Quickscan relevante projecten en initiatieven voor laadinfrastructuur

Bijlage bij 'Een Public Stack voor laadinfrastructuur'

Waag, februari 2021

Deze rapportage is opgesteld in opdracht van RVO voor de Topsector Energie op verzoek van het programma Digitalisering.

Inhoudsopgave

1. Inleiding

In deze quickscan presenteren we een overzicht van de relevante initiatieven voor een *Public Stack* voor laadinfrastructuur. Dit document dient als bijlage bij de gelijknamige publicatie en kan gelezen worden als een technische aanvulling op de daarin benoemde initiatieven. Aan het identificeren en selecteren van geschikte initiatieven is literatuuronderzoek en een consultatie bij experts voorafgegaan.[1] De quickscan geeft meer detail over de thema's *dataveiligheid, privacy, anonimisering, identiteit, databeheer* en *algoritmen*.

2. Het dataverkeer over de laadinfrastructuur

De Nederlandse laadinfrastructuur bestaat uit verschillende actoren alsmede apparatuur waar deze actoren zich mee bedienen. Deze actoren en apparaten communiceren digitaal met behulp van verschillende standaarden (zoals ISO 15118[2] tussen de auto en de laadpaalexploitant) en protocollen, zoals OCPP[3] tussen het laadpunt en het centrale back-endsysteem van de laadpaalexploitant (zie onderstaande figuur voor een voorbeeld van laadsessiedata), OSCP[4] tussen laadpaalexploitanten en de netbeheerder en OCPI[5] tussen laadpaalexploitanten en de laaddienstverleners. Er is in Nederland en de EU sprake van grote inspanning om deze communicatieprotocollen (verder) te standaardiseren.

Authentication_ID	*Session_ID*	*Charge_Point_Address*	*Charge_Point_ID*	*Charge_Point_ZIP*	*Start_datetime*	*Duration*	*Infra_Provider_ID*	*Service_Provider_ID*	*Volume*
046D562B94880	1612316046D56D2iY5b	Jansdam 14	EVB-P1607254_2	3512HB	2021-01-31T23:45:19	00:31:15	Nuon Public	THENEWMOTION	1.5
3EFAE8C0	1701010010043C0iYPb	Bollenhofsestraat 126	EVB-P1607294_1	3572VT	2021-01-31T23:45:20	09:20:03	Nuon Public	TRAVELCARD	8.43
04BAB92743B80	170101039684392iY0O	Stauntonstraat 119	EVB-P1548447_2	3554EZ	2021-01-31T23:45:21	05:56:28	Nuon Public	ENECO	7.92
3E7098C0	1701010117370C0iY63	Ravellaan 16	EVB-P1607242_1	3533JN	2021-01-31T23:45:22	00:36:09	Nuon Public	TRAVELCARD	1.68
04E8E72B94880	170101100E8E7D2iY7r	Heycopstraat 21	EVB-P1531137_1	3521EN	2021-01-31T23:45:23	09:54:03	Nuon Public	THENEWMOTION	4.75
045C0A8743B84	1701011128C0A82iZa4	Moerasvaren 1	EVB-P1552403_1	3452KA	2021-01-31T23:45:24	02:14:22	Nuon Public	TRAVELCARD	6.25
041F5D9A13C80	1701011141F5D9AiY3s	Paddenstoelenhof 66	EVB-P1552267_2	3451PZ	2021-01-31T23:45:25	14:28:49	Nuon Public	ENECO	6.85

Figuur 1: gestileerd voorbeeld van laadsessiedata afkomstig van meerdere laadpunten.

3. Dataveiligheid

Veiligheid in het dataverkeer is een kernzaak in de governance van een publieke digitale infrastructuur. Hoewel sommige delen van dit digitale ecosysteem steeds sterker beveiligd worden (zoals voor de nieuwste release van OCPP, 2.0.1), is het systeem als geheel nog niet veilig genoeg. De beveiliging is niet op consistente wijze geïmplementeerd in de genoemde protocollen. Zoals voorgesteld door Van Aubel en Poll[6], zou elk protocol van de partijen moeten eisen dat ze een *Transport Layer Security*

[1] Zie voor een overzicht van geraadpleegde experts de colofon van de Public Stack voor laadinfrastructuur.
[2] https://www.iso.org/standard/69113.html
[3] Zie ook Smart Charging Guide van ELaadNL en https://www.openchargealliance.org/protocols/ocpp-201/.
[4] https://www.openchargealliance.org/protocols
[5] https://github.com/ocpi/ocpi
[6] Van Aubel, Pol and Poll, Erik (2020), 'Security of EV-charging protocols', *in submission / draft*, https://www.polvanaubel.com/research/chargego/protocol-security-evaluation/protocol-security-evaluation-draft-2020-03-10.pdf.

implementeren met client- en server certificaten voor iedere vorm van communicatie tussen twee systemen. Transport Layer Security (TLS) is een encryptie-protocol die de communicatie tussen systemen kan beveiligen. De Transport Layer Security zorgt ervoor dat het niet mogelijk is de inhoud van berichten die onderweg zijn in te zien of aan te passen en vraagt om authenticatie van beide betrokken partijen aan de hand van certificaten. De protocollen zouden daarnaast ook specifieke parameters (settings) voor de Transport Layer Security moeten verplichten om de interoperabiliteit tussen technologische diensten van verschillende leveranciers te garanderen.

De protocollen ISO 15118 en OCPP 2.0.1[7] ondersteunen dit encryptieprotocol. Toch is dit encryptieprotocol momenteel niet verplicht, omdat ISO 15118 bijvoorbeeld niet is geïmplementeerd in oudere, nog in omloop zijnde elektrische voertuigen. Alternatieven die hetzelfde als een Transport Layer Security kunnen realiseren, dienen zorgvuldig onderzocht te worden om veilige dataverkeer en -communicatie te kunnen waarborgen. De Transport Layer Security beschermt overigens alleen berichten die onderweg zijn, dus niet de berichten die al zijn 'gearriveerd' bij hun eindstation - vergelijkbaar met videobellen. Deze communicatie is niet *end-to-end* versleuteld: de communicatie is beveiligd van een beller naar de server, maar de communicatie is niet beveiligd op de server zelf. In het geval van de laadinfrastructuur betekent dit dat een laadpaal communicaties kan registreren of wijzigen die niet voor de Charge Point Operator bedoeld zijn. Dit kan voorkomen worden door de inhoud van de data/berichten te versleutelen als vertrouwelijkheid vereist is, of digitaal te ondertekenen zodat de ontvanger er zeker van kan zijn dat het bericht niet tussentijds is gewijzigd.

Bovendien is een *Public Key Infrastructure* (een systeem waarmee uitgiften en beheer van digitale certificaten kan worden gerealiseerd) analoog aan die voor 'https' communicatie vereist om de *Transport Layer Security* met client- en servercertificaten uit te kunnen voeren. Een onafhankelijke partij zou een dergelijke infrastructuur kunnen beheren. ElaadNL pleit hiervoor in het specifieke geval van ISO 15118:

> De visie van ElaadNL is het streven naar een open PKI voor ISO 15118 die de weg plaveit voor optimaal gebruik en profijt voor iedere EV-gebruiker en brede acceptatie daarvan binnen de internationale EV-laadmarkten.[8]

In ieder geval staat het afzonderlijk benaderen van beveiliging binnen ieder protocol een globale, consistente benadering van de beveiliging voor het hele ecosysteem in de weg. Dit vraagt om betere coördinatie en afstemming tussen de verschillende partijen die de protocollen definiëren.

---

[7] De nieuwste versie van OCPP; zie ook https://www.openchargealliance.org/about-us/ocpp-and-gdpr/

[8] ElaadNL (2018), *Exploring the public key infrastructure for ISO 15118 in the EV charging ecosystem*, https://www.elaad.nl/uploads/files/Exploring_the_PKI_for_ISO_15118_in_the_EV_charging_ecoystem_V1.0s2.pdf.

4. Privacy in het dataverkeer

De zorgen onder veel mensen over het verlies van controle over hun persoonlijke data is de laatste jaren terecht toegenomen. Het is onduidelijk wat er met de vergaarde data gebeurt: de data wordt bijvoorbeeld doorverkocht aan derden en ingezet voor (politieke) marketing doeleinden. Naar privégegevens zoals adres, geboortedatum en zo nu en dan het burgerservicenummer wordt regelmatig gevraagd. Daarnaast worden er grote hoeveelheden data verzameld die het gedrag en de voorkeuren van de online burger in kaart brengen.

Privacy heeft meer aandacht gekregen sinds de inwerkingtreding van de AVG. Dat valt ook op te maken uit de *release* voor OCPP 2.0.1:

> OCPP 2.0.1 heeft een functionaliteit toegevoegd die implementeerders in staat stelt te voldoen aan de Algemene Verordening Gegevensbescherming (AVG). De verantwoordelijkheid om aan deze verordening te voldoen ligt echter niet bij het protocol of de Open Charge Alliance (OCA), maar bij de uitvoerders van het protocol. Dit vereist dat uitvoerders van OCPP op de hoogte zijn van de wet- en regelgeving en de benodigde maatregelen nemen.[9]

De AVG vereist dat persoonsgegevens alleen worden verwerkt als het strikt noodzakelijk is (dataminimalisatie) en alleen door de beoogde ontvangers. Het is daarom noodzakelijk om te bepalen wie (welke actor in de architectuur) toegang moet hebben tot welke data. Dit zou bijvoorbeeld betekenen dat gegevens moeten worden versleuteld wanneer deze gegevens via (centrale) knooppunten in het netwerk moeten worden verzonden voordat ze de beoogde ontvanger bereiken.

Volgens Pol van Aubel en Erik Poll ontbreekt een globale visie op deze kwestie.[10] De verschillende protocollen geven niet precies aan welke informatie persoonlijk is en wie deze zou moeten kunnen inzien of gebruiken. Een breed gedeelde, wereldwijde visie op privacy en veiligheid in de laadinfrastructuur zou de uitwisseling van gegevens op een AVG-conforme manier kunnen vergemakkelijken.

5. Anonimiseringstechnieken

Kijken we naar de privacy met betrekking tot datasets met de laadgegevens van vele gebruikers, dan is het relevant om anonimiseringstechnieken te beschouwen. Dit zijn technieken die enerzijds voldoende informatie uit de dataset verwijderen zodat individuele heridentificatie moeilijk is en anderzijds de bruikbaarheid van de informatie-inhoud behouden. Een relevante techniek is bijvoorbeeld *spatial cloaking*, waarbij de

[9] https://www.openchargealliance.org/about-us/ocpp-and-gdpr/
[10] Van Aubel, Pol and Poll, Erik. "Security of EV-charging protocols". In submission / Draft. https://www.polvanaubel.com/research/chargego/protocol-security-evaluation/protocol-security-evaluation-draft-2020-03-10.pdf

exacte locatie van de gebruiker wordt 'vervaagd' naar een breder ruimtelijk gebied om privacy te behouden (een vergelijkbare anonimiseringstechniek is *temporal cloaking*).[11]

Deze kunnen van betekenis zijn gezien de spanning tussen het belang van grote hoeveelheden data voor adequaat beheer van het energienetwerk en aansturing van alternatieve bedrijfsmodellen enerzijds, en de behoefte aan privacy van gebruikers anderzijds.

Anonimiseringstechnieken streven ernaar twee tegengestelde belangen in evenwicht te brengen: de bruikbaarheid van gegevens te maximaliseren en tegelijkertijd de privacy van de gebruiker te beschermen. Vaak proberen ze dit te bereiken door genoeg informatie uit de dataset te verwijderen of te wijzigen zodat heridentificatie van individuen moeilijk is, maar de informatie-inhoud nog steeds relevant voor gebruik blijft.

Een voor de hand liggende manier waar doorgaans op wordt ingezet is om alle primaire identificerende gegevens uit de data te verwijderen, zoals bijvoorbeeld naam of burgerservicenummer. Er worden wel gebruiker-ID's gecommuniceerd (in het geval van laadinfra gaat dat om RFID-waarden uit de laadpas; dit is de eerste kolom in Figuur 1) de persoonsinformatie ontbreekt. Deze techniek garandeert echter niet dat buitenstaanders toch personen kunnen identificeren. Hoewel sommige gegevens op zich niet-identificerend zijn (locatie = Jansdam 14, of tijdstip, of aantal auto's = 2), kunnen ze als *quasi-identifier* optreden doordat ze in combinatie met andere niet-identificerende gegevens opeens wél wijzen naar één gezin. Dit wordt 'correlatie-analyse' genoemd en is voor partijen met veel data een belangrijk risico.

Een bekend voorbeeld is het geval van gouverneur Weld uit Massachusetts, wiens medische dossiers beschikbaar waren in een openbaar beschikbare dataset van patiënten. Van deze set werd aangenomen dat deze anoniem was, omdat deze geen persoonsgegevens bevatten. Gouverneur Weld woonde in Cambridge, Massachusetts. Volgens de Cambridge Kiezerslijst hadden zes mensen zijn specifieke geboortedatum; slechts drie van hen waren mannen, hij was echter de enige met een 5-cijferige postcode.[12]

Er zijn anonimiseringstechnieken die dit probleem van *quasi-identifiers* aanpakken. Deze proberen de unieke combinaties van *quasi-identifiers* te elimineren en worden 'syntactische privacymodellen' genoemd.[13] Daartegenover staan 'semantische privacymodellen'. Deze privacymodellen houden geen rekening met *quasi-identifiers*, maar proberen de hoeveelheid kennis die een aanvaller opdoet over bepaalde individuen

---

[11] Chow, Chi-Yin (2008), Spatial Cloaking Algorithms for Location Privacy, *Encyclopedia of GIS*.
[12] Sweeney, Latanya (2002), 'K-Anonymity: A Model for Protecting Privacy', *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 10*(5), 557–570.
[13] De bekendste syntactische privacymodellen zijn *k*-anonimiteit, ℓ-diversiteit en *t*-nabijheid. Li, Ninghui; Li, Tiancheng & Venkatasubramanian, Suresh (2007), '*t*-Closeness: Privacy Beyond *k*-Anonymity and ℓ-Diversity', *Proceedings of IEEE 23rd International Conference on Data Engineering (ICDE '07)*.

in de dataset zo veel mogelijk te beperken. De meest bekende techniek van dit type heet 'differentiële privacy'.[14] Differentiële privacy werkt door gecontroleerde ruis toe te voegen aan de output van de te publiceren datasets. Differentiële privacy wordt gebruikt door bedrijven zoals Apple en door de Amerikaanse volkstelling bij het publiceren van hun rapporten.

Anonimiseringstechnieken proberen te voorkomen dat aanvallers kennis opdoen over gevoelige gegevens. Kijkend naar de EV-laadinfrastructuur zouden met name de locaties en tijden van de laadsessie gevoelig kunnen zijn. Geolocatiegegevens zijn gevoelige gegevens, zoals blijkt uit een studie over ongeveer vijftien maanden aan gegevens over menselijke mobiliteit (van een mobiele netwerkoperator) van anderhalf miljoen individuen.[15] Uit deze studie bleek dat in een dataset waarin de locatie van een persoon elk uur wordt gespecificeerd, met een ruimtelijke resolutie gelijk aan die van de antennes van een telecomprovider, vier spatio-temporele punten voldoende zijn om 95% van de individuen als uniek te identificeren.

6. Privacy en identificatie

De accumulatie van privacygevoelige informatie kan vaak sterk beperkt worden door het verstrekken van identificerende data in eerste instantie – zoals bij het registreren van een laadsessie – al te minimaliseren. Dit kan door de verschillende datastromen en identificerende informatie zoveel mogelijk te ontkoppelen en gespreid te beheren. Bij de identificatie en authenticatie (het aantonen van iemands recht, bijvoorbeeld om te gaan opladen) worden de relevante gegevens instantaan gekoppeld zonder dat individuele actoren de gecombineerde gegevens kunnen bekijken. Ofwel, slechts op initiatief van de eindgebruiker worden de afzonderlijke identifiers gekoppeld. Wij gaan hieronder in op enkele verschillende projecten die een decentraal beheer van 'linkable identifiers' gebaseerd zijn. Alle genoemde initiatieven geven de gebruiker tenminste een van deze twee strategieën: *eigen beheer* van persoonlijke data en controle over de transacties daarvan, en *zeer beperkt gebruik* van deze data in een transactie.

6.1. IRMA: Attribute-based credentials

Een eerste noemenswaardige applicatie is IRMA,[16] een acroniem van 'I Reveal My Attributes'. IRMA kan worden gebruikt om onszelf te authentiseren met behulp van slechts de minimaal benodigde gegevens. In IRMA worden stukjes identificerende informatie (zoals leeftijd en naam) 'attributen' genoemd. De attributen bevinden zich alleen op de telefoon van de gebruiker. Bij authenticatie geeft IRMA de gevraagde attributen alleen vrij als de gebruiker daarmee instemt (selectieve openbaarmaking).

[14] Dwork, Cynthia (2006), 'Differential Privacy', Proceedings of the 33rd international conference on Automata (2), 1-12.
[15] De Montjoye, Yves-Alexandre; Hidalgo, César A.; Verleysen, Michel & Blondel, Vincent D. (2013), 'Unique in the Crowd: The Privacy Bounds of Human Mobility', *Scientific Reports (3)*.
[16] https://privacybydesign.foundation/irma-en/

Zulke attributen worden verstrekt als 'credential' door een uitgever van deze attributen. De uitgever is een specifieke autoriteit: het attribuut 'woonplaats' kan bijvoorbeeld digitaal worden ondertekend door een gemeente. Deze zet de attributen om in de vorm van een credential, en voorziet de credential van een blinde digitale handtekening. Met deze handtekening is de oorsprong en de authenticiteit van het credential te controleren. De handtekening is 'blind', waardoor de uitgever de uiteindelijke vorm van het credential niet ziet. Bovendien kan hij daardoor niet nagaan waar de credential allemaal voor gebruikt wordt.

Anders dan binnen een gecentraliseerde architectuur heeft de gebruiker eenmalig contact met de uitgever om zijn attributen te verifiëren. Daarna worden de credentials decentraal opgeslagen – op je telefoon. Alleen de gebruiker kan zijn credentials gebruiken, zonder dat een derde partij het gebruik daarvan kan raadplegen.

De twee principes van IRMA, selectieve openbaarmaking van attributen en digitale handtekeningen, kunnen van betekenis zijn voor de aanpak van het verzamelen van gegevens over energieverbruik. Het principe van selectieve openbaarmaking zorgt ervoor dat niet-noodzakelijke persoonlijke gegevens niet worden verzonden (bijvoorbeeld alleen de locatie, en niet ook de naam). Het principe van de digitale handtekening garandeert dat de attributen authentiek zijn (bijvoorbeeld dat de locatie is uitgegeven door een lokale autoriteit, of dat de gegevens over energieverbruik daadwerkelijk afkomstig zijn van een bepaalde buurt).

6.2. W3C: Decentalised Identifiers en Verifiable Credentials

Uit de koker van het World Wide Web Consortium (W3C), een non-profit-organisatie die de webstandaarden voor het wereldwijde web ontwerpt, komen twee relevante specificaties. Decentralised Identifiers[17] kunnen willekeurige objecten en subjecten identificeren: personen, organisaties, voorwerpen, datamodellen, abstracte entiteiten, enzovoorts. Verifiable Credentials[18] zijn credentials (zie paragraaf 6.1) ontworpen om voor Internet-of-Things-assets ingezet worden: hiermee kan bijvoorbeeld bij smart meters, zonnepanelen, EV-auto's e.d. worden geverifieerd dat bepaalde data vanaf een bepaald object komt. Beide standaarden zijn in ontwikkeling en richten zich vooral op het ontwikkelen van een geschikte (programmeer)taal en datamodellen; het uitwerken van protocollen en tools valt vooralsnog buiten de scope.

6.3. Solid

Solid[19] voldoet, net als IRMA, aan de vereisten van een applicatie goedgekeurd door MyData (zie 'Databeheer'), en gaat nog een stapje verder. Solid streeft naar het ontkoppelen van data aan (sociale) applicaties, zodat gebruikers de controle over hun

[17] https://www.w3.org/TR/did-core/
[18] https://www.w3.org/TR/vc-data-model
[19] https://solidproject.org/use-solid/

data kunnen behouden en data geen eigendom is van en opgesloten zit in zogeheten 'pods' (datakluizen). Deze ontkoppeling zorgt er ook voor dat verschillende applicaties dezelfde gegevens kunnen gebruiken, zonder dat ze deze apart moeten verzamelen.

De opslag van persoonsgegevens wordt niet gehost door service providers (zoals bij MyData), maar gehost in een ruimte (cloud) die de gebruiker direct beheert. De technische werking is als volgt: afzonderlijke data-items worden opgeslagen in standaard formats en aan elkaar gekoppeld volgens het principe van *Linked Data*.[20] Deze formats zijn al jaren in gebruik in het domein van Semantic Web en zijn gestandaardiseerd door het W3C.[21]

Serviceproviders moeten vervolgens toestemming vragen om toegang te krijgen tot de gegevens in deze ruimtes, en dergelijke machtigingen kunnen bovendien eenvoudig worden ingetrokken. De interoperabiliteit van data tussen verschillende diensten wordt afgedwongen door het feit dat ze allemaal toegang moeten hebben tot een *Solid-compliant* gegevensopslag.

Deze mogelijkheid doorbreekt het monopolie van enkele providers die over alle gebruikersgegevens beschikken. Aangezien de opslag van data onder controle is van de gebruiker, biedt Solid ook een direct hogere mate van privacy. Solid stelt gebruikers in staat om te bepalen hoeveel informatie ze met derden willen delen. Er wordt dus wel van gebruikers gevraagd duidelijk te begrijpen hoe ze hun eigen privacy kunnen beschermen (net als in het geval van MyData). Een mogelijk risico is daarbij dat gebruikers door middel van financiële prikkels alsnog toegang kunnen verlenen tot gevoelige persoonlijke gegevens.

Solid baseert zich op enkele degelijke technieken en principes, maar lijkt als project niet erg actief ontwikkeld of gebruikt te worden. Het initiatief dient vooral als symbolische inspanning die de weg kan plaveien voor toekomstige ontwikkelingen.

6.4. Self-Sovereign Identity

Self-sovereign identity (SSI) is een benadering voor het beheer van identiteiten en persoonsgegevens. De eigenaar van de gegevens beschikt over de sleutel om anderen toegang tot data te verschaffen die is opgeslagen in een eigen 'kluis', zoals bij Solid. Een verschil met attribute-based credentials (zie IRMA) is dat de uitgifte niet via een geautoriseerde instantie loopt. 'Self-sovereign' verwijst dan ook naar het idee dat een individu geheel baas is over de eigen identiteit en haar attributen. Om toch gewicht toe te kennen aan claims maakt SSI gebruik van 'peer attestations': jouw gelijken bevestigen stukjes van je identiteit, die daarmee niet institutioneel is maar relationeel. De rationale achter SSI is echter controversieel. Prof. Mireille Hildebrandt acht de toepasbaarheid zeer beperkt omdat we in onze samenleving nu eenmaal rechten en plichten langs

[20] https://www.w3.org/standards/semanticweb/data
[21] https://www.w3.org/

juridische weg formaliseren met daarbij een centrale rol voor autoriteiten.[22] Duidelijk moet zijn wat de rechtmatigheid en het rechtsgevolg zijn van een claim of beslissing; dat kan niet met zelf-toegekende categorieën en claims. Ook de (op blockchain rustende) architectuur van SSI kent diverse zwaktes. Er vinden echter snelle ontwikkelingen[23] plaats in het ontwerp van SSI-systemen die aan de genoemde bezwaren mogelijk tegemoet komen en zouden kunnen bijdragen aan het ontwerp van permissieloze netwerkinfrastructuren (zie hiervoor de discussie bij 'Bruikbaarheid van blockchain').

7. Datamanagement

Dit hoofdstuk gaat in op technische methoden van datamanagement, die oplossingen bieden voor opslag en toegangsbeheer tot data. Ook hierbij zijn de principes van 'decentraliteit' en het versterken van de positie van de eindgebruiker leidend. De manier waarop deze worden benaderd en geïmplementeerd verschilt echter per genoemde techniek/initiatief.

7.1. Datamanagement door middel van blockchain

Een mogelijkheid voor datamanagement die vaak wordt voorgesteld de afgelopen jaren is door middel van Distributed Ledger Technologies (DLT): decentraal beheerde databases. DLT, en blockchains in het bijzonder, worden verkondigd als de technologie waarbij transparantie en openheid centraal staat; iedereen kan de log zien van transacties die plaatsvinden en iedereen kan een transactie uitvoeren. De transacties worden ongewijzigd op de blockchain vastgelegd zonder dat er centraal bestuur of toezicht nodig is.

Daarbij komt dat de transacties kunnen worden geïmplementeerd via *smart contracts,* een transactie protocol die de termen uit een contract automatisch uitvoert en door alle schakels in het decentrale netwerk kan worden gevolgd. De uitvoering ervan wordt in gang gezet door de DLT zodra aan de voorwaarden voor de inwerkingstelling van het contract is voldaan, zonder tussenkomst van de betrokken partijen, noch van een externe autoriteit. De transacties binnen een blockchain zijn volledig transparant en zouden daarnaast markten efficiënter kunnen maken door transactiekosten en het risico op conflicten potentieel te verlagen.

In Nederland is de Odyssey-hackathon,[24] waarvan in november 2020 de tweede editie plaatsvond, een initiatief waar sterk wordt ingezet op de mogelijkheden van blockchain.

---

[22] Mireille Hildebrandt, "De soeverein is niet thuis. Self-Sovereign Identity (SSI) en Attribute Based Credentials (ABC)", *Ars Aequi* juli/augustus 2019

[23] Bijvoorbeeld Quinten Stokkink, Dick Epema en Johan Pouwelse, "A Truly Self-Sovereign Identity System", Arxiv.org (2020) https://arxiv.org/pdf/2007.00415.pdf; Markus Luecking, Christian Fries, Robin Lamberti en Wilhelm Stork, "Decentralized Identity and Trust Management Framework for Internet of Things", *2020 IEEE International Conference on Blockchain and Cryptocurrency* (2020).

[24] https://www.odyssey.org/momentum/. In de recentste Odyssey hackathon zijn twee energiegerelateerde thema's aangedragen, beide zeer data-georiënteerd van aard: (1) Hoe

Volgens Odyssey is het een *"nieuwe vorm van gemeenschappelijke openbare digitale infrastructuur een alternatief voor de huidige praktijk waarin de belangrijke delen van de informatie- en communicatie-infrastructuur eigendom zijn van overheden en bedrijven. Het is een gedeelde openbare digitale infrastructuur die van niemand is en tegelijkertijd door iedereen wordt gebruikt en waarbij elk nieuw open protocol een nieuwe markt ontsluit. Het is een digitale infrastructuur waarop massale samenwerking kan floreren."*[25]

In Nederland wordt al verder geëxperimenteerd met energie 'handel' op basis van blockchain, bijvoorbeeld bij het Gorinchemse 'Hoog Dalem'-project van Stedin.[26] In deze praktijkproef wisselen vijftien woningen in de wijk met behulp van blockchain-technologie lokaal opgewekte energie onderling uit. Via slimme apparatuur wordt actief gestuurd op het realtime energieaanbod en verbruik, en zo worden de huishoudens grotendeels zelfvoorzienend. Hoog Dalem is een van de projecten omschreven in de whitepaper *Layered Energy System*,[27] waarin Stedin samen met energieconsultant Energy21 een duurzaam en lokaal energiemarktmodel ontwerpt. Een vergelijkbaar project is Jouliette[28], in 2017 opgezet vanuit duurzame community De Ceuvel in Amsterdam in samenwerking met Alliander en Spectral. Ook hier werd blockchain-technologie gebruikt voor *peer-to-peer* energiehandel. Het project leidde tot de publicatie van een whitepaper[29] door Spectral en een aantal vervolgprojecten[30].

Internationaal zijn er ook veel ontwikkelingen. Relevant om te benoemen is Energy Web[31] (EW), een wereldwijde non-profitorganisatie en partnership van lokale netbeheerders en andere partijen die ernaar streeft een *low-carbon*, klantgericht elektriciteitssysteem in gang te zetten op basis van blockchain en andere gedecentraliseerde technologieën. Hun streven is onder andere om een openbare digitale infrastructuur beschikbaar te stellen om de invoering van nieuwe commerciële technologische oplossingen te versnellen. In 2019 lanceerde Energy Web de zogeheten Energy Web Chain[32], 's werelds eerste open-source blockchain-platform voor bedrijven afgestemd op de energiesector. Ook bieden ze het Energy Web Decentralized Operating System (EW-DOS), een 'blockchain-plus' voor gedecentraliseerde oplossingen. Daarnaast ontwikkelden ze in 2017 Tobalaba: een openbaar toegankelijk testnetwerk

kunnen we consumenten stimuleren om de vraag naar en de productie van energie te communiceren, zodat alle belanghebbenden het net in evenwicht kunnen houden? (2) Hoe ontwerpen we infrastructuur voor zogenoemde 'Smart Meter Data Impact', om realtime gegevensverzameling van slimme meters te decentraliseren en te openen?

[25] https://www.odyssey.org/about/

[26] https://www.stedin.net/over-stedin/duurzaamheid-en-innovaties/een-klimaatneutrale-samenleving/hoog-dalem

[27] https://ileco.energy/wp-content/uploads/2019/08/layered-energy-system-white-paper.pdf

[28] https://www.jouliette.net/

[29] Deze richt zich op kansen en risico's van het gebruik van blockchain in het energiedomein, met name op 'initial coin offerings' (ICO's): de publieke 'beursgang' van een nieuwe blockchain-gebaseerde coin. Het stuk is in te zien op https://spectral.energy/news-3/ico-shortcomings/.

[30] https://www.jouliette.net/next.html.

[31] https://www.energyweb.org/

[32] https://www.energyweb.org/technology/energy-web-chain/

voor de ontwikkeling van decentrale, op blockchain gebaseerde applicaties binnen de energiesector.[33]

7.2. Bruikbaarheid van blockchain

De vraag naar nut en noodzaak van de inzet van blockchaintechnologie hangt af van de omstandigheden waarin de blockchain moet opereren. Blockchain veroorzaakt een paradigmaverschuiving, aangezien het partijen die elkaar niet noodzakelijkerwijs vertrouwen in staat stelt om toch (commerciële) transacties uit te voeren. Het ontbreken van de behoefte aan vertrouwen maakt een blockchain daarom vernieuwend. Op deze manier kan elke partij zich bij een blockchain aansluiten en transacties aangaan met andere partijen, zoals bijvoorbeeld het geval is bij bitcoin. De manier waarop 'vertrouwen' hier wordt geïnterpreteerd is echter beperkt. Het probleem dat blockchain oplost (of wil oplossen) is dat infrastructuur een eigenaar nodig heeft om te beslissen wat valide transacties zijn en wie welke rechten heeft. Blockchain maakt het mogelijk om het eigendom en de operaties van de techniek decentraal te maken zonder centrale autoriteit. Dat is echter, zou je kunnen zeggen, een zwaar middel in een samenleving die vaak juist goed functioneert doordat er vertrouwensstructuren zijn: vertrouwen in instituties en vertrouwen tussen mensen onderling.

Niet alle blockchains zijn echter ingericht op functioneren in zo'n 'trustless' context. Een relevant onderscheid is tussen publieke en private, ook wel 'permissieloze' (publiek) en geautoriseerde (privaat) blockchains genoemd. In een publieke blockchain kan iedereen meedoen aan het netwerk als knooppunt; in de private blockchain worden de blockchain-kernfuncties (validatie en mining) alleen uitgevoerd door betrokken belanghebbenden. Merk op dat publiek hier 'openbaar' in enige zin betekent (toegankelijk voor iedereen mits je over de juist kennis en middelen beschikt), en dus andere lading heeft dan publiek als duiding voor ofwel overheidsgerelateerd ofwel in de zin van 'publieke waarden'. Een publieke, permissieloze blockchain is enerzijds het elegantst omdat het een open netwerk creëert. Het introduceert qua governance echter een ingewikkelde puzzel en schiet daarin vaak (in afgebakende toepassingen) zijn doel voorbij. In die gevallen, zoals ook in veel energy grids, volstaat het om met geautoriseerde DLTs (zie 'Databeheer door middel van blockchain') te werken die ook de governance overzichtelijker maken. Zo kan het organiserend consortium controle houden over wie er aan de blockchain mag deelnemen. Ondernemingen kiezen meestal voor een geautoriseerde blockchain, waarbij ze strikte controle kunnen uitoefenen op de voorwaarden voor transacties en validatie. Equigy, een platform dat consumenten in staat stelt hun overschot aan zelf opgewekte energie te verkopen op de balanceringsmarkt, is bijvoorbeeld gebaseerd op een private Hyperledger-blockchain.[34]

Er zijn ook blockchains die zich positioneren op een spectrum tussen 'volledig publiek' en 'volledig privaat'. De eerder aangehaalde Energy Web Chain is bijvoorbeeld een

[33] Zie voor meer informatie over de lancering van Tobalaba https://www.prweb.com/releases/2017/11/prweb14891767.htm.
[34] https://www.emerce.nl/nieuws/ren-kerkmeester-equigy-breken-miljardenmarkt-open

openbaar toegankelijk netwerk (elke partij kan transacties indienen), maar met geautoriseerde validators (alleen aangewezen knooppunten kunnen de transacties valideren). Normaal gesproken zijn de prestaties van (semi-)private blockchains beter dan publieke, omdat het consensus-algoritme[35] vereenvoudigd kan worden. Energy Web Chain maakt bijvoorbeeld gebruik van een Proof-of-Authority-consensusmechanisme met een capaciteit voor 30 keer prestatieverbetering en twee tot drie keer lager energieverbruik vergeleken met Ethereum.[36] Andere voordelen van (semi-)private blockchains zijn bijvoorbeeld de mogelijkheid om een bepaalde mate van privacy te implementeren (bijvoorbeeld in het geval dat transacties betrekking hebben op gegevens van residentiële klanten) en de minder veeleisende client software waar deze blockchains gebruik van maken (dat is bijvoorbeeld relevant als apparaten met beperkte middelen, zoals slimme meters, op het netwerk aangesloten moeten worden).

Het grootste nadeel van (semi-)private blockchains is dat decentralisatie tot op zekere hoogte niet mogelijk is. Bovendien is de kans groot dat sommige actoren in dit netwerk samenspannen om het kwaadwillig te beïnvloeden. Elke blockchain is namelijk kwetsbaar wanneer meer dan 50% van de knooppunten kwaadaardig is - in een (semi-) private blockchain waarbij het aantal knooppunten gelimiteerd is, is dit risico groter. Wanneer het aantal partners dat een blockchain moet reguleren laag is, vervallen de voordelen en zijn andere technische oplossingen, gepaard met andere governance-modellen, al snel geschikter.

7.3. Datacommons

Een andere, meer waarden- dan technologie-gedreven benadering van datamanagement is om gegevens beschikbaar te stellen in dienst van het 'algemeen belang': een benadering volgens het concept van datacommons.[37] Dit is een oplossing voor databeheer waarbij stakeholders onder diverse (dynamische) voorwaarden data delen.[38] Het gebruik van datacommons voor gegevensbeheer wordt ook door Mozilla Foundation aangedragen als alternatief om ongelijke machtsverhoudingen in eigenaarschap van data tegen te gaan.[39]

---

[35] Het consensus-algoritme dat wordt gebruikt om blokken aan de keten toe te voegen. Zo gebruikt bitcoin proof-of-work, wat erg traag en resource-intensief is, terwijl andere blockchains snellere consensus-algoritmen gebruiken, zoals proof-of-stake.

[36] Energy Web Foundation (2019), *The Energy Web Chain*: *Accelerating the energy transition with an open-source, decentralized blockchain platform,* https://energyweb.org/reports/the-energy-web-chain/.

[37] Zie voor een discussie Bril, Teuntje, "Data als publiek goed. Een politiek-filosofische analyse". Amsterdam: Waag (2019). https://beleidslab.waag.org/publicatie/data-als-publiek-goed-een-politiek-filosofische-analyse/

[38] Schouten, Socrates & Veenkamp, Judith (2019), *Mobiliteitslab fietsdatacommons: Naar een publieke data-infrastructuur waarmee de stad en haar burgers grip houden op de (fiets)mobiliteit*, https://waag.org/sites/waag/files/2020-03/Definitief%20verslag%20Mobiliteitslab%20Fietsdatacommons_0.pdf.

[39] Zie voor de volledige publicatie en voor andere alternatieven (waaronder een data co"operatie en een data *trust*): Mozilla Insights ism Ana Brandusescu & Jonathan van Geus (2020), *Shifting Power Through Data Governance,* https://foundation.mozilla.org/en/initiatives/data-futures/data-for-empowerment/#10-data-governance-approaches-explored.

Volgens de definitie die is aangenomen in het DECODE-project[40] zijn datacommons:

- Geproduceerd door een gemeenschap;
- Gebruikt door de gemeenschap die het heeft geproduceerd op een manier dat het het bestaan van de gemeenschap versterkt;
- Gecontroleerd door de gemeenschap met door hen opgestelde regels (een definitie voor de bescherming van deze gegevens van de gemeenschap tegen externe partijen daarbij inbegrepen).

In dit scenario is het van fundamenteel belang dat de gemeenschap een actieve rol speelt in de 'levenscyclus' van de datacommons, met name in het beheer ervan. Datacommons zijn geenszins verenigbaar met de werkwijze van platformbedrijven waarbij doorgaans sprake is van een totaal gebrek aan controle door de gebruiker over de eigen data. Datacommons veronderstellen een geraffineerde *governance*: hoe wordt bepaald hoe men data kan genereren, wanneer deze wordt toegevoegd aan de commons? Wie gaan er over deze regels en protocollen: de energiecoöperatie, netbeheerder, gemeente?

Datacommons verwijst dus niet naar een geaggregeerde dataset, maar beschrijft de systematiek en spelregels van het data-ecosysteem als geheel. Datacommons gaat ook een stap voorbij de noties van dataportabiliteit en -interoperabiliteit (vereisten vanuit de AVG en andere verordeningen). Een voorbeeld uit een ander domein waarmee dat onderscheid geïllustreerd kan worden is de Europese *Payment Service Directive 2* (PSD2), waarmee derde partijen toegang tot de betaaldata van individuen kunnen krijgen om zo de onderlinge concurrentie tussen partijen te vergroten. Een valkuil van PSD2 is dat deze vooral vanuit marktwerking is beredeneerd: het verhoogt de mogelijkheid tot concurrentie en vermindert de kans op *vendor lock-in*, maar maakt persoonlijke data eerder *meer* tot handelswaar dan minder. Dit houdt per saldo het probleem van asymmetrische informatie- en machtsverhoudingen dat bestaat tussen gebruikers en platforms in stand. De meeste principes van datacommons zijn bij PSD2 dus niet overwogen of toegepast. Hetzelfde risico bestaat in de energiemarkt. Het Energy Web-initiatief zet bijvoorbeeld in op autonomie van gebruikers, maar lijkt hierbij de burger vooral als rekenmachine te duiden: "Gebruikers van blockchain-netwerken en -toepassingen hebben de macht om te bepalen hoe hun gegevens worden gebruikt en opgeslagen. Huishoudens kunnen hun meetgegevens anoniem aanbieden aan een reeks retailaanbieders om het beste retailtarief te krijgen, of om hun verbruiksprofiel te verkopen aan energie-efficiëntie bedrijven in ruil voor de kans om goederen en diensten aan te bieden".[41] Maar snappen deze gebruikers wel de risico's van het verstrekken van hun data aan deze commerciële derden? De aanstaande flexibilisering van ons

[40] DECODE project (2018), *Technopolitical Democratization and Digital Commoning: the Case of the Digital Democracy and Data Commons (DDDC) pilot,* https://www.decodeproject.eu/publications/technopolitical-democratization-and-digital-commoning-case-digital-democracy-and-data.
[41] Energy Web Foundation. "The Energy Web Chain". Version 2.0 | July 2019. https://energyweb.org/reports/the-energy-web-chain/

energiesysteem zal op korte termijn een stijgende vraag naar digitale diensten in de hand werken. Grote hoeveelheden data worden gegenereerd. Waar data over bijvoorbeeld het gebruik van laadinfrastructuur zich tot dusver beperkt tot gegevens over bijvoorbeeld frequentie en intensiteit van het gebruik, zal deze in de toekomst steeds meer kunnen informatie blootgeven over de gebruiker van de dienst. Zeker naarmate het aantal EV-rijders toeneemt zal de laadinfrastructuur grotere hoeveelheden data over het elektriciteitsverbruik voortbrengen. Het is belangrijk dat deze (geaggregeerde) data in beheer blijft van de gemeenschap of buurt blijft die deze produceert.

7.4. MyData

MyData[42] is een non-profitorganisatie met als visie om gebruikers controle te geven over hun eigen persoonsgegevens, die op dit moment worden verzameld en bewaard door (enkele) organisaties. Dit streven moet gegevensbescherming afdwingen en tegelijkertijd gebruikers aanmoedigen om hun gegevens op een veilige manier te delen met andere bedrijven om van hun diensten gebruik te maken. Een sterke gegevensbescherming en transparantie bij het gebruik van persoonsgegevens moet het vertrouwen tussen individuen en organisaties vergroten en kansen creëren voor de ontwikkeling van innovatieve diensten op basis van persoonsgegevens.[43]

De belangrijkste elementen van de aanpak van MyData:

- Mensen krijgen controle over hun gegevens.
- Er ontstaan meerdere aanbieders van diensten die op basis van persoonlijke gegevens voordelen kunnen bieden aan hun gebruikers.
- Deze diensten zijn interoperabel en onderling verwisselbaar.

Het uitgangspunt van MyData is dat mensen zelf de over hen verzamelde gegevens (denk aan winkel-, mobiliteits-, financiële of gezondheidsgegevens) kunnen gebruiken, beheren en machtigen in hun eigen voordeel. Hiermee heeft het initiatief veel raakvlakken met het thema identiteit, en is het tegelijkertijd een praktische implementatie van datagovernance.

MyData stelt dat haar aanpak de gewenste betrouwbaarheid van toekomstige Europese clouddiensten (zoals het Gaia-X project, zie hieronder) kan waarborgen, mits hun voorwaarden vanaf de eerste ontwerpfasen van deze diensten worden opgenomen. Een aantal van de benoemde initiatieven onder 'Identiteit' (IRMA, Solid) is conform de principes van MyData.

[42] https://mydata.org/
[43] Poikola, Antti et al. (2020), 'MyData: an introduction to human-centric use of personal data' *3rd, revised edition*, https://mydata.org/wp-content/uploads/sites/5/2020/08/mydata-white-paper-english-2020.pdf.

7.5. GAIA-X

GAIA-X,[44] in 2019 gelanceerd, streeft naar het bouwen van een gefedereerde data-infrastructuur[45] om Europese innovatie te stimuleren, gebaseerd op Europese waarden zoals soevereiniteit, veiligheid en privacy. Deze data-infrastructuur moet helpen om cloud- en edge-diensten[46] van (gevestigde en nieuwe) Europese aanbieders meer 'interoperabel' te maken; in feite is het een project dat streeft naar een Europese 'publieke digitale infrastructuur' zoals wij dat benoemen. Organisaties die deelnemen aan GAIA-X moeten gezamenlijke regels en normen naleven en leveren diensten op basis van technologieën die door alle deelnemers van GAIA-X worden onderschreven. Concreet betekent dit dat dienstenleveranciers mogelijk bepaalde garanties zullen (moeten) geven over privacy, lokalisering, het wel of niet toepassen van bepaalde technologieën voor specifieke doeleinden, et cetera. Het project heeft verschillende use-cases gebruikt om basisvoorwaarden op de funderen, waarvan twee energie-gerelateerd zijn: een data-infrastructuur voor nieuwe businessmodellen[47] en edge-datacenters[48].

Momenteel staat het project nog in een beginfase en beperkt het zich tot Franse en Duitse bedrijven. De meningen lijken nog verdeeld tussen enthousiasme en scepsis[49], waardoor het initiatief nog niet volledig van de grond komt. Doel is dat uiteindelijk veel meer Europese bedrijven deelnemen, om zo een systeem van cloud- en edge-diensten op te zetten waarbij alle leveranciers volgens dezelfde spelregels opereren en eindgebruikers grip houden op data.

8. Algoritmen

Gesteund door gegevens zouden consumenten c.q. prosumenten, laadpuntbeheerders en netbeheerders middelen voor automatische besluitvorming kunnen gebruiken om te onderhandelen over de vraag en het aanbod van energie, waarbij elke partij een systeem zou inzetten dat handelt op basis van zijn eigen belangen. Ook als het hierboven genoemde algoritme uit eenvoudige regels zou bestaan, maakt een grote hoeveelheid

---

[44] https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html

[45] Gefedereerde netwerken zijn gedecentraliseerde netwerken met een 'geneste' vertrouwensstructuur en architectuur. Zie bijvoorbeeld Institute for Network Cultures, https://networkcultures.org/unlikeus/resources/articles/what-is-a-federated-network/ (n.d.) en World Economic Forum, "Federated Data Systems: Balancing Innovation and Trust in the Use of Sensitive Data". White paper. Geneve: WEF (2019).

[46] Cloud- en edge-diensten zijn nodig om de enorme hoeveelheden data die wordt gegenereerd via nieuwe technologieën uit te wisselen en te verwerken. De *cloud* zijn gedistribueerde netwerken van serverclusters verspreid over datacenters binnen een regio of land. *Edge*-diensten gaan via serverparken in de buurt van deze locaties waar data wordt geproduceerd en verwerkt.

[47] https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Artikel/UseCases/infrastructure-data-for-new-business-models.html

[48] https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Artikel/UseCases/edge-data-centres.html

[49] Zie bijvoorbeeld de volgende opiniestukken: https://tweakers.net/nieuws/174720/bij-eu-tegenhanger-voor-amerikaanse-clouddiensten-heerst-onderlinge-argwaan.html en https://www.computable.nl/artikel/expertverslag/cloud-computing/6890493/4573232/iedereen-heeft-baat-bij-gaia-x.html.

aan algoritmen die met elkaar handelen de uitkomsten minder helder te doorgronden. Hoewel de algoritmen *an sich* niet extreem complex zijn, kan de combinatie aan algoritmen marktverstoringen veroorzaken zoals is waargenomen bij geautomatiseerde handelssystemen. Dit is vaak het gevolg van softwarefouten en een gebrek aan grondige tests voordat de algoritmen worden ingezet.

Als gevolg van deze marktverstoringen heeft de American Financial Industry Regulatory Authority verklaard[50] te willen beoordelen of bedrijven hun automatische handelssystemen adequaat testen en controleren. Deze autoriteit beoordeelt op de volgende gronden:

- Of bedrijven afzonderlijke, onafhankelijke en robuuste pre-implementatie tests van algoritmen en handelssystemen verrichten;
- of juristen, compliance en het 'operationele' personeel van het bedrijf het ontwerp en de ontwikkeling van de algoritmen en handelssystemen beoordelen op naleving van wettelijke vereisten;
- of een bedrijf actief algoritmen en handelssystemen controleert en beoordeelt nadat ze in productiesystemen zijn geplaatst en nadat ze zijn gewijzigd;
- of er procedures zijn er om catastrofale systeemstoringen te ondervangen of op te lossen.

Het is op dit moment niet duidelijk hoe tegenstrijdige belangen moeten worden gereguleerd, bijvoorbeeld wanneer een EV met een bepaald profiel moet worden opgeladen, maar een ander EV (of zelfs de huishoudens) in hetzelfde gebied een ander laadbeleid wil voeren. Tijdens een van onze expertsessies werd hierover het volgende gezegd: "*Je ziet daar ook langzaamaan conflict in ontstaan. Misschien wordt de [BMW] auto optimaler [opgeladen] door [een laadprofiel van fabrikant] BMW - maar wat als die nou in een gebouw staat waar het energiemanagement zelf wilt bepalen met welk profiel er wordt geladen? Conflict tussen verschillende belanghebbenden in slim laden. Ik ga zelf binnenkort starten met een project over botsende belangen. We zijn nog niet eens bij het certificeren van algoritmes aangeland*".

Alle bovengenoemde punten zijn dus relevant voor de inzet van automatische handelssystemen in de energiesector. Om te testen of een oplossing toereikend is, is het ook mogelijk deze oplossingen te simuleren. Initiatieven als D3A bieden een platform om bijvoorbeeld een energy exchange te kunnen modelleren en simuleren.[51] D3A, oftewel Decentralized Autonomous Area Agent, is een transactiegericht marktmodel opgezet door Grid Singularity (medeoprichter van Energy Web) om een gedecentraliseerd, gebalanceerd, toegankelijk en duurzaam energiesysteem te verwezenlijken via *peer-to-peer* energiehandel. Het is gebaseerd op de Energy Web blockchain en maakt gebruik van *smart contracts* om energiebronnen van elke maat en

[50] https://en.wikipedia.org/wiki/Automated_trading_system
[51] https://www.d3a.io/

type binnen het elektriciteitsnet uit te wisselen (van apparaten tot gebouwen en complete wijken).[52]

De situatie wordt ingewikkelder als we van eenvoudige algoritmen overgaan naar machine learning-toepassingen. Machine learning-toepassingen zijn 'black boxes': ze werken volgens criteria die niet (gemakkelijk) te kennen zijn en daarom moeilijk te reguleren. Dergelijke black boxen genereren twee problemen:

- een vertrouwensprobleem: de resultaten zijn moeilijk uit te leggen.
- een 'nalevingsprobleem': het is lastig te in te zien of de resultaten in overeenstemming zijn met gestelde eisen, ethisch verantwoord zijn of stroken met wet- en regelgeving, aangezien nergens in het proces deze afwegingen geformaliseerd (kunnen) worden.

De dringende behoefte aan de uitlegbaarheid van AI heeft geleid tot meer onderzoek en tools die pogen te laten zien wat de bepalende factoren zijn voor een specifiek resultaat. De bekendste tools die enige uitleg geven voor AI-resultaten zijn LIME[53] (Local Interpretable Model-agnostic Explanations) en SHAP[54] (SHapley Additive exPlanations).

De gemeente Amsterdam gebruikt SHAP om de resultaten van haar Vakantieverhuur woningfraude-algoritme[55] toe te lichten: "Om de door het algoritme gemaakte afwegingen inzichtelijk te maken voor mensen passen we de "SHAP"-methodiek toe (...). SHAP berekent voor iedere individuele zaak welke indicatoren hebben bijgedragen aan die voorspelling en of dit ervoor zorgde dat de voorspelling hoger of lager werd. Zo kan een medewerker altijd zien waar het algoritme de risico-inschatting op heeft gebaseerd en een afgewogen besluit nemen".

De gemeente Amsterdam heeft besloten om Amsterdammers het recht te geven te weten hoe algoritmen hun leven beïnvloeden. In lijn met deze gedachte heeft ze een algoritmeregister opgezet.[56] Dat is een overzicht van de algoritmen die de gemeente Amsterdam gebruikt bij haar gemeentelijke dienstverlening.

Het doel van het register is ook om feedback te ontvangen om deze algoritmen beter, eerlijker en verantwoordelijker te maken: "Dienstverlening of gegevensverwerking die met behulp van algoritmes is geautomatiseerd, moet dezelfde principes respecteren als alle andere dienstverlening door de gemeente. Ze moeten mensen gelijk behandelen, de vrijheid en zeggenschap niet inperken, open en controleerbaar zijn en in dienst staan van de Amsterdammer; niet andersom. Bovendien mogen algoritmes niet het laatste

[52] Zie voor nadere uitleg en toepassing https://gridsingularity.com/d3a/ en https://energyweb.org/wp-content/uploads/2019/05/EWF-D3A-ConceptBrief-FINAL201804-v1dot1.pdf.
[53] https://github.com/marcotcr/lime
[54] https://github.com/slundberg/shap
[55] https://algoritmeregister.amsterdam.nl/vakantieverhuur-woningfraude/
[56] https://algoritmeregister.amsterdam.nl/

woord hebben en niet uitsluitend werken op basis van toevallige verbanden (correlaties)"[57].

In 2020 is een groter samenwerkingsverband 'Publieke controle op algoritmen' opgezet bestaande uit de gemeenten Rotterdam (regie), Den Haag, Utrecht, Amsterdam; provincies: Noord-Brabant, Zuid-Holland, Limburg; Politie, Rijkswaterstaat, de Unie van Waterschappen en de VNG. Zij trachten gezamenlijk beleidsinstrumenten te ontwikkelen op het gebied van algoritmes. Hierbij wordt nadrukkelijk aandacht geschonken aan het ontwikkelen van de instrumenten samen met de doelgroep; dit kunnen burgers, bedrijven of ambtenaren zijn. De ambitie is om aan het eind van dit project vijf beleidsproducten gerealiseerd te hebben die de standaard zijn binnen Nederland.

De vraag over gelijke behandeling is een pregnant onderwerp binnen AI. Dit onderwerp heeft de laatste tijd veel gekregen, o.a. op conferenties[58] en door bedrijven die sinds kort producten aanbieden voor Fair AI.[59] De gemeente Amsterdam heeft in het bovengenoemde geval gebruik gemaakt van de 'AI Fairness 360 toolkit' van IBM.[60] Binnenkort verschijnt ook de handreiking 'Non-discriminatie by design' opgesteld in opdracht van met Ministerie van Binnenlandse Zaken.[61] Dit document "legt uit welke vragen en principes leidend zijn bij het ontwikkelen en implementeren van een AI-systeem met het oog op het discriminatieverbod, vanuit zowel juridisch, technisch, als organisatorisch perspectief". De handreiking is "bedoeld voor projectleiders die sturing geven aan systeembouwers, data-analisten en AI-experts" en behandelt de probleemdefinitie van nondiscriminatie in technische en juridische context, aspecten van datavoorbereiding en -verzameling, modellering, implementatie en evaluatie.

[57] Zie https://algoritmeregister.amsterdam.nl/meer-informatie/ en https://codefor.nl/ai-met-impact/
[58] Bijvoorbeeld een conferentie van de Association for Computing Machinery over Fairness, Accountability and Transparency, maart 2021: https://facctconference.org/
[59] https://www.claimsjournal.com/news/international/2018/06/14/285217.htm
[60] https://aif360.mybluemix.net
[61] Bart van der Sloot et al. (2021), te verschijnen.