoofd te houden dat het recht op privacy geen absoluut recht is. Dit wil zeggen dat, los van of u en ik het ermee eens zijn, inperkingen mogelijk zijn. Hier staat tegenover dat hiermee zeer bedachtzaam moet worden omgegaan. De verschillende wetgevers hebben niet voor niets het recht op privacy verheven tot een fundamenteel recht.

78. **INTERNATIONAAL & SUPRANATIONAAL.**[196] Het eerste niveau dat besproken dient te worden is het internationaal niveau. Via verdragen kunnen verschillende van elkaar onafhankelijke staten overeenkomsten sluiten. Dit wordt vaak gedaan over zaken waarin het maar weinig nut heeft om alleen te staan, zoals bijvoorbeeld kernenergie, biologische en chemische wapens en fundamentele (mensen-) rechten. Het eerste en nog steeds toonaangevende document dat in deze context werd uitgevaardigd is de Universele Verklaring van de Rechten van de Mens dat door de Verenigde Naties in 1948 werd gepubliceerd.[197] Het UVRM, hoewel het zeer invloedrijk is, bindt niets of niemand.

Daarom werden er onder andere door de Raad van Europa (RvE) en de Verenigde Naties zelf enkele teksten aangenomen die voor haar lidstaten wel bindende kracht hebben. Het gaat in deze om het Europees Verdrag voor de Rechten van de Mens[198] (EVRM) en het Internationaal Verdrag inzake Burgerlijke en Politieke Rechten[199] (IVBPR of BUPO-verdrag).

Sinds 1953[200] vrijwaart artikel 8 van het EVRM[201] natuurlijke personen van onrechtmatige inmenging in hun privéleven, familie- en gezinsleven, hun woning en hun correspondentie. Om de naleving van de bepalingen van het EVRM af te dwingen werd het Europees Hof voor de Rechten van de Mens in 1959 opgericht.[202]

---

[196] FRA, *Handbook on European data protection law – 2018 edition*, Luxemburg, Publications Office of the European Union, 2018, p. 21-24.
[197] Verenigde Naties, Universele Verklaring van de Rechten van de Mens, 10 december 1948;
In het UVRM wordt het recht op privacy beschermd door **Artikel 12 UVRM:** "*Niemand zal onderworpen worden aan willekeurige inmenging in zijn persoonlijke aangelegenheden, in zijn gezin, zijn tehuis of zijn briefwisseling, noch aan enige aantasting van zijn eer of goede naam. Tegen een dergelijke inmenging of aantasting heeft eenieder recht op bescherming door de wet.*"
[198] Raad van Europa, Europees Verdrag voor de Rechten van de Mens en de Fundamentele Vrijheden, 4 november 1950.
[199] Verenigde Naties, Internationaal verdrag inzake burgerrechten en politieke rechten, 19 december 1966.
[200] Inwerkingtreding van het EVRM.
[201] **Artikel 8 EVRM:** "*1. Een ieder heeft recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.*
2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen."
[202] FRA, *Handbook on European data protection law – 2018 edition*, Luxemburg, Publications Office of the European Union, 2018, p. 23; & artikel 19 ev. EVRM.

Het BUPO-verdrag bindt haar 169 lidstaten tot naleving van – onder andere – artikel 17[203], dat qua tekstuele inhoud nagenoeg identiek is aan artikel 8 EVRM. De handhaving van het BUPO-verdrag wordt aan het VN-comité voor de Rechten van de Mens toevertrouwd. Hoewel het Comité uiteraard een zeker gezag heeft, moet het zich beperken tot het formuleren van meningen en aanbevelingen. Afdwingen is dus niet mogelijk.

79. **EUROPESE UNIE.** De EU is het voorbeeld bij uitstek wanneer het gaat om een supranationale instantie. De oprichtingsverdragen vallen onder het internationaal recht[204], terwijl de wetgevende documenten die de EU zelf uitvaardigt onder de noemer "supranationaal recht" vallen.[205] Deze tweedeling wordt ook doorgetrokken in de rechtsleer omtrent het EU-recht, waarin twee onderdelen te onderscheiden zijn: het primair en het secundair recht. Het primair recht bestaat uit de twee verdragen die aan de Unie ten grondslag liggen: Het Verdrag betreffende de Europese Unie[206]; en het Verdrag betreffende de Werking van de Europese Unie.[207] Alle verordeningen, richtlijnen, besluiten, aanbevelingen en adviezen die door een EU-instelling zijn uitgevaardigd, vormen het secundair EU-recht.

In eerste instantie werd in geen van de verdragen tot oprichting van de Europese Unie melding gemaakt van mensenrechten omdat het historisch gezien eigenlijk enkel de bedoeling was om een vrije interne markt te creëren. Beetje bij beetje doken er echter problemen op met betrekking tot mensenrechten binnen de onderwerpen waarvoor de EU bevoegd is. Erkennend dat haar regelgevingen een impact kunnen hebben op fundamentele rechten, heeft de EU in 2000 het Handvest van de Grondrechten van de Europese Unie afgekondigd[208]. Enkele jaren later, in 2009,[209] kreeg het Handvest een juridisch bindend karakter, waardoor sindsdien de EU-instellingen en lidstaten verplicht zijn haar bepalingen in acht te nemen bij hun werking.[210]

Artikel 7 van het handvest volgt in de voetsporen van het UVRM, het EVRM en het BUPO-verdrag en verklaart in zeer gelijkaardige bewoording dat de eerbiediging van het privé leven, familie- en gezinsleven van personen, alsook hun woning en communicatie niet zomaar kunnen worden geschonden.[211] Omdat het Handvest significant jonger is dan alle voorgaande teksten is het recht op bescherming van persoonsgegevens in artikel 8 als fundamenteel recht opgenomen. Meer hierover volgt in het volgende hoofdstuk.[212]

---

[203] **Artikel 17 BUPO-verdrag**: "*Niemand mag worden onderworpen aan willekeurige of onwettige inmenging in zijn privé leven, zijn gezinsleven, zijn huis en zijn briefwisseling, noch aan onwettige aantasting van zijn eer en goede naam. Een ieder heeft recht op bescherming door de wet tegen zodanige inmenging of aantasting*."

[204] Omdat ze tussen lidstaten overeengekomen zijn. Elk van de lidstaten had de volledige bevoegdheid om al dan niet deel te nemen aan het verdrag.

[205] Omdat de lidstaten hier zelf geen echte zeg meer in hebben. Ze hebben in de oprichtingsverdragen namelijk de bevoegdheid voor bepaalde onderwerpen overgedragen aan de EU-instellingen, dewelke nu dus rechtstreeks in alle lidstaten toe te passen wetgeving kunnen uitvaardigen.

[206] Verdrag betreffende de Europese Unie (geconsolideerde versie) van 26 oktober 2012, (C 326/13).

[207] verdrag betreffende de werking van de Europese Unie (geconsolideerde versie) van 26 oktober 2012, (C 326/46).

[208] Handvest van de Grondrechten van de Europese Unie van 14 december 2007, (2007/C 303/01).

[209] Bij het in werking treden van het Verdrag van Lissabon.

[210] FRA, *Handbook on European data protection law – 2018 edition*, Luxemburg, Publications Office of the European Union, 2018, 397p.

[211] **Zie artikel 7 Handvest Grondrechten**: "*De eerbiediging van het privé-leven en van het familie- en gezinsleven. Eenieder heeft recht op eerbiediging van zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn communicatie*."

[212] Zie infra: Randnummer 86 – Europese Unie.

80. **NATIONAAL.** Op nationaal niveau wordt alle bovenstaande wetgeving, die niet uit haar aard rechtstreeks van toepassing zou zijn, uiteindelijk ten uitvoer gebracht. In België resulteerde dit in verschillende wetten, decreten, ordonnanties of uitvoeringsbesluiten. Denk hierbij bijvoorbeeld aan de Camerawet[213] en de Wet tot oprichting van de Gegevensbeschermingsautoriteit.[214]

Alvorens tot deze uitvoerende wetgeving te komen is er op het nationaal niveau echter nog een laatste keer een expliciete verklaring omtrent de grondrechten die elke inwoner van de desbetreffende staat geniet. In België is het artikel 22 van de Grondwet[215] dat het recht op privacy beschermt.

[213] Wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's, gewijzigd door de wetten van 12 november 2009, 3 augustus 2012, 4 april 2014 en 21 april 2016 (gecoördineerde versie), *BS* 31 mei 2007.
[214] Wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, *BS* 10 januari 2018; Zie ook: https://www.gegevensbeschermingsautoriteit.be/publications/bijlage-advies-op-het-voorontwerp-van-wet-tot-wijziging-van-de-gba-wet.pdf.
[215] **Zie artikel 22 Gw.**: *"Ieder heeft recht op eerbiediging van zijn privéleven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald.*
De wet, het decreet of de in artikel 134 bedoelde regel waarborgen de bescherming van dat recht."

2.2. Hoofdstuk 2. Bescherming van persoonsgegevens

2.2.1. Plaats binnen privacy

81. **KORTE INLEIDING.** Dat het recht op privacy en het recht op bescherming van persoonsgegevens niet één en hetzelfde recht is, lijkt op dit punt al wel evident. Geen beter bewijs dan dat het Handvest van de Grondrechten[216] beiden afzonderlijk verankerd als fundamentele rechten. Hoe de twee zich concreet tot elkaar verhouden, is echter nog niet besproken.

82. **VERHOUDING EN GESCHIEDENIS.**[217] Het recht op privacy is zonder twijfel het oudste van de twee. Ten tijde van Cooley, Warren en Brandeis was er namelijk nog geen sprake van computers, laat staan van artificiële intelligentie. Het was pas met de ontwikkeling van computers voor privégebruik en het internet, dat de zogenaamde "informatiesamenleving"[218] ontstond, waarin er een nood was aan de bescherming van de data die al deze mensen genereerden.

De bescherming van persoonsgegevens kwam in Europa op gang rond 1970 doordat sommige staten[219] uit eigen beweging gegevensbeschermingswetgeving begonnen aan te nemen. In 1981 werd door de Raad van Europa, Conventie 108[220] aangenomen en pas in 1995 volgde de EU met de Gegevensbeschermingsrichtlijn[221] die in 2018 door de GDPR werd vervangen. Ook Conventie 108 heeft in 2018 een update gekregen en gaat momenteel door het leven als Conventie 108+.[222]

Beide rechten hebben als doel de vrije persoonsontwikkeling van mensen te beschermen. In die zin zijn ze dus zeer gelijkaardig. Het verschil ligt hem echter in de formulering en de manier waarop ze worden toegepast. Het recht op privacy wordt geformuleerd als een verbod op inmenging met uitzondering van enkele specifieke, door wet bepaalde gevallen. Het recht op bescherming van persoonsgegevens voorziet in een systeem van "checks and balances" om natuurlijke personen te beschermen wanneer hun gegevens worden verwerkt. Het verschil tussen de twee werd door de EU-wetgever erkend door het afzonderlijk opnemen van de rechten[223] en ook Advocaat-Generaal Eleanor Sharpston merkte in 2010 het onderscheid op.[224]

---

[216] Europese Unie, Handvest van de Grondrechten van de Europese Unie, 26 oktober 2012.
[217] FRA, *Handbook on European data protection law – 2018 edition*, Luxemburg, Publications Office of the European Union, 2018, p. 18-19.
[218] M. CASTELLS, *Rise of the Network Society: The Information Age: Economy, Society and Culture, Malden*, Massachusetts, Blackwell Publishers, 1996 (herzien in 2010), 625p., https://urb.bme.hu/wp-content/uploads/2014/05/manuel_castells_the_rise_of_the_network_societybookfi-org.compressed.pdf; C. FUCHHS, *Internet and Society: Social Theory in the Information Age*, New York, Routledge, 2007, 816p., ISBN: 1135898820, 9781135898823; ….
[219] In 1970: Hesse (Duitsland); In 1973: Zweden; tegen 1980: Frankrijk, Duitsland (volledig), Nederland en het Verenigd Koninkrijk.
[220] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, (ETS No. 108).
[221] 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.
[222] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, (ETS no. 223).
[223] Zie artikelen 7 & 8 Handvest Grondrechten EU.
[224] Advocaat Generaal Sharpston beschrijft het recht op privacy als het "klassieke" recht ten opzichte van het "moderne en actieve recht" recht op bescherming van persoonsgegevens. HvJ-EU, samengevoegde zaken C-92/09 & C-93/02, *Volker und Markus Schecke GbR v. Land Hessen*, mening van Advocaat Generaal Sharpston, 17 juni 2010, paragraaf 71.

2.2.2. Wetgeving

83. **INTERNATIONAAL & SUPRANATIONAAL.** Het eerder besproken UVRM, EVRM en BUPO-verdrag benoemen geen van allen uitdrukkelijk het recht op bescherming van persoonsgegevens. Ze spreken enkel over het overkoepelende recht op privacy dat ten tijde van deze documenten ook het enige noodzakelijke was. Op de relatief recente ontwikkelingen omtrent computertechnologie die een afzonderlijk recht op dataprotectie nodig maakten, werd door de desbetreffende wetgevers[225] niet gereageerd met aanpassingen of aanvullingen van de originele artikelen 12 UVRM, 8 EVRM of 17 BUPO-verdrag.

84. **DE VERENIGDE NATIES.** De Verenigde Naties, die zowel verantwoordelijk waren voor het UVRM als voor het BUPO-verdrag, hebben geen aanpassingen doorgevoerd in bovenstaande teksten. Wel zijn er in 2013[226] en 2014[227] - niet geheel toevallig voorafgegaan door de Snowden-leaks[228] – resoluties aangenomen waaruit duidelijk blijkt dat massasurveillance niet door de beugel kan en dat het een zware impact kan hebben op fundamentele rechten en het functioneren van de democratie. In 2016[229] en 2017[230] werden de voorgaande resoluties herzien om nu, naast de focus op overheidsverantwoordelijkheden, ook aandacht te schenken aan de impact van dataverzameling en -verwerking in de private sector.

85. **DE RAAD VAN EUROPA.** Ook het EVRM vermeldt nergens het recht op bescherming van persoonsgegevens en de aanpak van de Raad van Europa vertoont enkele duidelijke verschillen met die van de VN. Ten eerste is het zo dat het recht op dataprotectie integraal onder de beschermde rechten van artikel 8 EVRM valt. Dit blijkt uit verschillende zaken voor het Europees Hof voor de Rechten van de Mens, dat problemen omtrent bescherming van persoonsgegevens steeds plaatst onder artikel 8 EVRM[231] en uit haar expliciet erkennen van het recht op bescherming van persoonsgegevens als een belangrijk onderdeel van het recht op privacy.[232]

Naast de ruime interpretatie van artikel 8 EVRM is er door het Comité van Ministers in 1981 Conventie 108 opgesteld,[233] die op 18 mei 2018 werd herzien tot Conventie 108+. Dit is vandaag de dag nog steeds

[225] *In casu* dus alle lidstaten die lid zijn van de verdragen. Aanpassingen aan het UVRM zijn niet echt nuttig aangezien het toch voornamelijk een ceremoniële functie heeft.
[226] VN, Algemene Vergadering, Resolution on the right to privacy in the digital age, A/RES/68/167, New York, 18 december 2013.
[227] VN, Algemene Vergadering, Revised draft resolution on the right to privacy in the digital age, A/C.3/69/L.26/Rev.1, New York, 19 november 2014.
[228] P. SZOLDRA, "This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks", *Businessinsider* 16 september 2016, https://www.businessinsider.com/snowden-leaks-timeline-2016-9?international=true&r=US&IR=T; & G. GREENWALD, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, New York, Henry Holt and Company, 13 mei 2014, 272p., ISBN: 1627790748, 9781627790741.
[229] VN, Algemene Vergadering, Revised draft resolution on the right to privacy in the digital age, A/C.3/71/L.39/Rev.1, New York, 16 november 2016.
[230] VN, Raad voor de mensenrechten, The right to privacy in the digital age, A/HRC/34/L.7/Rev.1, 22 maart 2017.
[231] Zie hiervoor bijvoorbeeld: EHRM, *Klass et all. v. Duitsland*, nr. 5029/71, 6 september 1978; EHRM, *Malone v. Verenigd Koninkrijk*, nr. 8691/79, 2 augustus 1984; EHRM, *Rotaru v. Roemenië* [GC], nr. 28341/95, 4 mei 2000; EHRM*, Uzun v. Duitsland*, nr. 35623/05, 2 september 2012; EHRM, *Szabó en Vissy v. Hongarije*, nr. 37138/14, 12 januari 2016; …
[232] FRA, *Handbook on European data protection law – 2018 edition*, Luxemburg, Publications Office of the European Union, 2018, p. 25 & p. 37; & EHRM, *Z v. Finland*, nr. 22009/93, 25 februari 1997.
[233] Raad van Europa, Conventie ter bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, CETS nr. 108, 1981.

het enige bindende internationale instrument ter bescherming van data.[234] Hoewel het niet onder toezicht van het EHRM valt, heeft dit Hof zich wel al meermaals laten beïnvloeden door haar bepalingen.

86. **EUROPESE UNIE.** Zoals eerder reeds kort vermeld[235], was in het Handvest van de Grondrechten van de Europese Unie de enige expliciete vermelding van gegevensbescherming als fundamenteel recht terug te vinden. Artikel 8[236] vermeldt in haar tweede lid de basisprincipes waarop gegevensverwerking moet geschieden en in haar derde lid wordt een onafhankelijke toezichthoudende instantie vereist. Deze criteria zullen later uitvoerig worden besproken aangezien ze van groot belang zijn voor de toepassing van de GDPR.[237]

Het Verdrag van Lissabon heeft niet enkel het Handvest verheven tot primair unierecht, maar onder de herzieningen van de constitutieve verdragen werd ook het recht op bescherming van persoonsgegevens ingevoegd in artikel 16 VWEU[238], waardoor het dus een expliciete bevoegdheid van de Unie is geworden.[239]

De Gegevensbeschermingsrichtlijn,[240] die aan de GDPR vooraf ging, werd aangenomen in 1995 om een zekere harmonisering te bekomen in de verschillende wetgevingen die lidstaten reeds volop aan het implementeren waren. Het was de bedoeling van de EU-wetgever om tot een volledige harmonisatie te komen zodat binnen de EU éénzelfde, hoogwaardige bescherming van persoonsgegevens kon worden gegarandeerd.[241] Dit bleek in de praktijk niet te lukken met een richtlijn en dus begonnen de gesprekken voor een modernisering in 2009, met als resultaat in 2016 de goedkeuring van de Algemene Verordening Gegevensbescherming, of GDPR zoals deze in België beter bekend is, dewelke in werking is getreden op 25 mei 2018.

---

[234] FRA, *Handbook on European data protection law – 2018 edition*, Luxemburg, Publications Office of the European Union, 2018, p. 24.

[235] Zie supra: Randnummer 79 – Europese Unie.

[236] Zie **artikel 8 Handvest Grondrechten**: "*De bescherming van persoonsgegevens. 1. Eenieder heeft recht op bescherming van zijn 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 van inzage in de over hem verzamelde gegevens en op rectificatie daarvan. 3. Een onafhankelijke autoriteit ziet erop toe dat deze regels worden nageleefd.*"

[237] Zie infra: Randnummer 103 – Beginselen inzake verwerking van persoonsgegevens; De vereiste van een onafhankelijke toezichthoudende overheid wordt in deze scriptie niet meer uitgebreid besproken. Hieraan werd in België echter voldaan door de voormalige Privacycommissie om te dopen tot de Gegevensbeschermingsautoriteit en haar de specifieke bevoegdheden toe te kennen die haar in staat moeten stellen het GDPR-regime af te dwingen.

[238] Zie **artikel 16 VWEU**: "*1. Eenieder heeft recht op bescherming van zijn persoonsgegevens. 2. Het Europees Parlement en de Raad stellen volgens de gewone wetgevingsprocedure de voorschriften vast betreffende de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie, alsook door de lidstaten, bij de uitoefening van activiteiten die binnen het toepassingsgebied van het recht van de Unie vallen, alsmede de voorschriften betreffende het vrij verkeer van die gegevens. Op de naleving van deze voorschriften wordt toezicht uitgeoefend door onafhankelijke autoriteiten.*
De op basis van dit artikel vastgestelde voorschriften doen geen afbreuk aan de in artikel 39 van het Verdrag betreffende de Europese Unie bedoelde specifieke voorschriften."

[239] FRA, *Handbook on European data protection law – 2018 edition*, Luxemburg, Publications Office of the European Union, 2018, p. 28.

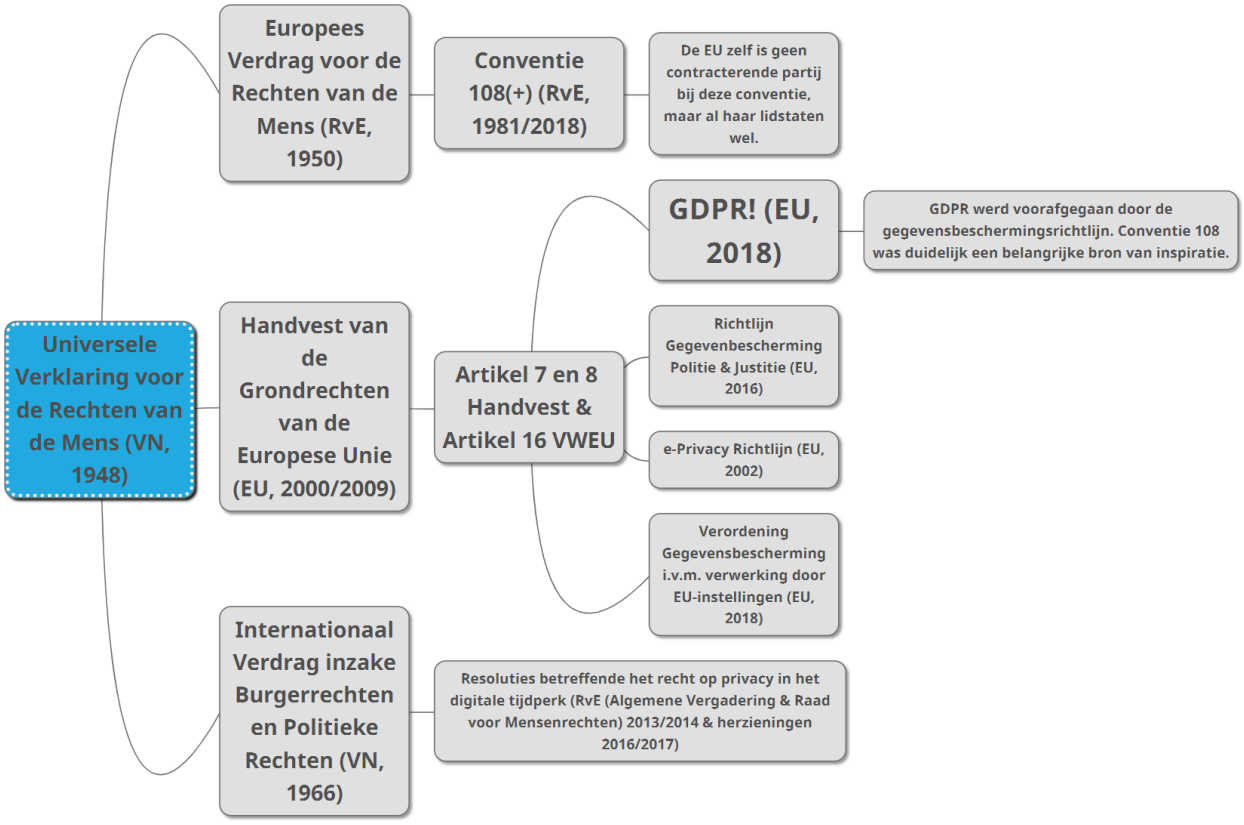
[240] RICHTLIJN 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

[241] FRA, Handbook on European data protection law – 2018 edition, Luxemburg, Publications Office of the European Union, 2018, p. 30; verwijzend naar HvJ-EU, samengevoegde zaken C-468/10 en C-469/10, *Asociación Nacional de Astablecimientos Financieros de Crédito (ANSEF)* en *Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 24 november 2011, para. 29.

Naast de GDPR zijn er op dit moment nog drie andere EU-instrumenten in werking die voor de volledigheid kort zullen worden benoemd, maar waaraan verder geen aandacht zal worden geschonken in deze scriptie.

1. De **Richtlijn Gegevensbescherming Politie en Justitie**:[242] Deze Richtlijn streef een harmonisatie van de verwerking van persoonsgegevens door ordediensten na, wanneer die verwerking gebeurt in verband met het voorkomen, opsporen en vervolging van criminele activiteiten. Ze dient samen te worden gelezen met de GDPR binnen haar toepassingsgebied.[243]
2. De **e-Privacy Richtlijn**:[244] Deze Richtlijn legt enkele specifieke regels op in verband met gegevensverwerking in de elektronische communicatiesector. Het was de bedoeling deze Richtlijn een update te geven in de vorm van een verordening die samen met de GDPR in werking zou treden en als *lex specialis* dienst zou doen.[245] Dat is spijtig genoeg niet gelukt en dus is het nog wachten op de e-Privacy Verordening. Ook deze zal verder niet concreet worden toegelicht.
3. De **Verordening Gegevensbescherming met betrekking tot verwerking door de communautaire instellingen en organen**:[246] Omdat alle bovengenoemde instrumenten enkel van toepassing zijn op (lid)staten en private spelers, was er ook nood aan regeling voor de dataverwerking die de EU-instituten zelf behartigen. In 2001 werd hiertoe een eerste verordening aangenomen die in 2018 werd ingetrokken teneinde met een nieuwe verordening mooi aan te sluiten op het GDPR-regime. Deze verordening stelt uiteraard dezelfde gekende verwerkingsprincipes voorop.[247]

[242] RICHTLIJN (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.
[243] FRA, *Handbook on European data protection law – 2018 edition*, Luxemburg, Publications Office of the European Union, 2018, p. 32.
[244] 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)
[245] VOORSTEL van 10 januari 2017 voor een verordening van het Europees Parlement en de Raad met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, en tot intrekking van Richtlijn 2002/58/EG (richtlijn betreffende privacy en elektronische communicatie) → https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52017PC0010.
[246] VERORDENING (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG.
[247] Zie supra: Randnummer 103 – Beginselen inzake verwerking van persoonsgegevens; en infra: Randnummer 86 – Europese Unie.



Figuur 11. Samenhang tussen alle met privacy & gegevensbescherming gerelateerde internationale instrumenten.

2.2.3. Terminologie m.b.t. bescherming van persoonsgegevens

87. **INLEIDING.** Wat betreft de relevante terminologie met betrekking tot de bescherming van persoonsgegevens kan worden gekeken naar artikel 4 GDPR. De definities van "persoonsgegevens", "verwerking", "profileren", "verwerkingsverantwoordelijke", "verwerker", "toestemming", "genetische gegevens" en "biometrische gegevens" zullen in de komende randnummers besproken worden alvorens in het volgende hoofdstuk over te gaan tot de krachtlijnen van de GDPR.

88. **KEUZE VAN RECHTSPRAAK.** Rechtspraak is tot op dit moment relatief afwezig geweest in deze scriptie. Dit is niet omdat niet werd gezocht, maar voornamelijk omdat niets werd gevonden. Met betrekking tot artificiële intelligentie is er op dit moment nog geen relevante rechtspraak. Dit is anders met betrekking tot gegevensbescherming. In dit gebied zijn er doorheen de jaren wel enkele belangrijke arresten geveld door alle Hoven die hiervoor reeds besproken werden.[248] Omdat deze scriptie focust op secundair EU-recht, zal er niet worden gekeken naar rechtspraak afkomstig van andere rechtscolleges, zoals het EHRM of nationale rechtbanken, tenzij het relevante hof, *in casu* het Hof van Justitie van de Europese Unie, deze uitspraken uitdrukkelijk volgt of in haar redenering zou betrekken.

Hoewel de relevante arresten voor het merendeel stammen van voor de inwerkingtreding van de GDPR, en dus betrekking hebben op de vroegere Richtlijn[249], zijn de arresten met betrekking tot interpretatie en applicatie van de terminologie en de principes nog steeds relevant. Het is op dit moment niet opportuun om een lijst op te stellen van rechtspraak die het HvJ-EU met betrekking tot bescherming van persoonsgegevens heeft uitgesproken, maar verder in deze tekst zal op verschillende punten worden verwezen naar interessante arresten.

Het begrip "persoonsgegevens"

89. **PERSOONSGEGEVENS.** Er is op de vorige pagina's van dit tweede deel bijna non-stop gesproken over de bescherming van persoonsgegevens, maar waar gaat dit nu eigenlijk precies over?

> *"Persoonsgegevens": alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;*[250]

[248] Zie supra: Randnummer 73.
[249] 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.
[250] Zie artikel 4(1) GDPR.

Uit bovenstaande definitie kunnen twee voorwaarden worden gedestilleerd die noodzakelijk zijn alvorens er over persoonsgegevens kan worden gesproken:

1. Het moet gaan om informatie over natuurlijke personen;
2. Die daardoor geïdentificeerd of identificeerbaar worden.

90. NATUURLIJKE PERSONEN.[251] De enige begunstigden van gegevensbeschermingsregels zijn natuurlijke personen en dit slechts voor zover ze in leven zijn.[252] De titularissen van de rechten die hem of haar worden toegekend door de GDPR worden rechtssubjecten genoemd – of "betrokkenen" –. In tegenstelling tot het uitbreidbaar toepassingsgebied ratione personae onder conventie 108+, houdt EU-gegevensbeschermingsrecht zich niet bezig met rechtspersonen als datasubject.[253] Dit principe werd door het Hof van Justitie van de Europese Unie (HvJ-EU) uitgelegd in *Volker und Markus Schecke en Hartmut Eifert v. Land Hessen*.[254] In dit arrest verklaarde het Hof dat rechtspersonen de bescherming van artikel 7 en 8 van het Handvest slechts kunnen inroepen in zoverre dat de officiële bedrijfsnaam één of meerdere natuurlijke personen identificeert.

91. IDENTIFICEREN OF IDENTIFICEERBAAR MAKEN.[255] Dit criteria wordt door artikel 4(1) zelf redelijk duidelijk verklaard. Identificeren gebeurt aan de hand van één of meerdere indicatoren, dit zijn elementen die kenmerkend zijn voor een persoon en waardoor hij dus onderscheiden kan worden van een andere persoon. Denk hierbij aan een naam, identificatienummer, IP-adres, …

Het onderscheid tussen directe en indirecte identificatie behoeft echter wel nog een woordje uitleg. Directe identificatie wilt zeggen dat door middel van de beschikbare gegevens, de persoon in kwestie perfect, zonder verdere tussenstappen kan worden aangeduid. De gegevens die nodig zijn voor directe identificatie laten dus geen ruimte over voor twijfel, want het kan maar om één natuurlijke persoon gaan.

Indirecte identificatie vereist in de regel nog bijkomende elementen. De data die verwerkt wordt is niet voldoende om met zekerheid één persoon aan te duiden. Denk hiervoor bijvoorbeeld aan een telefoonnummer, een IP-adres[256], cookies, … Al deze gegevens zijn wel degelijk gelinkt aan een persoon, maar zonder bijkomende elementen die deze data linken aan het datasubject, kan deze niet geïdentificeerd worden.

---

[251] FRA, *Handbook on European data protection law – 2018 edition*, Luxemburg, Publications Office of the European Union, 2018, p. 83-86.
[252] Zie overweging 27 GDPR; & ARTICLE 29 WORKING PARTY, "Opinion 4/2007 on the Concept of Personal Data", *WP 136*, 20 juni 2007, p.22.
[253] Zie overweging 14 GDPR.
[254] HvJ-EU, Gevoegde zaken C-92/09 & C-93/09, *Volker und Markus Schecke en Hartmut Eifert v. Land Hessen,* [GK], 9 november 2010, paragraaf 52.
[255] FRA, *Handbook on European data protection law – 2018 edition*, Luxemburg, Publications Office of the European Union, 2018, p. 88-90.
[256] IP-adressen zijn door het HvJ erkend als beschermde persoonsgegevens omdat ze het mogelijk maken om natuurlijke personen te identificeren. → HvJ-EU, C-70/10, *Scarlet Extended SA v. Société belge des auterus, compositeurs et éditeurs SCLR (SABAM)*, 24 november 2011, paragraaf 51; Het is bovendien ook niet vereist dat alle noodzakelijke gegevens om te kunnen identificeren bij dezelfde persoon aanwezig of in zijn bezit moeten zijn. Elk stukje van de puzzel, zelfs als het *an sich* niet naar een datasubject wijst, moet worden beschermd als zijnde persoonsgegevens → HvJ, C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, 19 oktober 2016, paragraaf 43.

Overeenkomstig overweging 26 is het niet relevant of het datasubject ook effectief geïdentificeerd wordt. Het is voldoende dat de gegevens die verwerkt worden de mogelijkheid van identificeerbaarheid met zich meebrengen en dat het redelijk te voorzien is dat de gebruikers van de gegevens dit zullen proberen.[257]

Het belangrijkste om te onthouden met betrekking tot het begrip "persoonsgegevens", is dat het zeer breed te interpreteren is. Het was de bedoeling van de Commissie om natuurlijke personen te beschermen met betrekking tot de verwerking van hun persoonsgegevens en om dit te bekomen is een eerste stap natuurlijk om bijna alle mogelijke data die ook maar iets met een persoon te maken heeft, onder deze noemer te doen vallen.

Bijzondere categorieën van persoonsgegevens.

92. **ARTIKEL 9 – VERWERKING VAN BIJZONDERE CATEGORIEËN VAN PERSOONSGEGEVENS**. Artikel 9(1) benoemt 8 categorieën van persoonsgegevens die in principe niet verwerkt mogen worden: (i) ras of etnische afkomst; (ii) politieke opvattingen; (iii) religieuze of levensbeschouwelijke overtuigingen; (iv) het lidmaatschap van een vakbond; (v) genetische gegevens;[258] (vi) biometrische gegevens met het oog op unieke identificatie van een persoon; (vii) medische gegevens;[259] en (viii) gegevens met betrekking tot iemands seksueel gedrag of seksuele geaardheid.

Dit verbod is echter niet absoluut en er zijn uitzonderingen mogelijk waardoor er toch verwerking kan plaatsvinden van de bovengenoemde persoonsgegevens.[260] Hierin wordt voorzien door artikel 9(2)(a) tot (j):

(a) Toestemming:[261] De uitdrukkelijke toestemming van het datasubject kan een rechtvaardigingsgrond voor de verwerking vormen, zolang er geen toepasselijk recht is dat dit onmogelijk maakt. Denk hiervoor voornamelijk aan bepalingen van openbare orde waar een beschermde partij niets over te zeggen heeft, en er dus ook geen afstand van kan doen.
(b) Wanneer de verwerking noodzakelijk is voor de uitoefening van specifieke rechten van het datasubject of de verwerkingsverantwoordelijke op het gebied van het arbeids-, sociale zekerheids- en sociale beschermingsrecht, in zoverre dit door nationaal recht of CAO op grond van dit nationaal recht is toegestaan, en mits passende waarborgen voor de grondrechten van het datasubject zijn getroffen.

[257] Overweging 26 GDPR. → AI vergroot de kans zeer significant dat een gebruiker van dit AI-systeem ten minste de mogelijkheid zal hebben om datasubjecten te identificeren er is een reëel risico op de-anonimisering van persoonsgegevens. Zie supra: Randnummer 54 – Concrete risico's → Het risico op de-anonimiseren.
[258] Zie **artikel 4(13) GDPR**: ""*genetische gegevens": persoonsgegevens die verband houden met de overgeërfde of verworven genetische kenmerken van een natuurlijke persoon die unieke informatie verschaffen over de fysiologie of de gezondheid van die natuurlijke persoon en die met name voortkomen uit een analyse van een biologisch monster van die natuurlijke persoon*";
[259] Zie **artikel 4(15) GDPR**: ""*gegevens over gezondheid": persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven*";
[260] Zie artikel 9(2) – (4) GDPR.
[261] Zie **artikel 4(11) GDPR**: ""*toestemming" van de betrokkene: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt*";

(c) Wanneer de verwerking noodzakelijk is ter bescherming van de vitale belangen van het datasubject of anderen.
(d) De verwerking van persoonsgegevens met betrekking tot politieke, religieuze of levensbeschouwelijke opvattingen door instanties die geen winstoogmerk nastreven, waarbij het datasubject lid is, of was, alsook de persoonsgegevens van personen die regelmatig contact met de instantie zonder winstoogmerk onderhouden.
(e) Wanneer de persoonsgegevens door het datasubject kennelijk openbaar zijn gemaakt.
(f) Wanneer de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering, of wanneer de gerechten handelen in uitvoering van hun taak.
(g) Wanneer de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang. Hierbij mag het evenredigheidsbeginsel niet uit het oog worden verloren en moeten de nodige maatregelen worden getroffen om de grondrechten van het datasubject te waarborgen.
(h) Wanneer de verwerking noodzakelijk is voor preventieve of arbeidsgeneeskunde. Met andere woorden: dokters mogen de medische gegevens van hun patiënten verwerken, zolang ze de voorwaarden en waarborgen uit het 3e lid kunnen garanderen. Die voorwaarden zijn *in casu* dat de verwerker of de verwerkingsverantwoordelijke een beroepsbeoefenaar is die gebonden is door het beroepsgeheim, of door een andere persoon die ook wettelijk tot geheimhouding is gehouden.
(i) Wanneer de verwerking noodzakelijk is voor redenen van volksgezondheid.
(j) Wanneer de verwerking noodzakelijk is met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.

Met betrekking tot de verwerking van genetische, biometrische of medische gegevens kunnen de lidstaten bijkomende voorwaarden of zelfs beperkingen aannemen.

93. Biometrische persoonsgegevens. Biometrische gegevens zijn een belangrijke categorie van data die ook in het voorstel van AI-verordening regelmatig terugkomt.[262] Daar is hun gebruik voor de specifieke toepassing door middel van AI voor real time identificatie op afstand met het oog op de ordehandhaving verboden, tenzij aan de rechtvaardigingsvoorwaarden is voldaan.[263] Deze werden uitgebreid besproken in figuur 8 over de "Risicobeoordeling in het voorstel van AI-verordening". "Biometrische gegevens" in de context van de GDPR worden als volgt gedefinieerd:

> *"(14) "biometrische gegevens": persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens"*[264]

[262] Zie supra: Randnummer 54 – Concrete risico's; 60 – Rechtszekerheid; 61 – Risicogebaseerde aanpak; 68 – Definities; 69 – Artikelen 5 en 6 – Verbod en hoog risico.
[263] Zie artikel 5(1)(d)(i)-(iii) voorstel van AI-verordening.
[264] Zie artikel 4(14) GDPR.

Het is op te merken dat deze definitie identiek is aan de definitie die in het voorstel van AI-verordening wordt aangehouden.[265] Dit is ook in overeenstemming met de bedoeling van de aanvullende werking van het Voorstel ten opzichte van de GDPR, zoals dat wordt vermeld in overweging 7 bij het Voorstel. De GDPR geeft in haar eigen overweging 51 een extra woordje uitleg bij de precieze invulling van "verwerking van biometrische gegevens":

> "De verwerking van foto's mag niet systematisch worden beschouwd als verwerking van bijzondere categorieën van persoonsgegevens, aangezien foto's alleen onder de definitie van biometrische gegevens vallen wanneer zij worden verwerkt met behulp van bepaalde technische middelen die de unieke identificatie of authenticatie van een natuurlijke persoon mogelijk maken."

Het begrip "Verwerking"

94. VERWERKING VAN PERSOONSGEGEVENS.

> *"(2) "verwerking": een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens."*[266]

Het gaat dus om een al dan niet geautomatiseerd proces waarmee om het even welke bewerking van persoonsgegevens wordt uitgevoerd. De lijst die in de bovenstaande definitie uit artikel 3(2) GDPR wordt weergegevens mag niet limitatief worden geïnterpreteerd.[267] Met betrekking tot de verdere invulling van wat nu wel of net niet een verwerking inhoudt, zijn de arresten *Frantisek Ryneš*[268] en *Salvatore Manni*[269] belangrijk om kort te bekijken. In *Frantisek Ryneš* wordt gesteld dat het filmen van personen door middel van beveiligingscamera's op de eigen, privé-eigendom, en het bewaren van die beelden een vorm van automatische verwerking van persoonsgegevens is die in het toepassingsgebied van de GDPR moet vallen.[270] In *Salvatore Manni* stelde het Hof vast dat het bijhouden van persoonsgegevens in het kader van een faillissement, en deze in sommige situaties aan derden verstrekken een daad van verwerking is en dat de instantie die dit doet dus als verwerkingsverantwoordelijke kan worden bestempeld.

---

[265] Ter herinnering: **artikel 3(33) Voorstel van AI-verordening**: ""*biometrische gegevens": persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met betrekking tot de fysieke, fysiologische of gedragsgerelateerde kenmerken van een natuurlijke persoon op grond waarvan eenduidige identificatie van die natuurlijke persoon mogelijk is of wordt bevestigd, zoals gezichtsafbeeldingen of vingerafdrukgegevens*";

[266] Zie artikel 4(2) GDPR

[267] Lees het woord "zoals", wat dus wijst op een lijst ter illustratie van mogelijke bewerkingen die de verwerking van persoonsgegevens zouden kunnen uitmaken.

[268] HvJ-EU, C-212/13, *Frantisek Ryneš v. Úřad pro ochranu osobních údajů*, 11 december 2014, paragraaf 25.

[269] HvJ-EU, C-398/15, *Camera di Commercio,Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 8 maart 2017, paragraaf 35.

[270] Wat dan met overweging 18, waarin staat dat de verwerking van persoonsgegevens, door een natuurlijke persoon voor louter huishoudelijke of persoonlijke doeleinden, en dus geen enkel verband houdend met een professionele activiteit, niet onder het toepassingsgebied van de GDPR moet vallen?

95. **AUTOMATISCHE VERWERKING VAN PERSOONSGEGEVENS.** Overeenkomstig artikel 2(1) van de GDPR zijn het enkel de verwerkingen die ten minste gedeeltelijk automatisch plaatsvinden, die onder het toepassingsgebied *ratione materiae* vallen. Automatische verwerkingen zijn deze waarbij geen menselijke inmenging aanwezig is. *In casu* is het eigenlijk al voldoende dat er een technisch hulpmiddel werd gebruikt om de bewerking die een verwerking uitmaakt tot stand te laten komen. Denk hierbij aan het gebruiken van een PC, smartphone of AI-systeem, dat al dan niet in samenwerking met een mens tot verwerkingen overgaat. Het simpelweg op een webpagina plaatsen van gegevens waarmee een natuurlijke persoon geïdentificeerd kan worden, is volgens het HvJ-EU een op zijn minst een gedeeltelijk automatische verwerking van persoonsgegevens.[271] In de Google Spain-zaak wordt de invulling van wat geautomatiseerde verwerking inhoudt, aangevuld met het geautomatiseerd, onophoudelijk en systematisch zoeken op het internet naar informatie en vervolgens deze gegevens: opvragen, vastleggen, ordenen, op servers bewaren, en soms ook verstrekken of ter beschikking stellen aan derden.[272] Het is daarbij niet van belang dat er bij eender welke stap in dit proces geen onderscheid wordt gemaakt tussen persoonsgegevens en andere, niet aan personen gelinkte data.

Om te voorkomen dat er al te gemakkelijk onder het toepassingsgebied van de GDPR uit te komen valt, door simpelweg een papieren geordend systeem aan te houden, wordt door overweging 15[273] deze optie expliciet toch nog onder de vleugels van GDPR gebracht. Kort samengevat zijn dus ook handmatig bijgehouden dossiers waarin persoonsgegevens vervat zijn, verwerkingen waardoor de verwerkers en verwerkingsverantwoordelijken van deze gegevens zich te houden hebben aan de GDPR.

De begrippen "Verwerkingsverantwoordelijke" en "Verwerker"

96. **TOEPASSINGSGEBIED *RATIONE PERSONAE* - VERWERKERS EN VERWERKINGSVERANTWOORDELIJKEN.** Verwerkers zijn de natuurlijke of rechtspersonen, overheidsinstanties, diensten of andere organen die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerken op een manier die hierboven werd beschreven.[274] De verwerkingsverantwoordelijke is de natuurlijke of rechtspersoon, overheidsinstantie, dienst of eender welk ander orgaan die/dat in samenspraak met een ander of alleen het doel en de middelen van de verwerking zal vaststellen.[275]

De verantwoordelijkheden met betrekking tot het naleven van de bepalingen van de Verordening liggen voornamelijk bij deze twee personen, al dan niet door hen gedeeld.

Verwerkers hebben de verplichting om met betrekking tot de door hen uitgevoerde verwerkingen gepaste technische en organisatorische maatregelen te treffen die, rekening houdend met de aard, omvang, context, verwerkingsdoeleinden en de waarschijnlijkheid van een bepaald risico een beschermingsniveau

[271] HvJ-EU, C-101/01, *Strafzaak tegen Bodil Lindqvist*, 6 november 2003, paragraaf 27.
[272] HvJ-EU, C-131/12, *Google Spain SL en Google Inc. tegen Agencia Española de Protección de Datos (AEPD) en Mario Costeja González*, [GK], 13 mei 2014, paragraaf 28.
[273] **Overweging "(15)** *Om te voorkomen dat een ernstig risico op omzeiling zou ontstaan, dient de bescherming van natuurlijke personen technologieneutraal te zijn en mag zij niet afhankelijk zijn van de gebruikte technologieën. De bescherming van natuurlijke personen dient te gelden bij zowel geautomatiseerde verwerking van persoonsgegevens als handmatige verwerking daarvan indien de persoonsgegevens zijn opgeslagen of bedoeld zijn om te worden opgeslagen in een bestand. Dossiers of een verzameling dossiers en de omslagen ervan, die niet volgens specifieke criteria zijn gestructureerd, mogen niet onder het toepassingsgebied van deze richtlijn te vallen*"
[274] Zie artikel 4(8) GDPR.
[275] Zie artikel 4(7) GDPR.

kunnen waarborgen dat, naargelang de situatie kan bestaan uit: (a) pseudonimisering of versleuteling van de gegevens; (b) het vermogen om permanent de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen te garanderen; (c) het vermogen om bij een incident de beschikbaarheid en toegang tot de gegevens tijdig te herstellen; (d) een procedure voor periodieke test-, beoordelings- en evaluatiemomenten van de maatregelen.[276 & 277]

Bijkomend moeten ze in sommige gevallen ook een Functionaris voor Gegevensbescherming of "*Data Protection Officer"* (DPO)[278] aanduiden en in geval van een "*data breach*" de verwerkingsverantwoordelijke op de hoogte stellen.[279]

Verwerkingsverantwoordelijken zijn de personen of instanties die het voor het zeggen hebben met betrekking tot de verwerkingen die door henzelf of voor hen, door verwerkers, worden uitgevoerd. Het zijn zij die beslissen over de categorieën van persoonsgegevens die verwerkt worden, de manier waarop deze verwerking zal plaatsvinden, wie er toegang toe heeft en voor welke doeleinden er verwerkt moet worden. Dit wil dus ook zeggen dat ze *de facto* het aanspreekpunt zijn in geval van de uitoefening van de rechten van datasubjecten die hieronder nog besproken zullen worden.[280] Tot hun specifieke verplichtingen behoren: het implementeren van gepaste technische en organisatorische maatregelen om de bescherming van persoonsgegevens te garanderen;[281] het geven van instructies en het uitoefenen van toezicht op de verwerker;[282] het op de hoogte stellen van de nationale toezichthoudende autoriteit in geval van een "*data breach*";[283]en het op de hoogte stellen van het datasubject in bepaalde, hoog-risico gevallen van *data breaches*.[284]

De onderlinge relatie tussen een verwerkingsverantwoordelijke en een verwerker wordt contractueel geregeld, waarbij er door de verwerker geen enkel gebruik van de persoonsgegevens mag plaatsvinden zonder uitdrukkelijke opdracht van de verwerkingsverantwoordelijke.[285] Verwerkt de verwerker de persoonsgegevens verder dan hem expliciet werd opgedragen, dan loopt hij het risico zelf verwerkingsverantwoordelijke te worden voor die verwerkingen en er dus ook de eindverantwoordelijkheid voor op zich te moeten nemen.

97. JOINT CONTROLLERS. In sommige gevallen zijn er twee of meerdere verwerkingsverantwoordelijken. Er wordt dan van "gezamenlijke verwerkingsverantwoordelijken" gesproken.[286] In dit geval bepalen de partijen in samenspraak de doeleinden en middelen van de verwerking. Ze dragen dus gezamenlijk de verantwoordelijkheid, maar kunnen deze contractueel ook

[276] Zie artikel 28 tot 32 GDPR.
[277] Dit wordt onder het voorstel van AI-verordening verwoord als "*nauwkeurigheid, robuustheid en cyberbeveiliging*" en wordt onder andere door artikel 15 van het voorstel behandelt.
[278] Zie artikel 37 GDPR.
[279] Zie artikel 33(2) GDPR.
[280] Zie infra: Randnummer 106 – Rechten van datasubjecten.
[281] Zie artikel 24(1) GDPR.
[282] Zie artikel 29 GDPR.
[283] Zie artikel 33(1) GDPR.
[284] Zie artikel 34 GDPR
[285] Zie artikel 28(3) GDPR juncto artikel 29 GDPR.
[286] Zie artikel 26 GDPR.

onderling verdelen. Hiervoor is het echter wel vereist dat de datasubjecten weten bij wie ze voor welke verwerkingen terecht kunnen.[287]

Gegevensbeschermingseffectenbeoordeling, "Data Protection Impact Assessment" of simpelweg "DPIA"

98. DPIA.

> "Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen voert de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden."[288]

In bepaalde gevallen is er de verplichting voor de verwerkingsverantwoordelijke om voorafgaand aan de implementatie van de verwerking een impactbeoordeling te doen. Er moet worden nagegaan in hoeverre de verwerking een risico kan inhouden voor de rechten en vrijheden van natuurlijke personen.[289] Een DPIA is onder andere verplicht in de gevallen die expliciet benoemd worden in artikel 35(3) GDPR[290], maar ook in de gevallen waarin de toezichthoudende autoriteit, overeenkomstig haar verplichting onder artikel 35(5), bepaald heeft dat dergelijke verwerkingen een voorafgaande DPIA vereisen.[291]

Wanneer de DPIA er op uitkomt dat de verwerking in kwestie een hoog risico zou kunnen inhouden, moet de verwerkingsverantwoordelijke hierover de toezichthoudende autoriteit raadplegen. Deze raadpleging moet geschieden om zich ervan te verzekeren dat er voldoende maatregelen ter bescherming van de belangen van datasubjecten werden getroffen. Indien de toezichthoudende autoriteit van mening is dat hieraan niet is voldaan, kan ze al haar onderzoeksbevoegdheden, [292]

---

[287] Zie artikel 26(2) GDPR.
[288] Zie artikel 35(1) GDPR.
[289] Denk hierbij zeker ook terug aan de verplichting van gebruikers van AI-systemen om een gegevensbeschermingseffectenbeoordeling uit te voeren in geval van implementering van Hoog-risico toepassingen. → Artikel 29(6) voorstel van AI-verordening. → Zie supra: Randnummer 67 – Inleiding en overzicht; voetnoot 162.
[290] **Artikel 35(3) GDPR.** "*Een gegevensbeschermingseffectbeoordeling als bedoeld in lid 1 is met name vereist in de volgende gevallen: **a)** een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen; **b)** grootschalige verwerking van bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9, lid 1, of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10; of **c)** stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.*"
[291] Ter illustratie kunnen via volgende links enkele uitvoeringsbesluiten/beslissingen van verschillende toezichthoudende autoriteiten worden ingekeken:
De beslissing van de Vlaamse Toezichtcommissie voor de verwerking van persoonsgegevens in uitvoering van haar verplichting onder artikel 35(5) GDPR is terug te vinden via volgende link: https://overheid.vlaanderen.be/sites/default/files/media/VTC/VTC_O_2020_01_DPIA_lijsten_v1_voor_web.pdf?timestamp=1589396929; Het besluit van de Nederlandse Autoriteit Persoonsgegevens in uitvoering van haar verplichting onder artikel 35(5) GDPR is terug te vinden via volgende link: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf;
[292] Zie artikel 58(1) GDPR.

corrigerende bevoegdheden[293] of autorisatie- en adviesbevoegdheden[294] uitoefenen, naargelang de situatie dat zou vereisen.[295 & 296]

De begrippen "Geautomatiseerde individuele beslissingen" en "Profilering"

99. **GEAUTOMATISEERDE INDIVIDUELE BESLISSINGEN.** Dit zijn beslissingen die automatisch worden gemaakt door het verwerkende systeem, zonder dat er enige menselijke inmenging plaatsheeft. Opvallend is dat dit begrip niet wordt gedefinieerd in artikel 4, terwijl "profilering", hetgeen een verwerking is die onder de overkoepelende term van geautomatiseerde individuele beslissingen valt, deze eer wel toekomt.[297]

Datasubjecten genieten het recht om aan dergelijke beslissingen niet te worden onderworpen indien ze voor hen bindende rechtsgevolgen met zich meebrengen, of indien ze hen op een andere manier aanmerkelijk treffen.[298] Zoals bijna altijd, zijn er op deze strenge beperking van de mogelijkheid op verwerking enkele uitzonderingen.[299]

De invulling van het verbod op automatische individuele beslissingen wordt door overweging 71 verduidelijkt: zo mag er geen automatische beslissing plaatsvinden met betrekking tot bijvoorbeeld de automatische weigering van een kredietaanvraag of met betrekking tot de verwerking van sollicitaties.

100. **PROFILERING.** Dit is een vorm van geautomatiseerde verwerking van persoonsgegevens waarbij de persoonlijke kenmerken van een datasubject worden beoordeeld. Het gaat hier met name om kenmerken met betrekking tot prestaties, gezondheid, interesses, betrouwbaarheid, gedrag, … Dit soort verwerking brengt logischerwijze en hele resem extra risico's met zich mee en wordt daarom in principe ook verboden. Dezelfde uitzonderingen als op de "gewone" geautomatiseerde individuele beslissingen zijn van toepassing.

[293] Zie artikel 58(2) GDPR.
[294] Zie artikel 58(3) GDPR.
[295] Zie artikel 36(2) GDPR.
[296] Hiervan bestaat onder regime van het voorstel van AI-verordening een gelijkaardige procedure waarbij de aanbieder van een hoog-risico AI-toepassing de verplichting heeft om de implementering ervan in een lidstaat te melden aan de toezichthoudende autoriteit; Zie artikel 22 van het voorstel van AI-verordening.
[297] Zie artikel 4(4) GDPR.
[298] Zie artikel 22(1) GDPR.
[299] Zie **artikel 22 (2) GDPR**: "*Lid 1 geldt niet indien het besluit: **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 die op de verwerkingsverantwoordelijke van toepassing is en die ook voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene; of **c)** berust op de uitdrukkelijke toestemming van de betrokkene*."

2.2.4. Tussentijdse terugblik

101. **TERUGBLIK.** In de twee eerste hoofdstukken van het tweede deel werd tot nu toe besproken wat het recht op bescherming van persoonsgegevens nu net inhoudt en hoe het zich verhoudt tot het recht op privacy. Het werd duidelijk dat, hoewel ze sterk aan elkaar gelinkt zijn, er toch een zeker onderscheid gemaakt kan worden en dat dit onderscheid ook door wetgeving, rechtspraak en rechtsleer wordt erkend. Met deze conclusies werden de subvragen die peilden naar de inhoud van deze rechten beantwoord.

Omdat het recht op bescherming van persoonsgegevens niet pas op 25 mei 2018 werd geboren, maar al een langere geschiedenis kent, werd deze kort besproken aan de hand van enkele andere toepasselijke wetgevende kaders die gelijktijdig spelen op het Europese toneel.

Hierna werd de geschiedenisles afgesloten en moest die de spotlights afstaan aan de toepasselijke terminologie. Onder titel 1.2.3. werden onder andere de begrippen: persoonsgegevens, verwerking en geautomatiseerde individuele beslissingen verklaard.

Uit die definiëringen is het duidelijk af te leiden dat verschillende AI-toepassingen onder het toepassingsgebied van de GDPR kunnen vallen. Veel systemen doen namelijk aan "verwerkingen" van al dan niet bijzondere categorieën van "persoonsgegevens" zoals deze termen werden afgelijnd in bovenstaand hoofdstuk.

2.3. Hoofdstuk 3. De krachtlijnen van de GDPR[300]

102. **INLEIDING.** Terwijl de belangrijkste krachtlijnen waarop het voorstel van AI-verordening werd gebaseerd moesten worden gezocht in de voorbereidende werken, de toelichting en de overwegingen, maakt de tekst van GDPR het ons aanzienlijk makkelijker door haar belangrijkste principes op te sommen in artikel 5. De principes zijn echter niet het enige waarvoor het GDPR-regime bekend is geworden. Zo zijn er ook de rechten van datasubjecten[301], de verwerkingsgronden waarop een verwerking kan worden gebaseerd met in het bijzonder de belangrijke plaats van toestemming in het regime[302] en de wereldbekende – en gevreesde – monsterboetes[303], waar reeds enkele bedrijven tot hun schade en schande mee in aanraking zijn gekomen.[304]

Dit hoofdstuk zal voornamelijk focussen op de principes waaraan de verwerking van persoonsgegevens onder het GDPR-regime steeds moet voldoen, de rechten van datasubjecten met betrekking tot de verwerking van hun gegevens en de verschillende verwerkingsgronden met een extra blik op de invulling van het concept "toestemming". De monsterboetes, hoewel ze een zeer belangrijk drukkingsmiddel vormen, zijn mijns inziens niet van dergelijke aard dat ze als een krachtlijn van de Algemene Verordening betreffende Gegevensbescherming kunnen worden gezien.[305]

---

[300] P. VOIGT & A. VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR) – A Practical Guide*, Cham, Springer, 2017, 383p.; C. KUNER, L.A. BYGRAVE, C. DOCKEY, & L. DRECHSLER, (eds.), *The EU General Data Protection Regulation (GDPR): a Commentary*, Oxford, Oxford University Press, 2020, 1393p.; IT GOVERNANCE, *EU General Data Protection Regulation (GDPR): an implementation and compliance guide*, Cambridgeshire, IT Governance Publishing Ltd, 2019, 390p.

[301] Zie infra: Randnummer 103 – Beginselen inzake verwerking van persoonsgegevens.

[302] Zie infra: Randnummer 104 – Rechtmatigheid van de verwerking; & 105 – Toestemming.

[303] Zie artikel 83 GDPR.

[304] G. SOMERS & D. FITEN, "2 jaar GDPR: Een overzicht van handhaving, waarschuwingen en boetes", *Timelex.eu* 8 juli 2020, https://www.timelex.eu/nl/blog/2-jaar-gdpr-een-overzicht-van-handhaving-waarschuwingen-en-boetes; H.W. ROERDINK & C.A.M. VAN DE BUNT, "Boetes onder het regime van de AVG", *P&I* (afl. 6) 6 december 2019, p.252-263, http://www.uitgeverijparis.nl/scripts/read_article_pdf_li.php?id=1001451801&cks=d08df3f5afc3aff42c970faaa4a024649e2bddd7; CLAEYS & ENGELS, "GDPR: monsterboete van 35 miljoen euro voor Duits servicecenter van H&M", *LegalNews.be* 13 november 2020, https://legalnews.be/arbeid-sociale-zekerheid/gdpr-monsterboete-van-35-miljoen-euro-voor-duits-servicecenter-van-hm-claeys-engels/; …

[305] Ter herinnering wordt hier kort verwezen naar het relevante artikel om duidelijk te maken wat, met welke boete gesanctioneerd kan worden door toepassing van **artikel 83 GDPR**: *"[…] **2**. Administratieve geldboeten worden, naargelang de omstandigheden van het concrete geval, opgelegd naast of in plaats van de in artikel 58, lid 2, onder a) tot en met h) en onder j), bedoelde maatregelen. Bij het besluit over de vraag of een administratieve geldboete wordt opgelegd en over de hoogte daarvan wordt voor elk concreet geval naar behoren rekening gehouden met het volgende:[…]*
***3**. Indien een verwerkingsverantwoordelijke of een verwerker opzettelijk of uit nalatigheid met betrekking tot dezelfde of daarmee verband houdende verwerkingsactiviteiten een inbreuk pleegt op meerdere bepalingen van deze verordening, is de totale geldboete niet hoger dan die voor de zwaarste inbreuk.*
***4**. Inbreuken op onderstaande bepalingen zijn overeenkomstig lid 2 onderworpen aan administratieve geldboeten tot 10 000 000 EUR of, voor een onderneming, tot 2 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is: […]*
***5**. Inbreuken op onderstaande bepalingen zijn overeenkomstig lid 2 onderworpen aan administratieve geldboeten tot 20 000 000 EUR of, voor een onderneming, tot 4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is: […]*
***6**. Niet-naleving van een bevel van de toezichthoudende autoriteit als bedoeld in artikel 58, lid 2, is overeenkomstig lid 2 van dit artikel onderworpen aan administratieve geldboeten tot 20 000 000 EUR of, voor een onderneming, tot 4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit cijfer hoger is.*
[…]"

103. **BEGINSELEN INZAKE VERWERKING VAN PERSOONSGEGEVENS.**[306] De belangrijkste principes waaraan elke verwerking van persoonsgegevens moet voldoen – in de mate van het mogelijke – zijn diegenen die artikel 5 oplegt. Het gaat in casu om zes beginselen die aan de basis liggen van zowel de GDPR als alle latere wetgeving betreffende gegevensbescherming.[307 & 308] Het is mogelijk voor de lidstaten en voor de Unie om beperkingen op deze principes toe te staan onder drie cumulatieve voorwaarden die besproken worden onder artikel 23(1) GDPR: (i) de beperkingen moeten bij wet zijn toegelaten; (ii) ze moeten een legitiem doel nastreven;[309] en (iii) ze moeten noodzakelijk en proportioneel zijn, zonder de wezenlijke inhoud van de grondrechten en fundamentele vrijheden van datasubjecten te schenden.

De zes beginselen van toepassing op elke verwerking van persoonsgegevens zijn:

- (a) "***Rechtmatigheid, behoorlijkheid en transparantie***":[310]

Deze drie delen van het eerste beginsel zijn door hun onderlinge samenhang in het eerste punt onder artikel 5(1) GDPR samengesmolten. Er is echter wel een duidelijk onderscheid te maken tussen elk van hen.

Rechtmatigheid heeft betrekking tot de grond waarop een verwerking van persoonsgegevens wordt gebaseerd. Deze vereiste wordt uitvoerig behandeld door artikel 6, waarin limitatief alle gronden van rechtmatige verwerking worden genoemd.

---

[306] **Artikel 5 GDPR**: "*Beginselen inzake verwerking van persoonsgegevens* ***1.*** *Persoonsgegevens moeten:* ***a)*** *worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is („rechtmatigheid, behoorlijkheid en transparantie");* ***b)*** *voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd („doelbinding");* ***c)*** *toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt („minimale gegevensverwerking");* ***d)*** *juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren („juistheid");* ***e)*** *worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig artikel 89, lid 1, mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen („opslagbeperking");* ***f)*** *door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging („integriteit en vertrouwelijkheid").* ***2.*** *De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 en kan deze aantonen („verantwoordingsplicht")."*

[307] FRA, *Handbook on European data protection law – 2018 edition*, Luxemburg, Publications Office of the European Union, 2018, p. 116.

[308] Dit wil dus ook zeggen de voor gegevensbescherming relevante bepalingen in het voorstel van AI-verordening.

[309] **Artikel 23(1)** … ***a)*** *de nationale veiligheid;* ***b)*** *landsverdediging;* ***c)*** *de openbare veiligheid;* ***d)*** *de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;* ***e)*** *andere belangrijke doelstellingen van algemeen belang van de Unie of van een lidstaat, met name een belangrijk economisch of financieel belang van de Unie of van een lidstaat, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;* ***f)*** *de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;* ***g)*** *de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen;* ***h)*** *een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de in de punten a), tot en met e) en punt g) bedoelde gevallen;* ***i)*** *de bescherming van de betrokkene of van de rechten en vrijheden van anderen;* ***j)*** *de inning van civielrechtelijke vorderingen.*

[310] FRA, Handbook on European data protection law – 2018 edition, Luxemburg, Publications Office of the European Union, 2018, p. 117-122.

Verwerkingen die op een rechtmatige basis worden uitgevoerd moeten ook behoorlijk en eerlijk zijn. Deze vereiste slaat voornamelijk op de onderlinge relatie tussen de verwerkingsverantwoordelijke en het datasubject. *In concreto* komt het erop neer dat een verwerkingsverantwoordelijke in de mate van het mogelijke open moet zijn over de verwerkingen die worden uitgevoerd, welke gegevens er worden verwerkt, op welke manier, of zijn er externe verwerkers aangesteld zijn, … Ook moet hij kunnen aantonen dat zijn handelingen in overeenstemming zijn met de regels van de GDPR. Een veruitwendiging van dit principe volgt later in de Verordening met artikel 24(1).

Heel nauw samenhangend met de behoorlijkheid, is de vereiste van transparantie. Dit gaat net iets verder dan aan kunnen tonen dat de verwerkingen GDPR-conform verlopen. De verwerkingsverantwoordelijke moet ook redelijke maatregelen nemen om datasubjecten op de hoogte te houden van hoe hun gegevens worden gebruikt. De transparantievereiste kan op verschillende momenten in de relatie plaatshebben. Denk hierbij voornamelijk aan de banners die je ziet wanneer je op de startpagina van een website komt, maar ook aan de mails die niemand ooit leest, maar waarin je zou kunnen uitschrijven, of de mogelijkheid om ten allen tijde, helemaal onderaan een webpagina, de privacy policy te lezen van de verwerkingsverantwoordelijke die achter de website zit. Artikel 12 vult dit principe verder in en maakt er een effectief recht van het datasubject van. Naast het recht op transparante informatie en communicatie zijn nagenoeg alle rechten van datasubjecten in meer of mindere mate gelinkt aan de beginselen van behoorlijkheid en transparantie.

- (b) "***Doelbinding***":[311]

Doelbinding, waarnaar in de praktijk couranter wordt verwezen door middel van de Engelse term "*purpose limitation*", heeft betrekking tot de verplichting van verwerkingsverantwoordelijken om, voorafgaand aan de verzameling van persoonsgegevens, op uitdrukkelijk omschreven manier vast te leggen welke welbepaalde gegevens, voor welke gerechtvaardigde doeleinden zullen worden verzameld, en zich vervolgens in de verwerkingen ook te beperken tot enkel met deze doeleinden verenigbare handelingen.

Een verwerkingsverantwoordelijke mag dus in principe niet zomaar *en masse* gegevens beginnen verzamelen met het oog op Big Data[312], voor de simpele reden dat deze later wel eens van pas zouden kunnen komen. Het principe van doelbinding verbiedt willekeur omtrent de verwerking van persoonsgegevens. Dit wil echter niet zeggen dat het onmogelijk is om reeds verzamelde gegevens, voor een ander doeleinde opnieuw te verwerken. Er is dan enkel een nieuwe, afzonderlijke grond van rechtmatigheid nodig.

[311] FRA, *Handbook on European data protection law – 2018 edition*, Luxemburg, Publications Office of the European Union, 2018, p. 122-125; Article 29 Working Party, *Opinion 3/2013 on purpose limitation*, WP 203, 2 april 2013.
[312] Zie supra: Randnummer 19 – Big Data, Algoritmen en AI.

- (c) "***Minimale gegevensverwerking***":[313]

Het principe van "*data minimisation*" maakt dat de verwerking moet worden beperkt tot hetgeen noodzakelijk en voldoende is om het vooropgestelde, legitieme doel te bereiken. Het is ook de bedoeling dat de verwerkingsverantwoordelijke omzichtig omspringt met de keuze om tot verwerken over te gaan. Als het redelijkerwijze mogelijk zou zijn om hetzelfde gevolg te bekomen, zonder dat er daarvoor een verwerking van persoonsgegevens nodig zou zijn, dan moet de voorkeur worden gegeven aan dat alternatief. Het is duidelijk dat massaal verzamelen van gegevens met betrekking tot elektronische communicatie van alle individuen, zonder enig onderscheid, overdreven en disproportioneel is, zelfs wanneer het wel een legitiem doel nastreeft, zoals de bestrijding van georganiseerde misdaad en terrorisme. Dit voorbeeld is niet zomaar lukraak gekozen. Het is namelijk gebaseerd op het mijlpaalarrest in de zaak: *Digital Rights Ireland*.[314]

- (d) "***Juistheid***":[315]

Het is niet de bedoeling dat er verwerkingen van foutieve persoonsgegevens plaatsvinden. Voor vanzelfsprekende redenen kan dit leiden tot problematische gevolgen. Hetzij in het licht van geautomatiseerde beslissingen[316], hetzij bij gewone normale beslissingsprocessen die per definitie steeds gebeuren op basis van de beschikbare informatie. De concrete uitoefening van dit principe kan door het datasubject zelf gebeuren op basis van het recht op informatie en toegang;[317] het recht op inzage;[318] en de rechten op rectificatie en wissing van gegevens.[319]

- (e) "***Opslagbeperking***": [320]

Vanaf het moment dat de persoonsgegevens verzameld zijn, is de verwerkingsverantwoordelijke verplicht om de opslag van de data die identificatie mogelijk maakt[321] op een zodanige manier te regelen dat deze niet langer wordt bijgehouden dan noodzakelijk is voor de vooropgestelde doeleinden.[322]

---

[313] FRA, *Handbook on European data protection law – 2018 edition*, Luxemburg, Publications Office of the European Union, 2018, p. 125-127.
[314] HvJ-EU, Gevoegde zaken C-293/12 en C-594/12*, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ierland* & *Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl e.a.*,[GK], 8 april 2014, paragrafen 44 en 57.
[315] FRA, Handbook on European data protection law – 2018 edition, Luxemburg, Publications Office of the European Union, 2018, p. 127-128.
[316] Zie supra: Randnummer 99 – Geautomatiseerde individuele beslissingen & 100 – Profilering.
[317] Zie artikel 13 & 14 GDPR.
[318] Zie artikel 15 GDPR.
[319] Zie artikelen 16 & 17 GDPR.
[320] FRA, *Handbook on European data protection law – 2018 edition*, Luxemburg, Publications Office of the European Union, 2018, p. 129-130.
[321] Hoe speelt pseudonimisering en anonimisering in dit principe? Mogen gegevens die niet rechtstreeks identificeren dan wel langer worden bijgehouden? **Artikel 4(5) GDPR**: *""pseudonimisering": 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;"* Wanneer gegevens geanonimiseerd kunnen worden, is de GDPR niet van toepassing. Anonimisering wordt door **overweging 26** als volgt beschreven: *"… gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon of op persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is."*
[322] Zie overweging 39 GDPR.

Het archiveren in het algemeen belang voor historisch onderzoek of statistische doeleinden kan wel mits de passende technische en organisatorische maatregelen worden genomen om de rechten en vrijheden van het datasubject te beschermen.

- (f) "***Integriteit en vertrouwelijkheid***":[323]

Het is de taak van de verwerkingsverantwoordelijke om erop toe te zien dat de verwerkingen van persoonsgegevens gebeuren in een situatie die passend beveiligd is. Het is uiteraard niet de bedoeling dat derden toegang kunnen krijgen tot de data waardoor dus een ongeoorloofde of onrechtmatige verwerking zou kunnen plaatsvinden. Hiertoe moeten wederom passende technische en organisatorische maatregelen worden getroffen, die er ook toe strekken het onopzettelijk verlies, vernietiging of beschadiging van de datasets tegen te gaan.

(2) "**Verantwoording**":[324]

Bovenop de voorgaande zes principes is er ook nog de verplichting voor de verwerkingsverantwoordelijke om de naleving van al deze beginselen aan te tonen.[325]

Deze verantwoordingsplicht onderscheidt zich ogenschijnlijk van de andere beginselen in die zin dat de voorgaanden allemaal betrekking hebben op de verwerking van persoonsgegevens, zonder specifiek een verplichting aan één bepaalde persoon hiertoe op te leggen. *De facto* zal de beslissingsbevoegdheid omtrent alle beginselen bij de verwerkingsverantwoordelijke liggen, terwijl de verantwoordelijkheid voor de effectieve implementatie ervan eerder aan de verwerker kan worden toegerekend.

Hiertegenover staat de verantwoordingsplicht, die duidelijk en ondubbelzinnig aan de verwerker wordt toegewezen.[326] Dit moet echter genuanceerd worden omdat ook verwerkers in sommige gevallen verantwoording moeten afleggen omdat ze wel degelijk verplichtingen hebben die er nauw mee verbonden zijn.[327]

De manier waarop aangetoond kan worden dat een verwerkingsverantwoordelijke haar verwerkingen GDPR-conform laat verlopen kan verschillende vormen aannemen, de meest duidelijke is iets verder in de Verordening terug te vinden onder artikel 35 in de vorm van een DPIA.[328]

104. **RECHTMATIGHEID VAN DE VERWERKING.** De invulling van het eerste beginsel wordt verzorgd door artikel 6, dat een limitatieve lijst opstelt van verwerkingsgronden. Hoewel de tekst van de verordening duidelijk stelt dat ten minste één van de verwerkingsgronden van toepassing moet zijn om over GDPR-conformiteit te kunnen spreken, moet dit onder invloed van 6(2) direct genuanceerd worden. Het is

[323] FRA, *Handbook on European data protection law – 2018 edition*, Luxemburg, Publications Office of the European Union, 2018, p. 131-134.
[324] FRA, *Handbook on European data protection law – 2018 edition*, Luxemburg, Publications Office of the European Union, 2018, p. 134-137.
[325] Zie artikel 5(2) GDPR.
[326] Zie artikel 24 GDPR.
[327] Denk hierbij aan de verplichting om afdoende maatregelen te treffen ter bescherming van de persoonsgegevens (artikel 28(3)(c) juncto artikel 32 GDPR), een register van de verwerkingsactiviteiten bij te houden (artikel 30(1) GDPR), een DPO aan te stellen wanneer nodig (artikel 37(1) GDPR), …
[328] Zie ook supra: Randnummer 98 – DPIA.

namelijk mogelijk voor de lidstaten om in de gevallen onder 6(1)(c) en (e), meer specifieke, strengere voorwaarden op te leggen om verwerkingen op die grond toe te laten.

De rechtmatigheid van de verwerking van bijzondere categorieën van persoonsgegevens wordt geregeld door artikel 9.[329] De verwerking van deze categorieën van gegevens is in principe verboden, maar kan toch worden toegestaan onder de voorwaarden bepaald in (2) en besproken onder randnummer 92.

Dat gezegd zijnde, zijn de verwerkingsgronden onder artikel 6 de volgende:

> *"a) de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;*
>
> *b) de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;*
>
> *c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;*
>
> *d) de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;*
>
> *e) de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;*
>
> *f) de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is."*[330]

105. TOESTEMMING.[331] Hoewel elk van bovenstaande verwerkingsgronden op zich uiteraard voldoende is om als basis te dienen voor verwerkingshandelingen door een verwerkingsverantwoordelijke of verwerker, wordt in de Verordening in het bijzonder de aandacht gevestigd op het concept "toestemming".

Om een rechtsgeldige toestemming te hebben moet het gaan om vrije, geïnformeerde, specifieke en ondubbelzinnige toestemming. Met betrekking tot deze 4 voorwaarden zijn reeds ettelijke liters inkt gevloeid en werden ook al verschillende arresten geveld door het Hof van Justitie.[332] De precieze invulling

[329] Zie supra: Randnummer 92 - artikel 9 – Verwerking van bijzondere categorieën van persoonsgegevens.
[330] Zie artikel 6(1) GDPR.
[331] FRA, *Handbook on European data protection law – 2018 edition*, Luxemburg, Publications Office of the European Union, 2018, p. 142-149.
[332] Ter informatie:
Met betrekking tot vrije toestemming: Groep artikel 29, *Advies 15/2011 over de definitie van "toestemming"*, WP 187, Brussel, 13 juli 2011.
Met betrekking tot geïnformeerde toestemming: Groep artikel 29, *Werkdocument inzake de verwerking van persoonsgegevens betreffende gezondheid in elektronische medische dossiers*, WP 131, Brussel, 15 februari 2007.

van dit begrip zal verder niet uit de doeken worden gedaan omdat dit op zich zonder problemen een scriptieonderwerp kan uitmaken en de invulling ervan geen echte verandering zal ondergaan in het licht van de toekomstige AI-verordening.

106. DE RECHTEN VAN DATASUBJECTEN. Zoals onder randnummer 103 reeds duidelijk werd, zijn de rechten van de datasubjecten voornamelijk de middelen waarmee een datasubject de beginselen van verwerking van persoonsgegevens kan controleren en doen uitwerking krijgen.

Wanneer een bepaalde verwerking van persoonsgegevens niet GDPR-conform is, wat dus wilt zeggen dat ze niet overeenkomstig de beginselen van verwerking is, dan kan een datasubject hierop uitkomen door haar rechten uit te oefenen. Ofwel rechtstreeks bij de betrokken verwerker of verwerkingsverantwoordelijke, ofwel, indien dat niet het gewenste resultaat heeft via een klacht bij de bevoegde autoriteit op nationaal niveau.[333] Deze heeft dan op haar beurt de mogelijkheid om sancties[334] op te leggen die kunnen ingevuld worden met de opties waartoe artikel 58(2) haar machtigt[335] met als meest tot de verbeelding sprekende, de monsterboetes die kunnen oplopen tot 20.000.000 euro of 4% van de totale, globale jaarlijkse omzet van het voorgaande boekjaar.[336]

Voor deze thesis heeft het geen echte meerwaarde om alle rechten van datasubjecten in detail te bespreken. De uitwerking hieromtrent wordt beperkt tot onderstaande figuur die een overzichtelijk beeld schetst van de artikelen 12 tot en met 22.

Met betrekking tot specifieke toestemming: HvJ-EU, zaak C-543/09, *Deutsche Telekom AG/Bondsrepubliek Duitsland*, 5 mei 2011, paragrafen 53 & 54; HvJ-EU, zaak C-536/15, *Tele2 (Nederland) BV e.a./Autoriteit Consument en Markt (ACM)*, 15 maart 2017; **Met betrekking tot ondubbelzinnige toestemming**: HvJ-EU, zaak C-536/15, *Tele2 (Nederland) BV e.a./Autoriteit Consument en Markt (ACM)*, 15 maart 2017, paragraaf 36.

[333] Zie artikel 77 juncto overweging 141 GDPR.

[334] Zie artikel 58(2) juncto overweging 129 GDPR.

[335] Zie artikel 58(2)(a) tot en met (j) GDPR.

[336] Zie artikel 83 juncto overwegingen 148 + 150-151 GDPR.

De rechten van datasubjecten onder het GDPR-regime			
Rechten van het datasubject op …	***Informatie***	Artikel 12(5) & (7), 13 & 14 GDPR.	Men heeft het recht om informatie te krijgen omtrent de verwerking van zijn of haar persoonsgegevens. Dit kan automatisch, op initiatief van de verwerkingsverantwoordelijke of verwerker door middel van een banner of privacy policy, of na een vraag die van het datasubject zelf uitgaat. Er wordt een onderscheid gemaakt tussen verwerkingen met betrekking tot gegevens die het datasubject zelf ter beschikking heeft gesteld en verwerkingen met betrekking tot gegevens over het datasubject die via een andere weg bij de verwerker / verwerkingsverantwoordelijke zijn geraakt.
	Inzage	Artikel 15 GDPR.	Het datasubject heeft het recht om te weten of zijn of haar gegevens verwerkt worden en zo ja, welke persoonsgegevens er dan effectief verwerkt worden. Ook moet informatie worden verstrekt over waar de persoonsgegevens vandaan komen indien ze niet door het datasubject zelf werden bezorgd en wat de doeleinden van de verwerking zijn.
	Rectificatie	Artikel 16 GDPR.	De betrokkenen hebben het recht om te eisen dat de persoonsgegevens die aan hen gelinkt zijn, correct zijn. Ze kunnen na inzage dus ook vragen dat de verwerker / verwerkingsverantwoordelijke de haar beschikbare data verbetert of aanvult zodat onvolledige gegevens niet voor nadelige gevolgen zouden kunnen zorgen.
	Vergetelheid	Artikel 17 GDPR.	In bepaalde gevallen heeft de natuurlijke persoon achter de verwerkte gegevens het recht om de wissing ervan te vragen. In deze gevallen is het dus aan de verwerker / verwerkingsverantwoordelijke om zonder overdreven vertraging deze eis in te willigen en de data te verwijderen.
	Beperking van verwerking	Artikel 18 GDPR.	In bepaalde gevallen, met name wanneer niet de vergetelheid wordt gevraagd, kan het datasubject ook opteren om de gevallen waarin de verwerking van zijn of haar persoonsgegevens plaatsvindt te beperken.
	Overdraagbaarheid	Artikel 20 GDPR.	Inzage en informatie moet in een dergelijke vorm worden gedaan, dat het datasubject haar persoonsgegevens quasi letterlijk met zich mee kan nemen en desgevallend aan een andere verwerker / verwerkingsverantwoordelijke overhandigen. *In casu* wil dit dus zeggen dat een Word-, PDF- of gelijkaardig bestand ter beschikking gesteld zal moeten worden.
	Bezwaar	Artikel 21 GDPR.	Elk datasubject heeft het recht om te protesteren tegen de verwerking van zijn of haar persoonsgegevens en de verwerker / verwerkingsverantwoordelijke zal aan dit protest gehoor moeten geven tenzij ze met legitieme gronden op de proppen kunnen komen die de rechten en vrijheden van het datasubject in ondergeschikte rang duwen.
	Niet onderworpen te zijn aan bindende geautomatiseerde beslissingen	Artikel 22 GDPR.	In principe heeft eenieder het recht om niet gebonden te worden door een geautomatiseerde individuele beslissing die ten minste een zekere uitwerking op hem of haar zal hebben. Hier bestaan echter enkele uitzonderingen op die reeds werden besproken onder randnummer 99.

Figuur 22. De rechten van datasubjecten onder het GDPR-regime.

2.4. Hoofdstuk 4. Relevante bepalingen met betrekking tot AI

107. INLEIDING & OVERZICHT. Zoals in hoofdstuk 4 van het vorige deel reeds werd aangehaald, is de volledige Algemene Verordening Gegevensbescherming integraal van toepassing op AI-systemen die onder het toepassingsgebied *ratione materiae* vallen, in zoverre hier niet expliciet door de toekomstige AI-verordening van afgeweken wordt.[337] Dit brengt met zich mee dat er dus geen enkele inhoudelijke bepaling van deze Verordening niet relevant zou zijn.

Omdat het echter niet nuttig zou zijn om simpelweg vast te stellen dat alles relevant is, wordt een keuze gemaakt omtrent de meest relevante bepalingen. Dit zijn mijns inziens de onderdelen waar zich potentieel het meeste problemen rond zouden kunnen voordoen en die in het derde deel van deze scriptie zullen worden samengelegd met de relevantste bepalingen uit het voorstel van AI-verordening die in het voorgaande deel werden geïdentificeerd.

Omdat definities de kern van de zaak uitmaken, zijn ze ook hier van uitermate groot belang. Denk hierbij voornamelijk aan artikel 4(7), (8), (13), (14) en (15), die respectievelijk bepalen wat moet worden verstaan onder: (7) verwerkingsverantwoordelijke; (8) verwerker; (13) genetische gegevens; (14) biometrische gegevens; en (15) gezondheidsgegevens. De kwalificering van de betrokken personen zal mogelijk overlap vertonen met de verantwoordelijken onder het regime van de AI-verordening.[338]

Ook zijn de verwerkingen van bijzondere categorieën van persoonsgegevens van belang met betrekking tot het bijkomend risico dat hen bedreigt wanneer ze verwerkt zouden worden met behulp van AI.

Tot slot kan, met het oog op de risicogebaseerde aanpak die het Voorstel implementeert, de regelgeving omtrent geautomatiseerde beslissingen, met inbegrip van profilering, niet worden weggelaten uit deze lijst met meest relevante bepalingen. Daarom zal kort ook nog worden teruggegrepen naar artikel 22 GDPR.

108. ARTIKEL 4(7) & (8) – VERANTWOORDELIJKE PERSONEN. Het toepassingsgebied *ratione personae* werd onder randnummer 96 reeds uitvoerig besproken. Ter herinnering is het belangrijk te vermelden dat de onderlinge verhouding tussen de verwerker en de verwerkingsverantwoordelijke er één is waarin een ondergeschiktheid bestaat.

De verwerker mag namelijk enkel verwerkingshandelingen uitvoeren die uitdrukkelijk, en op geschreven wijze aan haar werden opgedragen door de verwerkingsverantwoordelijke. Dit zorgt er dus voor dat het merendeel van de verantwoordelijkheid voor de verwerking van persoonsgegevens bij de verwerkingsverantwoordelijke. Indien meerdere personen de doeleinden en middelen van de

[337] AI systemen zijn per definitie geautomatiseerde verwerkingssystemen en wanneer de verwerkte data onder de noemer "persoonsgegevens" geplaatst kan worden, hebben de verwerkingsverantwoordelijken / gebruikers zich dus te houden aan de bepalingen van de GDPR.
[338] Zie infra: Randnummer 118. Verantwoordelijkheid – ratione personae.

verwerkingen van dezelfde datasets gaan bepalen, zal ook de verantwoordelijkheid hiervoor tussen hen worden verdeeld.[339]

Wie er in geval van gebruik van AI-systemen als verwerkingsverantwoordelijke of verwerker kan worden aangeduid, en hoe deze hoedanigheden zich verhouden tot de hoedanigheden van distributeurs, importeurs en gebruikers, zal worden besproken in het volgende deel.[340]

109. ARTIKEL 4(13), (14) & (15) – GEVOELIGE PERSOONSGEGEVENS. Ook voor de verwerking van gevoelige of bijzondere categorieën van persoonsgegevens kan naar hoger in dit deel verwezen worden.[341]

De onder artikel 9 bedoelde gevoelige persoonsgegevens zijn in principe verboden te verwerken met slechts uitzonderingen in welbepaalde gevallen. Dit is een belangrijk onderscheid met de verwerking van normale persoonsgegevens, die op zich gewoon kan plaatsvinden, zolang maar voldaan is aan de principes uit artikel 5.[342] Er is dus een verschillende startpositie.

De gedefinieerde gevoelige persoonsgegevens in artikel 4, zijnde (13) de genetische gegevens; (14) de biometrische gegevens; en (15) de medische / gezondheidsgegevens, zijn allemaal persoonsgegevens die rechtstreeks betrekking hebben op de fysieke integriteit van datasubjecten. Dit maakt hen mijns inziens bijzonder gevoelige persoonsgegevens, en dus bijgevolg ook eens zo belangrijk om te beschermen tegen potentieel nadelige verwerkingen door AI-systemen.

In het derde deel zullen deze gegevens gelinkt worden aan de AI-toepassingen die als hoog-risico systemen worden gecategoriseerd, op basis van Bijlage III bij het Voorstel van AI-verordening.[343]

110. ARTIKEL 22 – GEAUTOMATISEERDE BESLISSINGEN. Geautomatiseerde beslissingen vormen als het ware een rode draad doorheen deze scriptie. In het eerste deel werden verschillende risico's geïdentificeerd, die hun grondslag vinden in de automatisatie van fabrieken, wapens en beslissingen met eventuele individuele bindende werking.[344] Ook in het tweede deel is de automatisering van verwerkingshandelingen een belangrijk aspect, simpelweg omdat er zonder een minimum gedeeltelijke automatische verwerking, geen toepassing van de GDPR kan zijn.[345]

De geautomatiseerde individuele beslissingen, met inbegrip van profileringen werden voordien in dit deel reeds uitvoerig besproken, waardoor het op dit punt volstaat om daarheen te verwijzen.[346]

Het mag duidelijk zijn dat het hele punt van de huidige operationele AI nu net het bekomen van een bepaalde graad van automatisering is. Elk AI-systeem dat momenteel bestaat krijgt door haar schepper

[339] Zie hiervoor ook supra: Randnummer 96 – Toepassingsgebied *ratione personae* – Verwerkers en verwerkingsverantwoordelijken & 97 – Joint controllers.
[340] Zie infra: Randnummer 118. Verantwoordelijkheid – ratione personae.
[341] Zie supra: Randnummer 92 – Verwerking van bijzondere categorieën van persoonsgegevens.
[342] Zie supra: Randnummer 103 – Beginselen inzake verwerking van persoonsgegevens.
[343] Zie infra: Randnummer 120. Bijlage III & DPIA.
[344] Zie supra: Randnummer 28 – Overzicht van enkele nadelen; 29 – Jobverlies & socio-economische ongelijkheid; 31 – Autonome wapens; 41 – Zwarte zwanen; 44 – Thought Police; & 45 – LAWS.
[345] Zie artikel 2(1) GDPR; zie ook supra: Randnummer 95 – Automatische verwerking van persoonsgegevens.
[346] Zie supra: Randnummer 99 – Geautomatiseerde individuele beslissingen; & 100 – profilering.

een taak toebedeeld, waarin het zodanig wordt getraind dat nagenoeg geen enkele natuurlijke persoon een dergelijke graad van specialisatie kan evenaren. Op dit moment aangekomen, wordt de voorheen door mensen uitgevoerde taak uitbesteed aan het AI-systeem en wordt die al dan niet intellectuele handeling dus automatisch.

2.5. Overzicht deel 2

111. NOTENDOP GEVULD MET PRIVACY, BESCHERMING VAN PERSOONSGEGEVENS EN GDPR.

Dit tweede deel volgde min of meer hetzelfde stramien als deel 1 door een afgelijnd begrip te plaatsen in een breed concept waar geen vaste definiëring voor bestaat. De bescherming van persoonsgegevens is een afgescheiden recht dat sinds haar ontstaan als een onderdeel van het recht op privacy, meer en meer een eigen karakter heeft ontwikkeld. Dit maakt dat het op dit moment een volledig op zichzelf staand recht is dat weliswaar nauw in verband staat met het recht op privacy.

Er werd in detail gekeken naar verschillende kernbegrippen in de Algemene Verordening Gegevensbescherming, zoals: (i) verwerking; (ii) verwerkingsverantwoordelijke en verwerker; (iii) DPIA; en (iv) geautomatiseerde individuele beslissingen en profilering. Deze begrippen zijn in de context van deze scriptie bijzonder relevant omdat enkelen van hen simpelweg de basis vormen om het GDPR-regime toe te kunnen passen en anderen gewoon niet weg gedacht kunnen worden wanneer over AI wordt gesproken.

In de hoofdstukken 3 en 4 kon worden overgegaan naar een *in depth* bespreking van de krachtlijnen van de Verordening, om ten slotte enkele van de meest relevante bepalingen voor bescherming van persoonsgegevens in de context van verwerkingen door AI-systemen extra toe te lichten. Het gaat in casu om de bepalingen omtrent de verantwoordelijke personen; de verwerkingsverantwoordelijken en verwerkers; de gevoelige persoonsgegevens; en geautomatiseerde individuele beslissingen.

3. Deel 3: Het samenspel van AI en Privacy[347]

Inleiding en opbouw.

111. Terugblik en het begin van het einde. In dit derde en laatste deel zal alles wat in de vorige twee delen werd besproken worden samengevoegd en op elkaar worden geïmplementeerd. Het is op het einde van dit deel dat deze masterscriptie zal worden afgesloten met een conclusie omtrent de algemene vraag waarrond deze hele tekst draait:

> *Hoe verhouden de Algemene Verordening Gegevensbescherming en het voorstel van Artificiële Intelligentie-Verordening zich tot elkaar met betrekking tot het recht op privacy als een fundamenteel mensenrecht?*

112. Deel 1 - Artificiële Intelligentie. In deel 1 werd begonnen met een analyse van de terminologie. Zoals gezegd was dit geen simpele opgave doordat er een veelheid van meningen is omtrent de definitie van gewone, menselijke "intelligentie" en dat de artificiële vorm hiervan het alleen maar complexer maakt. Het voorstel van AI-verordening beëindigt mogelijke twijfels omtrent de definiëring door in artikel 3(1) zelf vier voorwaarden op te lijsten waaraan een systeem moet voldoen om als AI te worden gecategoriseerd voor de toepassing van de toekomstige Verordening.[348] Op dit punt werden toen reeds enkele bedenkingen opgeworpen waarop in dit deel dieper zal worden ingegaan.

Vervolgens werden de meest risicovolle en de meest waardevolle AI-toepassingen geïdentificeerd, voorafgegaan door een korte inleiding tot de verschillende technieken en benaderingen waarmee AI wordt gemaakt.[349] Als belangrijkste risico's voor de bescherming van persoonsgegevens kwamen naar voor: (i) het risico op de-anonimiseren; (ii) de risico's met betrekking tot real time monitoring; (iii) de risico's verbonden met het nemen van geautomatiseerde individuele beslissingen door AI-systemen; en het daarmee samenhangende (iv) risico op discriminatie op basis van persoonsgegevens.[350]

Het eerste deel werd afgesloten met een beschrijving van de krachtlijnen van het voorstel van AI-verordening en er werden enkele bepalingen extra in de schijnwerpers gezet die betrekking hebben op bepaalde definities van data en de risicogebaseerde aanpak die het voorstel uitwerkt[351]

113. Deel 2 – Bescherming van persoonsgegevens. Het tweede deel volgde min of meer dezelfde logica als het eerste. Na een korte inleiding waarin de geschiedenis van het recht op privacy en het nauw verwante recht op bescherming van persoonsgegevens werd besproken,[352] werd overgegaan tot een uitgebreidere bespreking van de twee rechten en hoe ze zich tot elkaar verhouden. Het werd duidelijk dat, hoewel ze zeer nauw op elkaar aansluiten, ze zeker niet als één behandeld kunnen worden. Het

[347] In dit deel zal steeds met de correcte en volledige benaming naar de twee besproken (toekomstige) verordeningen worden verwezen, tenzij het uit de tekst zeer duidelijk blijkt over welke wetgeving het gaat.
[348] Zie artikel 3(1) van het voorstel van AI-verordening & zie supra: Randnummer 12 – Juridische definitie.
[349] Zie supra: Randnummers 18 tot en met 21 – titel 1.1.2. Een onderverdeling naar werking en aard.
[350] Zie supra: Randnummers 22 tot en met 55 – Hoofdstuk 2 De voor- en nadelen van AI.
[351] Zie supra: Randnummers 56 tot en met 70 – Hoofdstuk 3 de krachtlijnen van het voorstel van AI-verordening & Hoofdstuk 4 Relevante bepalingen met betrekking tot privacy en bescherming van persoonsgegevens.
[352] Zie supra: Randnummer 72 ev. – Korte inleiding & geschiedenis.

onderscheid wordt trouwens unaniem erkend in de rechtsleer, rechtspraak en ondertussen ook de wetgeving.[353] Het blijkt dat de bescherming van persoonsgegevens op het Europese continent reeds een rijke rechtsgeschiedenis heeft, waarvan deze scriptie een kleine, maar belangrijke schakel belicht heeft: de Algemene Verordening Gegevensbescherming.

Omdat het niet opportuun was om in het kader van deze scriptie de volledige GDPR tot in detail te bespreken werd vooreerst de belangrijkste terminologie toegelicht. Herinner onder andere: (i) persoonsgegevens; (ii) verwerking; (iii) verwerkingsverantwoordelijke en verwerker; (iv) DPIA; en (v) geautomatiseerde individuele beslissing en profilering.[354]

Verder werden slechts de krachtlijnen van de Verordening weergegeven. Dit was geen moeilijke zoektocht aangezien de wettekst deze zelf op een zeer overzichtelijke manier samenbrengt in artikel 5. Elke verwerking van persoonsgegevens van EU-burgers door middel van een minstens gedeeltelijk geautomatiseerd systeem of door middel van een niet-geautomatiseerd systeem maar met de bedoeling een bestand samen te stellen, moet aan de beginselen inzake de verwerking van persoonsgegevens voldoen.[355] Het is vanzelfsprekend dat verschillende AI-toepassingen onder dit materieel toepassingsgebied zullen vallen.

Het tweede deel werd beëindigd door enkele bijzonder relevante bepalingen extra toe te lichten omdat deze de essentie van het gegevensbeschermingsrecht vormen. Het ging om: (i) de verantwoordelijke personen; (ii) gevoelige persoonsgegevens; en (iii) geautomatiseerde beslissingen.[356]

114. **OPBOUW.** Dit laatste deel zal afstappen van de aanpak die de vorige twee hoofdstukken heeft gekenmerkt. Nu moet namelijk niet langer worden beschreven hoe iets is, maar zal al die beschrijvende informatie worden samengebracht om bepaalde conclusies te trekken.

In een eerste hoofdstuk zal nogmaals kort de verhouding tussen het voorstel van AI-verordening en de Algemene Verordening Gegevensbescherming worden beschreven. Ook worden de toepassingsvoorwaarden en definities van elk van deze wetteksten kort overlopen om af te bakenen in hoeverre GDPR van toepassing kan zijn op AI, wat de verschillen en gelijkenissen zijn in soorten data en welke personen de verantwoordelijkheden dragen voor de verwerkingen door AI.

Het volgende hoofdstuk zal dieper ingaan op de manier waarop er onder het gecombineerde regime van de twee (toekomstige) verordeningen aan de risico's met betrekking tot de bescherming van persoonsgegevens tegemoet gekomen wordt en of dit volgens de auteur een voldoende bescherming biedt en zal blijven bieden in de toekomst.

Het laatste hoofdstuk alvorens een allesomvattende conclusie te formuleren zal gaan over de belangrijkste bedenking die de auteur heeft en die al in zijn hoofd rondspookt sinds het eerste hoofdstuk

[353] Zie supra: Randnummer 82 – Verhouding en geschiedenis.
[354] Zie supra: Randnummers 87 tot en met 100 – 2.2.3. Terminologie m.b.t. bescherming van persoonsgegevens.
[355] Zie supra: Randnummers 102 tot en met 106 – Hoofdstuk 3 De krachtlijnen van de GDPR.
[356] Zie supra: Randnummers 107 tot en met 110 – Hoofdstuk 4 Relevante bepalingen met betrekking tot AI.

van het eerste deel. Er zal daarom dieper worden ingegaan op de opmerkingen die daar reeds werden geformuleerd, gevolgd door een mogelijke oplossing.

3.1. Hoofdstuk 1. De verhouding tussen het Voorstel en de GDPR

115. ***LEX SPECIALIS DEROGAT LEGI GENERALI*.**[357] Eén van de belangrijkste conclusies of bevindingen van deze scriptie is dat het voorstel van AI-verordening de bedoeling heeft om als *lex specialis* te fungeren ten aanzien van het veel algemenere regime onder de GDPR. Dit wil zeggen dat eerst moet gekeken worden of de AI-verordening van toepassing zal zijn om pas wanneer dat niet is, of voor de delen waarover het Voorstel niets vastlegt, naar de GDPR terug te grijpen.

116. **TOEPASSINGSGEBIED.** Alvorens over te gaan tot de kern van de zaak is het aangewezen om nog eens kort te kijken naar de essentie van deze scriptie. Het hele verhaal is erop gericht een antwoord te bieden op de vragen of er problemen zijn met de verwerking van persoonsgegevens door AI-toepassingen en of deze problemen in voldoende mate worden opgelost door het gezamenlijk regelgevend kader van de GDPR en het voorstel van AI-verordening.

Hierin zijn de kernwoorden duidelijk: verwerking, persoonsgegevens, en AI. In het algemeen kan worden gesteld dat, los van het specifieke toepassingsgebied van het Voorstel, elke AI-toepassing die een verwerking van persoonsgegevens uitvoert, wordt opgevangen door de GPDR. Elke AI is namelijk een systeem dat op een geautomatiseerde manier gegevens verwerkt.[358]

Persoonsgegevens zijn alle stukken van informatie die betrekking hebben op natuurlijke personen en het ten minste mogelijk maken hen te identificeren, al dan niet met behulp van bijkomende data.[359]

117. **SOORTEN GEGEVENS & *RATIONE MATERIAE*.** De GDPR maakt een opdeling in soorten gegevens volgens hun gevoeligheid. Zo zijn er de gegevens die onder de algemene definitie van artikel 4(1) vallen, maar niet onder de lijst van gevoelige data van artikel 9(1).

Het Voorstel maakt iets meer opdelingen en vertrekt hierbij vanuit een andere zienswijze. Wat betreft de gevoeligheid van gegevens wordt, in de voor deze scriptie relevante bepalingen, namelijk quasi uitsluitend over biometrische gegevens gesproken, hetgeen een vorm van gevoelige gegevens is volgens de GDPR.

Er zijn verder opdelingen gemaakt naargelang het moment waarop de data wordt gebruikt en naargelang de doeleinden die worden nagestreefd met deze gegevens.[360] Het zijn de doeleinden van de verwerkingen door AI-systemen die in artikel 5 en 6 van het Voorstel worden gecategoriseerd als verboden of hoog-risico.

[357] 1.2. Verenigbaarheid met bestaande bepalingen op het beleidsterrein, in de Toelichting bij het voorstel van AI-verordening.
[358] Zie artikel 2(1) GDPR.
[359] Zie artikel 4(1) GDPR.
[360] Zie supra: Randnummer 68 – Artikel 3 – Definities.

118. **VERANTWOORDELIJKHEID – *RATIONE PERSONAE*.** De GDPR richt haar pijlen op de ***verwerkingsverantwoordelijken*** en ***verwerkers*** van persoonsgegevens. Het zijn deze personen die in eerste instantie moeten toezien op de naleving van de principes van verwerking en de legaliteit ervan op basis van één van de verwerkingsgronden; Het zijn zij die in de mate van het mogelijke en redelijke moeten voorzien in technische en organisatorische maatregelen om de verwerking in goede banen te leiden; en het zullen zij zijn die worden aangesproken wanneer er iets misloopt met de door of voor hen uitgevoerde verwerkingen.[361]

Het voorstel van AI-verordening houdt voornamelijk gebruikers en aanbieders van AI-systemen in het vizier. ***Gebruikers***[362] zijn die personen of instanties die voor hun professionele doelen de hulp van een AI-systeem inschakelen. Ze worden ten aanzien van de persoonsgegevens die door hun systeem worden verwerkt gezien als de verwerkingsverantwoordelijken omdat de beslissingsbevoegdheid omtrent de doeleinden en middelen bij hen ligt. Het gebruikte middel is *in casu* het AI-systeem.

Aanbieders zijn personen of instanties die een AI-systeem hebben ontwikkeld of erover kunnen beschikken en dit in de handel willen brengen. Ze worden importeurs of distributeurs vanaf het moment dat ze het systeem in de handel brengen op de interne markt van de EU. Zolang ze zelf geen gebruik maken van het systeem en het dus ook geen verwerkingen laten uitvoeren, komen deze personen niet in de vuurlinie van de GPDR te liggen.

119. ***RATIONE LOCII*.** Ten slotte, maar verre van onbelangrijk, moet kort nog worden vermeld dat beide verordeningen gericht zijn op verwerkingen van gegevens afkomstig uit de EU, door eender welke partij. Specifiek voor het Voorstel moet worden opgemerkt dat de Output van AI-systemen die een uitwerking hebben binnen één van de lidstaten, ervoor zorgt dat de verantwoordelijken zich aan die toekomstige verordening dienen te houden.

[361] Zie supra: Randnummer 96 – Toepassingsgebied ratione personae – Verwerkers en verwerkingsverantwoordelijken.
[362] Zie artikel 3(4) voorstel van AI-verordening.

3.2. Hoofdstuk 2. De bescherming van persoonsgegevens in het licht van enkele risico's

120. BIJLAGE III & DPIA. Het voorstel van AI-verordening neemt als belangrijkste ankerpunt een risicogebaseerde benadering aan, waarbij door artikel 5 principieel enkele AI-systemen worden verboden. Het gaat hier om systemen die een zodanig verregaande impact zouden hebben op de fundamentele rechten en vrijheden van mensen dat ze niet geaccepteerd kunnen worden met de normen en waarden die aan de Unie ten grondslag liggen in het achterhoofd.

Een iets minder streng lot treft de systemen die onder artikel 6 vallen, en dus louter een hoog risico vormen. Deze systemen zijn de beoogde AI-toepassingen van de volledige verordening aangezien AI die niet-hoog-risico is enkel wordt aangemoedigd om aan de bepalingen te voldoen.

De afweging wordt gedeeltelijk aan de verantwoordelijke personen en instanties gelaten door artikel 6(1), maar voor een significant aantal systemen wordt deze beoordelingsbevoegdheid hen uit handen genomen. De wetgever heeft in deze gevallen zelf een risicoanalyse uitgevoerd en geoordeeld dat de AI-systemen die werden opgenomen in Bijlage III een hoog risico vormen.

Het vraagt niet veel moeite om na een blik op Bijlage III te weten waar de Commissie het meeste risico's voorziet, namelijk in de gevallen waarin AI wordt losgelaten op biometrische gegevens[363] en in de gevallen waarin AI gebruikt zou worden om geautomatiseerde beslissingen te nemen over allerhande onderwerpen.[364]

Bijlage III kan daardoor dus eigenlijk worden gezien als een veruitwendiging van artikel 35 van de GDPR, in uitvoering waarvan een gegevensbeschermingseffectenbeoordeling moet worden uitgevoerd zodra een bepaald type van verwerking, naar alle waarschijnlijkheid, een hoog risico zou kunnen inhouden voor het recht op de bescherming van persoonsgegevens. Hierbij wordt zelfs expliciet verwezen naar het gebruik van nieuwe technologieën.[365]

Omdat een DPIA per definitie een *ex-ante* risicobeoordeling is, past dit dus ook perfect in het plaatje van de krachtlijnen van het Voorstel.[366]

121. Tegemoet komen aan risico's. Er zijn enkele risico's met betrekking tot de bescherming van persoonsgegevens die inherent zijn aan een verwerking door middel van AI-systemen. Zo is er het risico op de-anonimisering door de enorme verwerkingskracht en -snelheid waarover dergelijke systemen beschikken. Ook surveillance kan betrekkelijk vereenvoudigd worden wanneer hiervoor de hulp van een

[363] Zie 1e punt – *biometrische identificatie en categorisering van natuurlijke personen*, onder Bijlage III van het voorstel van AI-verordening juncto overweging 33.
[364] Zie quasi alle volgende punten onder Bijlage III van het voorstel van AI-verordening juncto overwegingen 34 tot en met 40.
[365] Zie **artikel 35(1) GDPR**. "*Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen voert de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden*."
[366] Zie supra: Randnummer 66 – Ex-ante risicobeoordeling & ex-posthandhavingsmaatregelen.

AI-systeem kan worden ingeschakeld. Daarom worden bepaalde vormen hiervan ook gewoonweg verboden door artikel 5 van het Voorstel, of ten minste als hoog-risico systeem gemerkt.

Het belangrijkste risico waaraan door het voorstel van AI-verordening mijns inziens in hoge mate tegemoet gekomen wordt, is dat welk kleeft aan geautomatiseerde individuele beslissingen. Het blijkt duidelijk uit Bijlage III dat dit iets is waar regelgeving haar nut kan hebben en dat deze kans dan met beide handen wordt gegrepen. Belangrijk om op te merken is dat de mogelijkheden van geautomatiseerde beslissingen stevig worden gereguleerd door hen te bestempelen als hoog-risico systemen. Hierbij komt ook nog dat systemen die worden bedoeld in Bijlage III en die voldoen aan de vereisten die door het Voorstel worden opgelegd, niet noodzakelijkerwijze over een verwerkingsgrond beschikken.[367] Hiervoor moet namelijk nog steeds worden gekeken naar artikel 5 van de GDPR. Het recht om niet te worden onderworpen aan geautomatiseerde individuele beslissingen, dat wordt voorzien door artikel 22 GDPR, blijft dus ongeschonden door het voorstel van AI-verordening.

122. Belangrijkste wijziging door het Voorstel. De meest concrete en duidelijke afwijking van het GDPR-regime is te vinden in de maatregelen ter ondersteuning van innovatie en de zogenaamde testomgevingen. De regels van artikel 53 tot en met 55 van het Voorstel dienen namelijk wel te worden gelezen als een specifieke, bijkomende verwerkingsgrond in de zin van artikel 6 ev. van de GDPR. Ook mogen de verwerkingen van persoonsgegevens binnen deze AI-testomgeving verder gaan dan de grond waarop ze in eerste instantie werden verzameld. Dit is mijns inziens geen disproportionele inbreuk op het gegevensbeschermingsrecht omdat het enkel maar mogelijk is in enkele strikt afgelijnde situaties.[368]

[367] Zie overweging 41 bij het voorstel van AI-verordening.

[368] Zie **artikel 54(1) voorstel van AI-verordening**. "*In de AI-testomgeving voor regelgeving worden rechtmatig voor andere doeleinden verzamelde persoonsgegevens onder de volgende voorwaarden verwerkt ten behoeve van het ontwikkelen en testen van bepaalde innovatieve AI-systemen in de testomgeving:*
(a)*de innovatieve AI-systemen worden ontwikkeld voor het beschermen van zwaarwegend algemeen belang op een of meer van de volgende gebieden: i)de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, onder de controle en verantwoordelijkheid van de bevoegde autoriteiten. De verwerking is gebaseerd op het recht van de lidstaten of de Unie;* ii)*de openbare veiligheid en volksgezondheid, waaronder ziektepreventie, -beheersing en -behandeling;* iii)*een hoog niveau van bescherming en verbetering van de kwaliteit van het milieu;* ***(b)****de verwerkte data zijn nodig om te voldoen aan een of meer van de in titel III, hoofdstuk 2, beschreven voorschriften wanneer die voorschriften niet doeltreffend kunnen worden vervuld door het verwerken van geanonimiseerde, synthetische of andere niet persoonsgebonden data;* ***(c)****er zijn doeltreffende monitoringmechanismen om vast te stellen of zich tijdens de experimenten in de testomgeving hoge risico's voor de grondrechten van de betrokkenen kunnen voordoen evenals responsmechanismen om die risico's onmiddellijk te beperken en indien nodig de verwerking stop te zetten;* ***(d)****in het kader van de testomgeving te verwerken persoonsgegevens bevinden zich in een functioneel gescheiden, geïsoleerde en beschermde omgeving voor dataverwerking onder de controle van de deelnemers, waarbij alleen bevoegde personen toegang hebben tot die data; (e)verwerkte persoonsgegevens mogen niet door andere partijen worden verzonden, doorgegeven of anderszins worden geraadpleegd;* ***(f)****de verwerking van persoonsgegevens in het kader van de testomgeving mag niet leiden tot maatregelen of besluiten die gevolgen hebben voor de betrokkenen;* ***(g)****in het kader van de testomgeving verwerkte persoonsgegevens worden gewist nadat de deelname aan de testomgeving is beëindigd of de periode van bewaring van de persoonsgegevens ten einde is gekomen;* ***(h)****de logbestanden van de verwerking van persoonsgegevens in het kader van de testomgeving worden tijdens de duur van de deelname aan de testomgeving en één jaar na beëindiging ervan bewaard, uitsluitend ten behoeve van en alleen zo lang als nodig is voor het nakomen van aansprakelijkheids- en documenteringsverplichtingen overeenkomstig dit artikel of andere toepasselijke wetgeving van de Unie of de lidstaten;* ***(i)****een volledige en gedetailleerde beschrijving van het proces en de onderbouwing van het trainen, testen en valideren van het AI-systeem wordt samen de testresultaten bewaard als onderdeel van de technische documentatie in bijlage IV;* ***(j)****een korte samenvatting van het in de testomgeving ontwikkelde AI-project en de doelstellingen en verwachte resultaten ervan worden op de website van de bevoegde autoriteiten gepubliceerd.*"

3.3. Hoofdstuk 3. Problematische definiëring van "Artificiële Intelligentie"

123. Terugblik. Helemaal in het begin van deze scriptie werd begonnen met een blik op het begrip "artificiële intelligentie".[369] Artikel 3(1)[370] van het voorstel van AI-verordening stelt vier elementen voorop die samen bepalen wat wordt aanzien als een AI-toepassing en dus onder het toepassingsgebied van de verordening zal vallen. Reeds in die allereerste titel in het eerste hoofdstuk van dat eerste deel werden kort enkele bedenkingen verwoord omtrent de definiëring, dewelke nu iets verder zullen worden uitgewerkt. Het gaat *in concreto* om de drie laatste criteria. De voorwaarde dat het om software moet gaan is mijns inziens zo voor de hand liggend dat ze in de praktijk geen problemen zal geven. Als het om intelligentie zou gaan die niet voortkomt uit software, dat moet het gaan om een biologische bron; met name hersenen.

124. Bijlage I. De wettelijke definitie van artikel 3(1) verwijst naar Bijlage I bij het voorstel waarin op dit moment drie technieken of benaderingen worden opgesomd. Het gaat om: (a) benaderingen voor machinaal leren; (b) op logica en kennis gebaseerde benaderingen; en (c) statistische benaderingen, dewelke kort werden omschreven in titel 1.1.2.[371]

Uit de toelichting bij het voorstel blijkt duidelijk dat het de bedoeling van de wetgever is om van deze bijlage I een werktuig te maken dat vlot aan te vullen moet zijn wanneer de situatie zich voordoet waarin de lijst niet meer *up to date* is. Deze werkwijze geeft op zich blijk van een vooruitstrevende aanpak waarmee wordt geanticipeerd op mogelijke nieuwe ontwikkelingen van technieken en benaderingen waarop en waarmee AI kan werken. Onder invloed van de huidige vooruitgang in het gebied van computersystemen[372] is het namelijk niet ondenkbaar dat deze ontwikkeling in de nabije toekomst zou kunnen plaatsvinden en ook een sprong voorwaarts met zich meebrengt voor AI, dit mogelijk in de vorm van een nieuwe techniek/benadering.

Wat mijns inziens echter problematisch is aan het gebruik van een limitatieve lijst zoals Bijlage I, is dat het recht per definitie achter de feiten aanloopt. En eens te meer wanneer het gaat om zaken waarmee veel emoties en grote bedragen geld gemoeid zijn. Laat beiden nu spelen in het geval van AI.

Voor deze scriptie werd aangenomen dat AI als term en onderzoeksgebied is geboren in 1955 toen een groep computerwetenschappers naar Dartmouth afgezakten voor het zogenaamde "*Summer research project on artificial intelligence*". Het heeft de wetgevers wereldwijd sindsdien dus meer dan 50 jaar

[369] Zie supra: Randnummer 12 – Juridische definitie.
[370] Ter herinnering: "*"Artificiële-intelligentiesysteem" (AI-systeem): software die ontwikkeld is aan de hand van een of meerdere technieken en benaderingen die zijn opgenomen in de lijst van bijlage I en die voor een bepaalde reeks door mensen gedefinieerde doelstellingen output kan genereren, zoals inhoud, voorspellingen, aanbevelingen of beslissingen die van invloed zijn op de omgeving waarmee wordt geïnterageerd."*
[371] Zie supra: Titel 1.1.2. Een onderverdeling naar werking en aard, Randnummers 18 tot en met 21.
[372] Op het gebied van Quantumcomputers zijn recentelijk verschillende vooruitgangen geboekt. Voor een idee van waarop deze vooruitgang gebaseerd is, wordt verwezen naar: S.-S. LI, G.-L. LONG, F.-S. BAI & H.-Z. SHENG, "Quantum Computing", PNAS (vol. 98, nr. 21) 9 oktober 2001, p. 11847-11848, https://doi.org/10.1073/pnas.191373698; P.W. SHOR, "Quantum Computing", Documenta Mathematica – extra volume IMC 1998, p. 467-486, http://nozdr.ru/data/media/biblio/kolxoz/M/ICM-1998,%20Berlin.%20Proceedings,%20Vol.%201%20Plenary%20lectures%20(no%20p.%2023-52)%20(Documenta%20Mathematica,%201998)(660s)_M_.pdf#page=434; …

gekost om op de proppen te komen met een wettelijk afdwingbaar kader zoals de nu voorliggende AI-verordening. Het is uiteraard onzin om te verwachten dat de wetgever in 1955 reeds serieuze risicoanalyses had beginnen maken omtrent een onderzoeksveld dat toen inderdaad nog geen enkele reële en in de nabije toekomst geplaatste dreigingen met zich meebracht. Recentere ontwikkelingen die wel duidelijke risico's aan het licht brachten[373] bestaan echter ook al best lang zonder noemenswaardige reactie in de wetgeving. De wettelijke regeling van het onderzoeks- en werkveld heeft namelijk steeds onder andere rechtstakken gevallen naargelang de sector waarin en waarvoor de AI werd ontwikkeld.

Met dit in het achterhoofd en de trage reactie van wetgeving in het algemeen is dit een potentieel probleem dat mijns inziens niet uit het oog mag worden verloren.

125. Doelgerichte output & interageren met omgeving. Het derde criterium uit de definitie van AI gaat erom dat de software, die bestaat uit één of meerdere van de voornoemde technieken en benaderingen uit Bijlage I, een zekere output moet genereren op basis van door de mens gedefinieerde doelstellingen. De vierde en laatste vereiste is dat de AI in kwestie de omgeving waarmee ze in interactie staat moet beïnvloeden.

De verwoording van art. 3(1) van het voorstel tot AI-verordening maakt duidelijk dat aan alle vier criteria moet worden voldaan. Wat echter niet duidelijk is, is hoe het criterium van "beïnvloeding" moet worden ingevuld. Hoewel de wetgever er soms bewust voor opteert om de concrete invulling van begrippen aan lagere wetgevende instanties, de uitvoerende macht of aan de rechtsleer te laten, is dat *in casu* ogenschijnlijk niet het geval. In de voorbereidende werken is hier namelijk niets over te lezen.

Los van alle menselijke fouten die in de praktijk voor een problematische input – en bijgevolg dus ook output – zouden kunnen zorgen, is er mijns inziens ook een duidelijk potentieel interpretatieprobleem naar de invulling van deze criteria.

Zoals in randnummer 17[374] reeds werd aangehaald is het belangrijk om een zo breed mogelijke interpretatie van zowel het concept "door de mens gedefinieerde doelstellingen" als van het begrip "beïnvloeden" aan te houden, teneinde te vermijden dat de praktijk op zoek zal gaan naar manieren om onder de AI-verordening uit te komen.

Concreet wil dit dus zeggen dat eender welke, weloverwogen en bewust ingevoerde input moet worden geaccepteerd als een "door de mens gedefinieerde doelstelling". Dit wil dus ook zeggen dat een AI-systeem dat bijvoorbeeld de mogelijkheid heeft om via camera's te "zien", en een output genereert op een onwillekeurige beweging[375], hier niet onder kan vallen.

Met betrekking tot "beïnvloeden" wilt dit zeggen dat elke materiële of rechtshandeling van een persoon, hetzelfde of een ander systeem, ten gevolge van een output van het AI-systeem, gebaseerd op de

[373] Zoals de racistische chatbots, …
[374] Zie supra: Randnummer 17 – Cumulatief en sensu lato interpretatie.
[375] Onwillekeurige bewegingen zijn bewegingen die niet bewust aan te sturen zijn. Denk hierbij aan de hartspier, het maag-darmsysteem en al dan niet pathologische stuiptrekkingen.

verwerking van concrete input door mensen gegeven, met toepassing van de relevante techniek of benadering, moet worden gezien als een beïnvloeding van de omgeving.

Ik zie geen direct voordeel in het laten afhangen van rechtspraak en rechtsleer van de invulling van deze begrippen. Dit zorgt voor rechtsonzekerheid terwijl het nu net het doel is van het voorstel om zekerheid en vertrouwen te scheppen met betrekking tot deze technologie. Waar uiteraard wel plaats moet zijn voor rechtspraak is voor de volstrekt van de pot gerukte toepassingen van deze brede interpretatie. Een mens is nu eenmaal het product van zijn ervaringen en het louter lezen of zien van output om die kennis vervolgens te bewaren of negeren, mag niet worden gezien als "beïnvloeden", zelfs als de handeling van het bewaren/negeren uiteraard nooit had kunnen plaatsvinden zonder de output in kwestie. Het moet aan de discretie van de rechter zijn om overdreven interpretaties te weren.

Conclusie

126. **ONDERZOEKSVRAAG.** Tot afronding van deze masterscriptie moet nog eenmaal een laatste blik worden geworpen op de algemene onderzoeksvraag die aan de grondslag van dit onderzoek ligt.

Hoe verhouden de GDPR en het voorstel van AI-verordening zich tot elkaar met betrekking tot het recht op privacy als fundamenteel mensenrecht?

Al snel werd duidelijk dat een deel van deze vraag ons in deze scriptie te ver zou brengen en dus werd geopteerd om de rol van het recht op privacy te beperken tot historisch en inhoudelijk kader waarin het meer relevante recht op bescherming van persoonsgegevens is ontstaan.

127. **Overzicht van deze scriptie.** Het eerste deel bevat een overzicht van artificiële intelligentie en het Voorstel dat voor deze familie van technologieën een wettelijk kader tracht op poten te zetten. Vooreerst werd gekeken naar definities en een ietwat technischere kant. Dit omdat het zinloos zou zijn om te trachten regelgeving te beoordelen waarvan het onderwerp totaal niet gekend is. Vervolgens werd aan de hand van verschillende, juridische en niet-juridische bronnen een beeld geschetst van de potentiële voor- en nadelen. Een laatste stap in dit eerste deel zorgde voor een vogelvlucht over de risicogebaseerde aanpak die door het Voorstel wordt vooropgesteld.

In het tweede deel werd hetzelfde stramien gevolgd, maar nu toegepast op de GDPR. Na een inleiding in het concept van het recht op privacy kon de link gelegd worden naar het recht op bescherming van persoonsgegevens en haar toch al redelijk rijke geschiedenis binnen de Europese wetgevende documenten. Na een kort overzicht van het kader van rechtsnormen waartussen de GDPR zich manoeuvreert, werd overgegaan tot de kern van de zaak door de beginselen met betrekking tot de verwerking van persoonsgegevens uit artikel 5 te bespreken, alsook de verwerkingsgronden van normale persoonsgegevens (artikel 6) en die voor bijzondere persoonsgegevens.

128. **PROBLEMATISCHE DEFINIËRING.** Reeds in het eerste hoofdstuk van het eerste deel werden vraagtekens geplaatst bij de performantie van de definiëring van "artificiële intelligentie-systemen" die door het Voorstel wordt gehanteerd. In deel 3 werd beargumenteerd dat voornamelijk door de zeer trage werking van de wetgevende macht er in de praktijk een risico bestaat op achterstand in het bijhouden van de technieken en benaderingen, opgenomen in Bijlage I. Ook met betrekking tot de invulling van de vereisten van een "gedefinieerde doelstelling" en "interactie met de omgeving" is het niet duidelijk wat precies onder deze concepten moet worden geplaatst. Er werd door de auteur vastgesteld dat een te limitatieve invulling van deze begrippen zou leiden tot actieve zoektochten naar manieren om onder de verplichtingen van de toekomstige Verordening uit te komen.

129. **VERHOUDING TOT ELKAAR.** Hoewel het reeds meermaals werd herhaald in het corpus van deze masterscriptie, is het ook voor de conclusie noodzakelijk om nogmaals aan te duiden dat het voorstel van AI-verordening zich tot de GDPR zal verhouden als lex specialis. Dit wil dus zeggen dat, wanneer de toekomstige Verordening van toepassing is, er eerst naar haar verplichtingen moet worden gekeken.

Pas als deze niets vaststellen of lacunes laten, zullen verwerkingen van persoonsgegevens door AI-toepassingen in het vangnet van de GDPR vallen.

130. RISICO'S BETREFFENDE GEGEVENSBESCHERMING IN HET AI-RECHT. Met het oog op de risico's die in hoofdstuk 2 van het eerste deel werden vastgesteld kan relatief kort worden geconcludeerd dat het voorstel deze ter harte heeft genomen. Artikel 5 verbiedt in principe de meest kwalijke AI-toepassingen, die zouden beogen om mensen of groepen van mensen te manipuleren, die personen zouden categoriseren op basis van bepaalde persoonskenmerken om hen een score toe te kennen, of die hen door middel van biometrische gegevens in openbare ruimtes en in real time zouden identificeren. Artikel 6 stelt vervolgens de voorwaarden vast die voldaan moeten zijn om van een hoog-risico AI-toepassing te spreken.

Naast deze voorwaarden heeft de wetgever ook zelf haar *due dilligence* gedaan in uitvoering van artikel 35 GDPR (DPIA) om zo een aan te vullen lijst van systemen op te stellen die sowieso een hoog risico-label worden toegekend. Dit is dan Bijlage III, waarin een duidelijke focus ligt op geautomatiseerde beslissingen. In veel gevallen gaat het om geautomatiseerde individuele beslissingen, waarbij er dus een risico bestaat dat het recht van datasubjecten om niet gebonden te worden door geautomatiseerde beslissingen, uit artikel 22 GDPR, wordt miskend. Hieraan wordt echter tegemoet gekomen door overweging 41 bij het Voorstel, die expliciet verklaart dat een categorisering als hoog-risico systeem, en het voldoen aan de verplichtingen van het Voorstel, niet mag worden gezien als een rechtsgrondslag voor de verwerking van persoonsgegevens. Dit wil dus zeggen dat verwerkingen van persoonsgegevens door middel van een AI-systeem nog steeds een verwerkingsgrondslag moeten vinden onder respectievelijk artikel 5 of 9 van de GDPR en dat er door de EU-wetgever ook niet wordt geraakt aan het recht om niet door geautomatiseerde beslissingen te zijn gebonden.

Het toepassingsgebied *ratione personae* van beide verordeningen vertoont enkele overlappingen, met name tussen de begrippen van verwerkingsverantwoordelijke of verwerker met dat van gebruiker van een AI-systeem. Het zal in de praktijk namelijk bijna altijd zo zijn dat een gebruiker ook het doel van de verwerkingen bepaalt. Is dit niet het geval, dan werkt de gebruiker waarschijnlijk in opdracht van iemand anders die wel het doel heeft bepaald. Het middel staat *in casu* vast want het zal steeds een AI-systeem zijn dat de verwerking uitvoert.

131. TOEKOMSTIGE UITDAGINGEN. De laatste subvraag die werd gesteld peilde naar het toekomstperspectief dat de samenwerking tussen deze twee (toekomstige) verordeningen biedt. Hieromtrent kan mijns inziens geconcludeerd worden dat de open bewoording van de technieken en benaderingen onder Bijlage I op dit moment zeker allesomvattend genoeg is om de huidige stand van de techniek te capteren. Er schuilt echter een probleem in toekomstige nieuwe ontwikkelingen van technieken of methoden, die door de trage werking van wetgevers voor minstens enkele maanden aan de verplichtingen van de toekomstige AI-verordening zouden ontsnappen.

Hieraan zou mogelijk tegemoet gekomen kunnen worden door een *catch-all* die in te vullen is door deskundigen uit het werk- en onderzoeksveld van deze bijzonder interessante technologie.

Kort samengevat:

Mijns inziens is het regelgevend kader op zich zeker voldoende en zal het ervoor zorgen dat AI-toepassingen met hoog risico niet ongecontroleerd op de EU interne markt zullen worden losgelaten. Wat betreft de definiëring van het begrip "AI" en dus het materieel toepassingsgebied, ben ik van mening dat er ruimte is voor verbetering in de vorm van bijvoorbeeld een *catch-all* die wordt ingevuld door de expertise van deskundigen in het vakgebied.

Bibliografie

Wetgeving

Internationaal

Verenigde Naties

Verenigde Naties, Universele Verklaring van de Rechten van de Mens, 10 december 1948, (A/RES/217).

Verenigde Naties, Internationaal verdrag inzake burgerrechten en politieke rechten, 19 december 1966.

Verenigde Naties, Algemene Vergadering, *Resolution on the right to privacy in the digital age*, A/RES/68/167, New York, 18 december 2013.

Verenigde Naties, Algemene Vergadering, *Revised draft resolution on the right to privacy in the digital age*, A/C.3/69/L.26/Rev.1, New York, 19 november 2014.

Verenigde Naties, Algemene Vergadering, *Revised draft resolution on the right to privacy in the digital age*, A/C.3/71/L.39/Rev.1, New York, 16 november 2016.

Verenigde Naties, Raad voor de mensenrechten, *The right to privacy in the digital age*, A/HRC/34/L.7/Rev.1, 22 maart 2017.

Raad van Europa

Raad van Europa, Europees Verdrag voor de Rechten van de Mens en de Fundamentele Vrijheden, 4 november 1950.

Raad van Europa, Conventie ter bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, CETS nr. 108, 1981. (Conventie 108)

Raad van Europa, Consultative Committee of Convention 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23 januari 2017.

Raad van Europa, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, CETS nr. 223, 2018. (Conventie 108+)

Andere

International Telecommunication Union, Aanbeveling nr Y.3600 (11/55) betreffende, *Big data - Cloud computing based requirements and capabilities*, November 2015.

Europese Unie

Primair recht

Verdrag betreffende de Europese Unie (geconsolideerde versie) van 26 oktober 2012, (C 326/13).

Verdrag betreffende de werking van de Europese Unie (geconsolideerde versie) van 26 oktober 2012, (C 326/46).

Europese Unie, Handvest van de Grondrechten van de Europese Unie, van 14 december 2007, (2007/C 303/01).

Secundair recht

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.

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)

MEDEDELING (Comm.) aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's - Naar een bloeiende data-economie, COM(2014) 442 final, Brussel, 2 juli 2014.

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.

RICHTLIJN (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

VOORSTEL (Comm.) voor een verordening van het Europees Parlement en de Raad van 10 januari 2017 met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, en tot intrekking van Richtlijn 2002/58/EG (richtlijn betreffende privacy en elektronische communicatie).

VERORDENING (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG.

ETHISCHE RICHTSNOEREN (Comm.) van het Directoraat-Generaal Communicatienetwerken, Inhoud en Technologie, voor betrouwbare KI, Publications Office, 8 april 2019.

WITBOEK (Comm.) over kunstmatige intelligentie – een Europese benadering op basis van excellentie en vertrouwen, 19 februari 2020, COM (2020) 65 final.

VOORSTEL (Comm.), 2021/0106 voor een verordening van het Europees Parlement en de raad van 21 april 2021 tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (wet op de artificiële intelligentie) en tot wijziging van bepaalde wetgevingshandelingen van de unie, [COD].

Nationaal

België

Gecoördineerde Belgische Grondwet, *BS* 17 februari 1994.

Voorstel van Resolutie, 23 juni 2021, betreffende een internationaal verbodsverdrag op dodelijke autonome wapensystemen, (DOC 55 2087/001), https://www.dekamer.be/FLWB/PDF/55/2087/55K2087001.pdf.

Wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's, gewijzigd door de wetten van 12 november 2009, 3 augustus 2012, 4 april 2014 en 21 april 2016 (gecoördineerde versie), *BS* 31 mei 2007.

Wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, *BS* 10 januari 2018; Zie ook: https://www.gegevensbeschermingsautoriteit.be/publications/bijlage-advies-op-het-voorontwerp-van-wet-tot-wijziging-van-de-gba-wet.pdf.

Beslissing (VTC nr. O/2020/01) van 14 januari 2020 betreffende Aanname van de lijst met verwerkingen waarvoor een Gegevensbeschermingseffectbeoordeling dient te worden uitgevoerd conform artikel 35.4 van de Algemene Verordening Gegevensbescherming door Vlaamse bestuursinstanties, https://overheid.vlaanderen.be/sites/default/files/media/VTC/VTC_O_2020_01_DPIA_lijsten_v1_voor_web.pdf?timestamp=1589396929.

CAO nr. 68 betreffende camerabewaking op de werkplek

CAO nr. 81 betreffende controle op de elektronische netwerkcommunicatie

Het advies van de GBA betreffende de geolocatie van voertuigen van werknemers, https://www.gegevensbeschermingsautoriteit.be/burger/thema-s/privacy-op-de-werkplek/toezicht-van-de-werkgever/geolocalisatie.

Nederland

Nederlandse Grondwet, *STB* 24 augustus 1815.

Besluit (Nr. 64418) inzake lijst van verwerkingen van persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling (DPIA) verplicht is, Autoriteit Persoonsgegevens, *Staatscourant* 27 november 2019, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/stcrt-2019-64418.pdf.

Frankrijk

Code Civil des Français, *Journal officiel de la République française*, 21 maart 1804, https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006070721/.

Loi n° 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens,

Rechtspraak

Europees Hof voor de Rechten van de Mens

EHRM, *Klass et all. v. Duitsland*, nr. 5029/71, 6 september 1978.

EHRM, *Malone v. Verenigd Koninkrijk*, nr. 8691/79, 2 augustus 1984.

EHRM, *Rotaru v. Roemenië* [GK], nr. 28341/95, 4 mei 2000.

EHRM, *Szabó en Vissy v. Hongarije*, nr. 37138/14, 12 januari 2016.

EHRM*, Uzun v. Duitsland*, nr. 35623/05, 2 september 2012.

EHRM, *Z v. Finland*, nr. 22009/93, 25 februari 1997.

Hof van Justitie van de Europese Unie

HvJ-EU, zaak C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů*, 11 december 2014.

HvJ-EU, Gevoegde zaken C-293/12 en C-594/12*, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ierland* & *Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl e.a*.,[GK], 8 april 2014.

HvJ-EU, Gevoegde zaken C-468/10 en C-469/10, *Asociación Nacional de Astablecimientos Financieros de Crédito (ANSEF)* en *Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado*, 24 november 2011.

HvJ-EU, Gevoegde zaken C-92/09 & C-93/09, *Volker und Markus Schecke en Hartmut Eifert v. Land Hessen,* [GK], 9 november 2010.

HvJ-EU, zaak C-101/01, *Strafzaak tegen Bodil Lindqvist*, 6 november 2003.

HvJ-EU, zaak C-131/12, *Google Spain SL en Google Inc. tegen Agencia Española de Protección de Datos (AEPD) en Mario Costeja González*, [GK], 13 mei 2014.

HvJ-EU, zaak C-398/15, *Camera di Commercio,Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 8 maart 2017.

HvJ-EU, zaak C-536/15, *Tele2 (Nederland) BV e.a./Autoriteit Consument en Markt (ACM)*, 15 maart 2017.

HvJ-EU, zaak C-543/09, *Deutsche Telekom AG/Bondsrepubliek Duitsland*, 5 mei 2011.

HvJ-EU, zaak C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, 19 oktober 2016.

HvJ-EU, zaak C-70/10, *Scarlet Extended SA v. Société belge des auterus, compositeurs et éditeurs SCLR (SABAM)*, 24 november 2011.

Rechtsleer

Boeken (online en fysiek)

AGRAWAL, A., GANS, J., & GOLDFARB, A. (eds.), *The economics of Artificial Intelligence- An Agenda*, Chicago, University of Chicago Press, 2019, 648 p., https://doi.org/10.7208/chicago/9780226613475.001.0001.

ASIMOV, I., *I, Robot*, New York, Bantam Books, 1950, 253p.

BARBÉ, E., & BADELL, D., "The European Union and Lethal Autonomous Weapons Systems: United in Diversity?", in JOHANSSON-NOGUÉS, E., VLASKAMP, M.C., & BARBÉ, E. (eds.), *European Union Contested – Foreign policy in a New Global Context*, Cham, Springer, 2020, 219 p., https://doi.org/10.1007/978-3-030-33238-9.

BARRAT, J., *Our Final Invention: Artificial Intelligence and the End of the Human Era*, New York, Thomas Dunne Books/St Martin's Press, 2013, 336 p., ISBN13: 9780312622374.

BEIGNIER, B., "La Vie Privée", p. 139-141 in CABRILLAC, R., FRISON-ROCHE, M.-A., REVET, T., ALBIGÈS, C., ALFANDARI, E., BERNARD, B., *Libertés et Droits Fondamentaux*, Parijs, Toulouse Capitole Publications, 2013, ISBN 2-247-05122-7.

BENNETT, D.J., *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Ithaca NY, Cornell University Press, 2018, 288 p., ISBN: 1501722131, 9781501722134.

BERTRAND, A., *Droit a la Vie Privee et Droit à l'image*, Lexis Nexis, 1999, XIII - 222 p.

BLÄSIUS, K.H., HEDTSTÜCK, U., & ROLLINGER, C.-R., "Sorts and types in Artificial Intelligence" in SIEKMANN, J., *Lecture notes in Artificial Intelligence*, Berlijn, Springer-Verlag, 1989, ISBN 3-540-52337-5.

BOLOGNE, J.C., *Histoire de la Pudeur*, Zaventem, Hachette, 1986, p. 168, ISBN13: 9782012788800.

BOUCHER, P.N., *Artificial intelligence: How does it work, why does it matter, and what can we do about it?*, Brussel, Scientific Foresight Unit (STOA), within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament, juni 2020, 76 p., https://doi.org/10.2861/44572.

BROOKS, R.A., *Cambrian Intelligence. The Early History of the New AI*, Cambridge, (MA), MIT Press, 199 p., https://doi.org/10.7551/mitpress/1716.001.0001.

CASTELLS, M., *Rise of the Network Society: The Information Age: Economy, Society and Culture,* Malden, Massachusetts, Blackwell Publishers, 1996 (herzien in 2010), 625p., https://urb.bme.hu/wp-content/uploads/2014/05/manuel_castells_the_rise_of_the_network_societybookfi-org.compressed.pdf.

COHEN, J.L., *Regulating Intimacy: A New Legal Paradigm*, Princeton and Oxford, Princeton University Press, 2004, 304p, https://doi.org/10.1017/S1743923X05222079.

CONNOLLY, R., & FOX, G., "Dataveillance and Information Privacy Concerns", p. 391-410, in NORMORE, A., JAVADI, M., & LONG, L. (eds.), *Handbook of Research on Strategic Communication, Leadership, and Conflict Management in Modern Organizations*, Hershey, PA, IGI Global, 2019, 553p., https://doi.org/10.4018/978-1-5225-8516-9.

COOLEY, T.M., *A Treatise on the Law of Torts or the Wrongs Which Arise Independ of Contract*, Chicago, Callaghan and Company, 1879, 755 p., https://repository.law.umich.edu/books/11/.

COUNCIL OF EUROPE, EUROPEAN COURT OF HUMAN RIGHTS, EUROPEAN DATA PROTECTION SUPERVISOR, EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Handbook on European data protection law : 2018 edition*, Publications Office, 2019, 350 p., https://data.europa.eu/doi/10.2811/343461.

DUERR, H.P., *Der Mythos vom Zivilisationsprozess*, Frankfurt am Main, Suhrkamp, 1988.

EUROPEAN UNION AGENCY FOR CYBERSECURITY, *Handbook on security of personal data processing*, European Network and Information Security Agency (ENISA), 2018, 67p.

FINN, R.L., WRIGHT, D., & FRIEDEWALD, M., "Seven Types of Privacy", in GUTWIRTH, S., LEENES, R., DE HERT, P., & POULLET, Y. (eds), *European Data Protection: Coming of Age*, Dordrecht, Springer, 2013, XII, 440p., https://doi.org/10.1007/978-94-007-5170-5_1.

FLOREANO, D., & MATTIUSSI, C., *Bio-Inspired Artificial Intelligence: Theories, Methods, and Technologies*, Cambridge (Massachusetts) & Londen (Engeland), The MIT Press, 2008, 674 p., ISBN 9780262303910.

FRA, *Handbook on European data protection law – 2018 edition*, Luxemburg, Publications Office of the European Union, 2019, p. 350., https://data.europa.eu/doi/10.2811/343461.

FUCHS, C., *Internet and Society: Social Theory in the Information Age*, New York, Routledge, 2007, 816p., ISBN: 1135898820, 9781135898823.

GABRIELS, K., *Conscientious AI – Machine Learning Morals*, Brussel, VUBPRESS, 2020, 174 p., ISBN: 978 90 5718 956 2.

GARDNER, H.E., *Intelligence reframed: Multiple intelligences for the 21st century*, New York, Basic Books, 1999, 292 p., ISBN: ISBN-0-465-02610-9.

GOOLD, B.J., and LAZARUS, L., *Security and Human Rights*, Bloomsburry Publishing, 2019, 240p., ISBN: 1509917780, 9781509917785.

GREENWALD, G., *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, New York, Henry Holt and Company, 13 mei 2014, 272 p., ISBN: 1627790748, 9781627790741.

GUTWIRTH, S., *Privacy and the information age*, Lanham, MD, Rowman & Littlefield, 2002, 152 p., ISBN: 0742517462, 9780742517462.

GUTWIRTH, S., LEENES, R. & DE HERT, P. (eds.), *Data Protection on the Move – Current Developments in ICT and Privacy/Data Protection*, Dordrecht, Springer, 2016, 476p.

HAYES-ROTH, F., WATERMAN, D., & LENAT, D., *Building Expert Systems*, San Francisco, Addison-Wesley Pub. Co., 1983, 472 p., ISBN 0-201-10686-8.

LYON, D., *Surveillance after September 11*, Cambridge, Polity Press, 26 september 2003, 197 p., ISBN: 0745631819, 9780745631813.

CONIX, S., PEETERS, L., VAN LOOVEREN, A. en VERHELST, I., *Privacy, 1e editie*, Brussel, Intersentia, 2019, 194p.

CUDD, A.E. & NAVIN, M.C. (eds.), *Core Concepts and Contemporary Issues in Privacy*, Cham, Springer, 2018, 265p.

SOLOVE, D.J., *Understanding Privacy*. Cambridge MA, Harvard University Press, 2008.

MC CARTHY, J., MINSKY, M.L., ROCHESTER N., & SHANNON, C.E., *A proposal for the Dartmouth summer research project On artificial intelligence*, 31 augustus 1955, 13 p., https://doi.org/10.1609/aimag.v27i4.1904.

MOORE Jr., B., *Privacy: Studies in Social and Cultural History*, Londen, Routledge, p. 59-65, ISBN13: 9780394538198.

ORWELL, G., *Nineteen Eighty-Four*, Londen, Secker & Warburg, 1949, 328p.

RIFKIN, J., *The Third Industrial Revolution – How lateral power is transforming energy, the economy, and the world*, New York, Palgrave Macmillan, 2011, 291p., ISBN13: 9780230115217.

SOLOVE, D.J., *Understanding Privacy,* Cambridge MA, Harvard University Press, 2010, 272p, ISBN: 9780674035072.

THOMSON, J.J., "The Right to Privacy", in SCHOEMAN, F.D. (ed.), *Philosophical Dimensions Of Privacy: An Anthology*, Online, Cambridge University Press, 12 december 2009, p. 272-289, https://doi.org/10.1017/CBO9780511625138.012.

VAN OTTERLO, M., & WIERING, M., "Reinforcement Learning and Markov Decision Processes", p. 3-42, in VAN OTTERLO, M., & WIERING, M., *Reinforcement Learning – State of the Art*, Berlijn Heidelberg, Springer-Verlag, 2012, 503 p., https://doi.org/10.1007/978-3-642-27645-3.

WESTIN, A., "The origins of modern claims to privacy", in SCHOEMAN, F.D. (ed.), *Philosophical Dimensions of Privacy: An Anthology*, Online, Cambridge University Press, 12 december 2009, p. 56-74, https://doi.org/10.1017/CBO9780511625138.004.

CAVE, S.,DIHAL, K., & DILLON, S. (eds.), *AI Narratives: A History of Imaginative Thinking about Intelligent Machines*, Oxford, Oxford University Press, 2020, 448p, https://doi.org/10.1093/oso/9780198846666.001.0001.

CAVE, S., DIHAL, K., & DILLON; S. (eds.), *AI Narratives: A History of Imaginative Thinking about Intelligent Machines*, Oxford, Oxford University Press, 2020, 448p, https://doi.org/10.1093/oso/9780198846666.001.0001.

SHARMA, S.K.; BHUSHAN, B. & DEBNATH, N.C. (eds.), *Advances in ubiquitous sensing applications for healthcare, Security and Privacy Issues in IoT Devices and Sensor Networks*, Oxford, Academic Press, 2021, 318p, https://www.sciencedirect.com/book/9780128212554/security-and-privacy-issues-in-iot-devices-and-sensor-networks#book-info.

VOIGT, P. & VON DEM BUSSCHE, A., *The EU General Data Protection Regulation (GDPR) – A Practical Guide*, Cham, Springer, 2017, 383p.

IT GOVERNANCE, *EU General Data Protection Regulation (GDPR): an implementation and compliance guide*, Cambridgeshire, IT Governance Publishing Ltd, 2019, 390p.

KUNER, C., BYGRAVE, L.A., DOCKEY, C. & DRECHSLER, L., (eds.), *The EU General Data Protection Regulation (GDPR): a Commentary*, Oxford, Oxford University Press, 2020, 1393p.

Tijdschriften & papers (online en fysiek)

ABBASI, F., "The pursuit to creating the most human-like AI", *Technative* 10 december 2020, https://technative.io/the-pursuit-to-creating-the-most-human-like-ai/.

AGRAWAL, A., "De risico's en voordelen van AI-ondersteunde intelligente automatisering beheren", CISIN.com , https://www.cisin.com/coffee-break/nl/technology/managing-the-risks-and-benefits-of-ai-assisted-intelligent-automation.html.

AMAZON, "Top 10 Alexa features for spring", *Amazon.com*, https://www.amazon.com/b?node=21576558011.

BARTH, S. & DE JONG, M.D.T., "The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review", *Telematics and Informatics* (vol. 34, issue 7) November 2017, p. 1038-1058, https://doi.org/10.1016/j.tele.2017.04.013.

BEKARA, C., "Security Issues and Challenges for the IoT-based Smart Grid", *Procedia Computer Science* (vol 34) 2014, p. 532-537, https://doi.org/10.1016/j.procs.2014.07.064.

BOONSTRA, S., "Inzicht in data als eerste stap naar effectieve privacy en security", outvie.nl 17 december 2021, https://outvie.nl/kennisbank/effectieve-privacy-security/.

BRANDEIS, L.D., & WARREN, S.D., "The Right to Privacy", Cambridge (USA), *Harvard Law Review* 1890, p. 193-220.

BRANDON, J., "Terrifying high-tech porn: Creepy 'deepfake'videos are on the rise", *Foxnews* 20 februari 2020, https://www.foxnews.com/tech/terrifying-high-tech-porn-creepy-deepfake-videos-are-on-the-rise.

BROUX, A., "Allemaal lachen naar de slimme camera", *DeJuristen.be* 21 maart 2018, https://dejuristen.be/privacy/allemaal-lachen-naar-de-slimme-camera/.

BUOLAMWINI, J., "Artificial Intelligence Has a Problem With Gender and Racial Bias. Here's How to Solve It", *Time* 7 februari 2019, https://time.com/5520558/artificial-intelligence-racial-gender-bias/.

CLAEYS & ENGELS, "GDPR: monsterboete van 35 miljoen euro voor Duits servicecenter van H&M", *LegalNews.be* 13 november 2020, https://legalnews.be/arbeid-sociale-zekerheid/gdpr-monsterboete-van-35-miljoen-euro-voor-duits-servicecenter-van-hm-claeys-engels/.

CLARKE, L., "Forget the hype, we have no idea how to reach human-like artificial intelligence", *Techmonitor* 13 mei 2021, https://techmonitor.ai/technology/we-have-no-idea-how-to-reach-human-like-artificial-intelligence

CLARKE, R., "Introduction to Dataveillance and Information Privacy, and Definitions of Terms", *Xamax Consultancy*, augustus 1997, http://www.rogerclarke.com/DV/Intro.html.

CORREA, M., "What is Legal Technology and how is it Changing our Industry?", *The Lawyer Portal* 29 januari 2019, https://www.thelawyerportal.com/blog/what-is-legal-tech-and-how-is-it-changing-industry/.

DE KETELAERE, M., "Wat is artificiële intelligentie en wat ben ik ermee?", *imec.be* 19 mei 2020, https://www.imec.be/nl/artikelen/wat-is-artificiele-intelligentie-en-wat-ben-ik-ermee.

DELGADO-SEGURA, S., PÉREZ-SOLÀ, C., NAVARRO-ARRIBAS, G.,HERRERA-JOANCOMARTÍ, J., "A fair protocol for data trading based on Bitcoin transactions", *Future Generation Computer Systems* (vol. 107) juni 2020, p. 832-840, https://doi.org/10.1016/j.future.2017.08.021.

DIETZ, F., "Why your AI might be racist and what to do about it", *Towardsdatascience.com* 9 november 2019, https://towardsdatascience.com/why-your-ai-might-be-racist-and-what-to-do-about-it-c081288f600a.

DOSHI-VELEZ, F., KORTZ, M., BUDISH, R., BAVITZ, C., GERSHMAN, S.J., O'BRIEN, D., SCOTT, K., SHIEBER, S., WALDO, J., WEINBERGER, D., WELLER, A., & WOOD, A., "Accountability of AI Under the Law: The Role of Explanation", onuitgegeven, 3 november 2017 (laatst herzien 22 december 2019), 21 p., https://papers.ssrn.com//sol3/Papers.cfm?abstract_id=3064761.

ENGELHARDT, M., & ECKES, J., "From BLM to IBM: Racism and Bias in AI", *MTS.mediencampus.h-da.de* 10 november 2020, https://mts.mediencampus.h-da.de/blog/from-blm-to-ibm-racism-and-bias-in-ai/.

FUCHS, C., "Towards an alternative concept of privacy", *Journal of Information, Communication and Ethics in Society* (vol.9, issue 4) 2011, p.671-687, https://doi.org/10.1108/14779961111191039.

GHOSHAL, A., "Twitter, Pornhub and other platforms ban AI-generated celebrity porn", *TNW* 7 februari 2018, https://thenextweb.com/news/twitter-pornhub-and-other-platforms-ban-ai-generated-celebrity-porn.

GOLDFARB, A. & TUCKER, C., "Shifts in Privacy Concerns." *American Economic Review* (vol. 103, nummer 3) mei 2012, p. 349-53, http://dx.doi.org/10.1257/aer.102.3.349.

GOODMAN, B., & FLAXMAN, S., "EU Regulations on Algorithmic Decision-Making and a 'Right to Explanation'", *AI MAGAZI*NE (vol.38, no. 3) oktober 2017, https://doi.org/10.1609/aimag.v38i3.2741.

GOOLD, B.J., "Surveillance and the Political Value of Privacy", *Amsterdam Law Forum* 2009, https://doi.org/10.37974/ALF.80.

GUETLEIN, M., "Lethal autonomous weapons — Ethical and doctrinal implications", Naval War College Newport 14 februari 2005, onuitg., https://apps.dtic.mil/sti/pdfs/ADA464896.pdf.

IBM, "Deep Blue", *IBM.com*, https://www.ibm.com/ibm/history/ibm100/us/en/icons/deepblue/.

IBM, "What is deep learning?", IBM 1 mei 2020, https://www.ibm.com/cloud/learn/deep-learning.

IBM, "What is Software Development? – Learn the essentials of software development and how it helps businesses innovate and compete*.", ibm.com/topics*, https://www.ibm.com/topics/software-development.

JOBIN, A., LENCA, M., & VAYENA, E., "The global landscape of AI ethics guidelines", *Nature Machine Intelligence* 2 september 2019, p. 389-399, https://www.nature.com/articles/s42256-019-0088-2.

JOHNSON, D., *"What is software? A guide to all of the different types of programs and applications that tell computers what to do",* Business Insider *26 maart 2021*, https://www.businessinsider.com/what-is-software?r=US&IR=T.

KAPLAN, A. & HAENLEIN, M., "Siri, Siri in my Hand, who's the Fairest in the Land? On the Interpretations, Illustrations and Implications of Artificial Intelligence", *Business Horizons* (vol. 62, issue 1) 2018, p.15-25, https://doi.org/10.1016/j.bushor.2018.08.004.

KASPAR, D.V.S., "The Evolution (or Devolution) of Privacy," *Sociological Forum* (vol. 20, nr. 1) 2005, p. 69-92, https://www.jstor.org/stable/4540882.

KAYSER-BRIL, N., "Google apologizes after its Vision AI produced racist results", *Algorithm Watch* 7 april 2020, https://algorithmwatch.org/en/google-vision-racism/.

KERR, O., "The Privacy Paradox", *The Washington Post* 21 mei 2015, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/05/21/the-privacy-paradox/.

KIETZMANN, J., LEE, L.W., MCCARTHY I.P., & KIETZMANN, T.C., "Deepfakes: Trick or treat?", *Business Horizons* 2020, 63(2), p. 135–146, https://www.sciencedirect.com/science/article/pii/S0007681319301600?via%3Dihub.

KRAAIJVANGER, C., "De Vierde Industriële Revolutie is begonnen: Zijn we straks allemaal overbodig?", Scientas.nl 21 oktober 2018, https://scientias.nl/de-vierde-industriele-revolutie-is-begonnen-zijn-we-straks-allemaal-overbodig/.

KRAFT, A., "Microsoft shuts down AI chatbot after it turned into a Nazi", *CBS News* 25 maart 2016, https://www.cbsnews.com/news/microsoft-shuts-down-ai-chatbot-after-it-turned-into-racist-nazi/.

KROLL, J.A., BAROCAS, S., FELTEN, E.W., REIDENBERG, J.R., ROBINSON, D.G., & YU, H., "Accountable Algorithms", *University of Pennsylvania Law Review* (Vol. 165) 2017 Forthcoming, 66 p., https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2765268#.

MICHAEL, G. "The Future of Artificial Intelligence: Benevolent or Malevolent?", *Skeptic Magazine* (vol. 20, nummer 1) 2015, p. 57-60, https://www.researchgate.net/profile/George-Michael-8/publication/294876416_The_Future_of_Artificial_Intelligence_Benevolent_or_Malevolent_Book_Reviews_of_Michio_Kaku_The_Future_of_the_Mind_The_Scientific_Quest_to_Understand_Enhance_and_Empower_the_Mind_and_James_Barrat_Our_F/links/56c5207e08aea564e304dcab/The-Future-of-Artificial-Intelligence-Benevolent-or-Malevolent-Book-Reviews-of-Michio-Kaku-The-Future-of-the-Mind-The-Scientific-Quest-to-Understand-Enhance-and-Empower-the-Mind-and-James-Barrat-O.pdf.

MYCROFT, "The Private and Open Voice Assistant", *Mycroft.ai*, https://mycroft.ai/.

NISSENBAUM, H., "Privacy as Contextual Integrity", *Washington Law Review* (vol.79, nr.1) 2004, p.119-158, https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10.

PAUW, S., "Wat is industrie 4.0?", Salesforce.com 12 augustus 2020, https://www.salesforce.com/nl/blog/2017/05/wat-is-industrie-4-0.html.

PELUSI, N., "The Privacy Paradox", *Psychology Today* November 2007 (laatst herzien 9 juni 2016), https://www.psychologytoday.com/us/articles/200711/the-privacy-paradox.

PERSONA, L., "AI still needs humans to stay intelligent—here's why", *Technative*, 27 april 2022, https://technative.io/ai-still-needs-humans-to-stay-intelligent-heres-why/.

PETITJEAN, F., "België in Europese kop van AI-onderzoek", Computable.be 31 oktober 2018, https://www.computable.be/artikel/nieuws/big-data/6504435/5440850/belgie-in-europese-kop-van-ai-onderzoek.html.

PICKOVER, C.A., *Kunstmatige Intelligentie – Van middeleeuwse robots tot neurale netwerken: Een chronologisch overzicht*, Kerkdriel (Nederland), Librero, 2021, XI, 211 p.

POITRAS, C., "The Privacy Paradox", *UConn Today* 18 augustus 2016, https://today.uconn.edu/2016/08/privacy-paradox/#.

RIDINGS, C., GEFEN, D. & ARINZE, B., "Psychological Barriers: Lurker and Poster Motivation and Behavior in Online Communities", *Communications of the Association for Information Systems* (vol. 18, article 16) 10 juni 2006, p. 329-354, https://doi.org/10.17705/1CAIS.01816.

RIOS, E., "Facebook's AI Seems to Have a Racism Problem", *Mojo Wire* 5 september 2021, https://www.motherjones.com/mojo-wire/2021/09/facebooks-ai-seems-to-have-a-racism-problem/.

RISTESKA STOJKOSKA, B.L., TRIVODALIEV, K.V., "A review of Internet of Things for smart home: Challenges and solutions", *Journal of Cleaner Production* (vol. 140, part 3) 1 januari 2017, p. 1454-1464, https://doi.org/10.1016/j.jclepro.2016.10.006.

ROERDINK, H.W., & VAN DE BUNT, C.A.M., "Boetes onder het regime van de AVG", *P&I* (afl. 6) 6 december 2019, p.252-263, http://www.uitgeverijparis.nl/scripts/read_article_pdf_li.php?id=1001451801&cks=d08df3f5afc3aff42c970faaa4a024649e2bddd7.

ROFF, H.M., "The Strategic Robot Problem: Lethal Autonomous Weapons in War", Journal of Military Ethics (vol. 13, issue 3) 2013, https://doi.org/10.1080/15027570.2014.975010.

SAAD AL-SUMAITI, A., AHMED M.H., & SALAMA, M.M.A., "Smart Home Activities: A Literature Review", *Electric Power Components and Systems* 5 februari 2014, p. 294-305, https://doi.org/10.1080/15325008.2013.832439.

SAMSUNG, "Vraag het Sam!", *Samsung.com*, https://www.samsung.com/be/chatbot-sam/.

SAMSUNG, "What is bixby?", *Samsung.com*, https://www.samsung.com/global/galaxy/what-is/bixby/.

SARWAR, N., "AI Created To Give Ethical Advice Is Being Racist And Murderous", *ScreenRant* 25 oktober 2021, https://screenrant.com/ai-ethical-advice-racist-murderous/.

SCHREYER, M., SATTAROV, T., REIMER, B., & BORTH, D., "Adversarial Learning of Deepfakes in Accounting", *onuitgegeven*, https://doi.org/10.48550/arXiv.1910.03810.

SCHWARTZ, O., "You thought fake news was bad? Deep fakes are where truth goes to die", *The Guardian* 12 november 2018, https://www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth.

SOMERS, G., & FITEN, D., "2 jaar GDPR: Een overzicht van handhaving, waarschuwingen en boetes", *Timelex.eu* 8 juli 2020, https://www.timelex.eu/nl/blog/2-jaar-gdpr-een-overzicht-van-handhaving-waarschuwingen-en-boetes.

SZOLDRA, P., "This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks", *Businessinsider* 16 september 2016, https://www.businessinsider.com/snowden-leaks-timeline-2016-9?international=true&r=US&IR=T.

TADDICKEN, M., "The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure", *Journal of Computer-Mediated Communication* (vol. 19, issue 2) 1 januari 2014, p. 248-273, https://doi.org/10.1111/jcc4.12052.

TECHOPEDIA, *"Software",* techopedia.com, https://www.techopedia.com/definition/4356/software.

TENNERY, A., & CHERELUS, G., "Microsoft's AI Twitter bot goes dark after racist, sexist tweets", *Reuters* 24 maart 2016, https://www.reuters.com/article/us-microsoft-twitter-bot-idUSKCN0WQ2LA.

THOMAS, M., "7 Dangerous Risks of Artificial Intelligence", builtin.com 6 juli 2021 (laatste update: 28 juli 2021), https://builtin.com/artificial-intelligence/risks-of-artificial-intelligence.

TRAN, T., "Scientists Built an AI to Give Ethical Advice, But It Turned Out Super Racist", *Futurism* 22 oktober 2021, https://futurism.com/delphi-ai-ethics-racist.

TURING, A.M., "Computing Machinery and Intelligence", *Mind* 1950, 59, p. 433-460, https://www.cs.mcgill.ca/~dprecup/courses/AI/Materials/turing1950.pdf.

VAN MILTENBURG, O., "Zelflerende AI wint van 's werelds bekendste schaakengine", *Tweakers* 19 april 2019, https://tweakers.net/nieuws/151828/zelflerende-ai-wint-van-s-werelds-bekendste-schaakengine.html.

VANHOOIJDONCK, R., "Top 20 AI-trends om in de gaten te houden in 2021 en daarna" , blog.richardvanhooijdonk.com 16 december 2020, https://blog.richardvanhooijdonk.com/nl/top-20-ai-trends-om-in-de-gaten-te-houden-in-2021-en-daarna/.

VERMEULEN, G., "Explorerend onderzoek naar de aard van essentiële informatiestromen van de Lokale Politie - Een verkenning van enkele cruciale spanningsvelden", *biblio.ugent.be*, 2009.

WACHTER, S. MITTELSTADT, D., & FLORIDI, L., "Transparent, Explainable, and Accountable AI for Robotics", *SCIENCE ROBOTICS* (vol. 2, issue 6) 31 mei 2017, https://doi.org/10.1126/scirobotics.aan6080.

WHITMAN, J.Q., "The two western cultures of privacy: Dignity versus liberty." *Yale Law Journal* (vol. 113, nr. 6) 1 april 2004, p. 1151-1221, https://doi.org/10.2139/ssrn.476041.

WITTES, B. & LIU, J.C., "The privacy paradox: The privacy benefits of privacy threats", *Centre for Technology Innovation at Brookings* mei 2015, 21 p., https://www.brookings.edu/wp-content/uploads/2016/06/Wittes-and-Liu_Privacy-paradox_v10.pdf.

X, "5 belangrijke voordelen van kunstmatige intelligentie", Uniquenewsonline.com 5 oktober 2020, https://www.uniquenewsonline.com/nl/5-belangrijke-voordelen-van-kunstmatige-intelligentie/.

X, "89% van de organisaties schiet dramatisch tekort met data protectie", Ictmagazine.nl 23 februari 2022, https://www.ictmagazine.nl/bedrijfsnieuws/89-van-de-organisaties-schiet-dramatisch-tekort-met-dataprotectie/.

X, "AI in Daily Life", *Exponenta.io* 23 februari 2021, https://exponenta.io/ai-in-daily-life/.

X, "Artificial intelligence: Algorithms face scrutiny over potential bias", *BBC News* 20 maart 2019, https://www.bbc.com/news/technology-47638916.

X, "Autonomous Weapons: An Open Letter From AI & Robotics Researchers", https://futureoflife.org/2016/02/09/open-letter-autonomous-weapons-ai-robotics/.

X, "De vierde industriële revolutie.", Rixels.com 3 november 2020, https://rixels.com/nl/blog/de-vierde-industriele-revolutie/.

X, "De voordelen van het gebruik van AI om jouw bedrijfsbezittingen te beveiligen", stanleysecurity.com 1 juli 2021, https://www.stanleysecurity.com/nl/blog/de-voordelen-van-het-gebruik-van-ai-om-jouw-bedrijfsbezittingen-te-beveiligen.

X, "Smart factories: dé slimme fabrieken van de toekomst", *Mecalux.be* 1 maart 2022, https://www.mecalux.be/blog/smart-factories-slimme-fabrieken-toekomst.

X, "Welke soorten kunstmatige intelligentie (AI) ken jij?", *vboxxcloud.nl* 2021, https://vboxxcloud.nl/blog/soorten-kunstmatige-intelligentie/.

ZALLONE, R., "Artificial Intelligence vs Autonomous Cars vs General Data Protection Regulation", *AEIT International Conference of Electrical Technologies for Automotive* 2020, p. 1-6, https://doi.org/10.23919/AEITAUTOMOTIVE50086.2020.9307410.

ZHAO, Y., YU, Y., LI, Y., HAN, H., & DU, X., "Machine learning based privacy-preserving fair data trading in big data market", *Information Sciences* (vol. 478) april 2019, p. 449-460, https://doi.org/10.1016/j.ins.2018.11.028.

Andere bronnen

Video's

DE HERT, P., *Is privacy passé?*, Universiteit van Vlaanderen (video), https://www.youtube.com/watch?v=SNGfjU75iCI.

Websites

https://noyb.eu/en.

https://ministryofprivacy.eu/.

https://www.medtecheurope.org/.

https://builtin.com/fintech.

https://lawren.io/nl/.