Brain-be 2.0
Belgian Research Action through Interdisciplinary Networks
POLICY BRIEF

Policy Brief n° 2

DIGI4FED- Digitale (r)evolutie in de Belgische federale overheid: een open governance-ecosysteem voor big data, kunstmatige intelligentie en blockchain (DIGI4FED)

DIGI4FED wil begrijpen hoe (big) data door het Belgische federale bestuurssysteem ingezet kan worden om publieke dienstverlening te verbeteren met de hulp van nieuwe technologieën zoals artificiële intelligentie en blockchain. Door zich te concentreren op de technische, morele, juridische en organisatorische voorwaarden binnen de interne en externe federale besluitvormingsprocessen, wil DIGI4FED een governancemodel ontwikkelen dat ten dienste staat van de administratieve en publieke dienstverleningsprocessen van de Belgische federale overheid en ten volle gebruik maakt van het potentieel van big data en de toepassing ervan via artificiële intelligentie en blockchaintechnologie. DIGI4FED richt zich op de ontwikkeling van een proof of concept (PoC) van een governancemodel – het design artefact – in twee specifieke federale beleidsdomeinen: inbreuken inzake sociale zekerheid en belastingfraude.

Projectpartners: KU Leuven, UAntwerpen, ULiège, UNamur
Timing: 2020 – 2022

Context en onderzoeksvra(a)g(en)

Drie factoren bepalen de context die DIGI4FED beïnvloedt. De eerste factor is de groeiende aandacht voor de potentiële impact van big data (BD) en artificiële intelligentie (AI) op traditionele overheidsinformatieprocessen. De tweede factor is de groeiende verwachting van de maatschappij ten aanzien van overheidsadministraties om nieuwe technologische middelen in te zetten ter bevordering van efficiënt en effectief bestuur en publieke dienstverlening, waarbij belangrijke democratische en morele kernwaarden niet uit het oog worden verloren. De derde factor betreft de Belgische federale administratie zelf. Hoewel er reeds verschillende stappen werden gezet om de digitale transformatie van de Belgische federale staat te bewerkstelligen, blijven verschillende uitdagingen aanwezig.

DIGI4FED heeft de voorwaarden onderzocht om nieuwe digitale technologieën zoals big data, AI en blockchain te introduceren om fraudeopsporingsprocessen in de fiscale en sociale zekerheidsdomeinen te verbeteren. Het uiteindelijke doel van DIGI4FED is het ontwerpen van een governancemodel voor een data-uitwisselingsplatform dat open government data (OGD) en nieuwe digitale technologieën inzet en voldoet aan de specifieke vereisten van het ecosysteem van de Belgische federale overheid. Tijdens de looptijd van het project heeft het DIGI4FED-team op verschillende manieren gegevens verzameld (bijvoorbeeld door middel van experimenten, interviews en een living lab) om de uitdagingen te identificeren om aan deze doelstelling te voldoen. De details van de gegevensverzameling en analyseprocessen zijn gerapporteerd in verschillende documenten (zie D.1.3, D.1.4, D.2.2, D.2.3, D.3.2, D.3.3) die als onderdeel van het project zijn geproduceerd. Om een beter inzicht in deze processen te krijgen, nodigen wij de lezers uit deze documenten door te nemen.

Voornaamste bevindingen

Het onderzoek heeft verschillende soorten uitdagingen aan het licht gebracht voor het gebruik van nieuwe digitale technologieën door de Belgische federale overheid. Hieronder belichten we de belangrijkste conclusies over hoe de uitdagingen kunnen worden aangepakt in zeven rubrieken: uitdagingen op het vlak van vertrouwen, operationele uitdagingen, administratieve uitdagingen, technische uitdagingen, uitdagingen op het vlak van gebruikersacceptatie, juridische uitdagingen en beleidsuitdagingen.

1. *Vertrouwensproblemen:*

   - Transparantie alleen kan soms het vertrouwen van de burger in AI-projecten en gegevensuitwisselingplatforms schaden, met name als de vrijgegeven informatie als risicovol wordt beschouwd.
   - Een combinatie van transparantie en controle van de burgers over de gegevens houdt het vertrouwen in AI-projecten en gegevensuitwisselingplatform in stand.
   - Burgers zijn bereid gegevens te delen met de federale overheid, maar minder met commerciële bedrijven of regionale en lokale overheden.
   - De perceptie van mogelijke discriminatie is sterk gerelateerd aan vertrouwen in AI-projecten.

2. *Operationele uitdagingen:*

   - De Belgische overheidsdiensten zijn zich onvoldoende bewust over de data die de verschillende diensten tot hun beschikking hebben. Dit belemmert een doeltreffend gebruik van data bij fraudebestrijding en leidt tot verspilling van inspanningen en middelen bij concurrerende projecten.
   - Er is een zekere mate van onwil om gegevens te delen uit vrees voor een bijkomende administratieve last en een gebrek aan een strategische en samenhangende langetermijnvisie om gegevensuitwisseling aan te moedigen.
   - Gegevensuitwisseling bij fraudebestrijding wordt belemmerd door een gebrek aan gemeenschappelijke procedurele en technische standaarden en een gemeenschappelijk platform dat de gegevensuitwisseling tussen federale overheidsdiensten en externe organisaties zou vergemakkelijken.

3. *Administratieve uitdagingen:*

   - Risico's in verband met de toegang tot gevoelige gegevens en het onvermogen om aanbieders van gegevensdiensten te controleren, maken het noodzakelijk dat overheidsorganisaties het voortouw nemen bij de governance van het gegevensuitwisselingplatform.
   - Overheidsorganisaties ondervinden echter nadelen ten opzichte van particuliere dienstverleners wat betreft het mobiliseren van financiële middelen en personeel om de governance van een gegevensuitwisselingplatform te ondersteunen.
   - Oplossingen van Europese actoren en opensourceoplossingen zouden de overheid minder afhankelijk kunnen maken van de particuliere sector.

4. *Technische uitdagingen:*

   - Meer geavanceerde analytische oplossingen in de strijd tegen fraude doen de bezorgdheid over de verklaarbaarheid en eerlijkheid van beslissingen herleven. XAI, gedecentraliseerde technologieën en controle over de trainingdatasets kunnen oplossingen bieden, maar de doeltreffendheid hiervan moet nog bewezen worden.

- Fraudeanalyse met nieuwe digitale technologieën moet zorgen voor een evenwicht tussen verklaarbaarheid en doeltreffendheid bij de opsporing van fraude, maar er zal een aanpassings- en leerperiode nodig zijn voordat meer geavanceerde technologische oplossingen toegepast kunnen worden.

- Investeringsbeslissingen in gecentraliseerde of gedecentraliseerde technologieën ter ondersteuning van fraudeanalyse hangen nauw samen met uitdagingen op vlak van publieke waarde, administratie en beleid.

5. *Uitdagingen omtrent gebruikersacceptatie:*

- Keuzes op het gebied van governance design vereisen een beoordeling over de gevolgen voor de publieke waarde.

- Onder de respondenten heersen tegenstellingen over het doel van een fraudedetectiesysteem, zoals doeltreffendheid tegen transparantie, geautomatiseerde processen tegen door mensen gestuurde processen, en door burgers gestuurde processen tegen het only-for-once principle**.**

- Bruikbaarheid en begrijpelijkheid zijn evenzeer uitdagingen bij ontwerpprocessen. De digitale kloof, de technologische zelfredzaamheid van burgers en regionale verschillen in bereidheid om gegevens te delen, zijn belangrijke maatschappelijke factoren die bepalend kunnen zijn voor het succes van technologische oplossingen.

6. *Juridische uitdagingen:*

- Het huidige wetgevingskader inzake gegevensverwerking beperkt de aanpasbaarheid van geavanceerde data-analyses in de strijd tegen fraude. Er zijn uiteenlopende interpretaties door functionarissen voor gegevensbescherming en moeilijkheden bij de coördinatie en uitwisseling tussen overheidsdiensten.

- Het wetgevingskader moet beter worden afgestemd op nieuwe digitale technologieën. Hoe deze afstemming kan worden bereikt, is echter voor discussie vatbaar.

- Regulatory sandboxes en recente EU-initiatieven en -wetgeving inzake nieuwe digitale technologieën kunnen een oplossing bieden, maar er zijn duidelijke richtlijnen en regels nodig om een wijdverspreide toepassing te bekomen.

7. *Beleidsuitdagingen:*

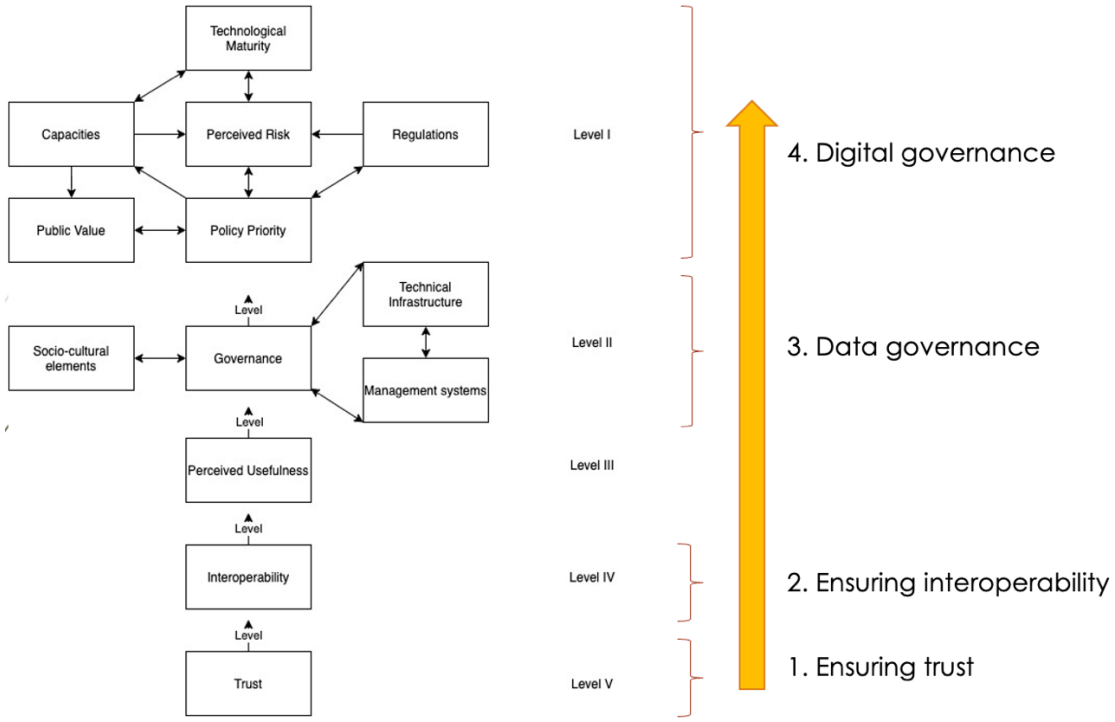
- Er zijn tegenstrijdige standpunten over de wenselijkheid van gedecentraliseerde en gecentraliseerde systeemoplossingen voor de governance van het gegevensuitwisselingsplatform.

- Het governancemodel moet de wanverhoudingen tussen de verschillende overheidsniveaus aanpakken en een samenhangende visie nastreven om de coördinatie tussen Europese, federale, regionale en lokale initiatieven op het gebied van gegevensuitwisseling te vergemakkelijken.

- De rol van particuliere actoren bij data governance moet duidelijk worden omschreven.

Conclusie en aanbevelingen

De aanbevelingen voor het opzetten van een governancemodel volgen de methodologische stappen die zijn vastgesteld in het interpretatieve structurele model (ISM) dat in D.3.3 wordt beschreven. Dit model verklaart de onderlinge verbanden tussen de drijvende krachten achter de implementering van nieuwe digitale technologieën bij de bestrijding van sociale en fiscale fraude. De onderzoeksbevindingen zijn samengebracht onder vier categorieën: (1) het vertrouwen vergroten, (2) het garanderen van interoperabiliteit, (3) data governance en (4) digital governance. Hieronder presenteren wij de aanbevelingen om een governancemodel op te zetten dat gebruik maakt van geavanceerde analytics voor de opsporing van fraude.



Vraagstukken omtrent governance	**Beleidsaanbevelingen**
Vertrouwen	**Beleidsaanbeveling 1:** Streef naar een transparant gegevensuitwisselingsysteem dat gebruik maakt van SSI-oplossingen (self-sovereign identity) en gebruikers in staat stelt om hun gegevenstransacties te volgen.
	Beleidsaanbeveling 2: Combineer technologische oplossingen met pedagogische/communicatieve inspanningen ten behoeve van de burgers. Maar, let op: communicatie op zich is geen tovermiddel.
Interoperabiliteit	**Beleidsaanbeveling 3:** Ontwerp een enkele toegangspoort tot verschillende departementen, administraties, bedrijven en betrokken partijen om na te kunnen gaan welke datasets worden bijgehouden door de verschillende administraties.
	Beleidsaanbeveling 4: Ontwerp standaarddocumenten en regels om de gegevensuitwisseling via de centrale toegangspoort te vergemakkelijken.
	Beleidsaanbeveling 5: Integreer SSI-oplossingen in het systeem voor gegevensuitwisseling en volg daarbij de EBSI- en ESSIF-oplossingen.
Data Governance	**Beleidsaanbeveling 6:** Bouw geen nieuw gegevensuitwisselingplatform om fraude te bestrijden, maar pak de uitdagingen aan op het gebied van systeemintegratie tussen de betrokken publieke en particuliere organisaties en bestaande systemen voor gegevensuitwisseling.
	Beleidsaanbeveling 7: Richt geen nieuwe entiteit op om de gegevensuitwisseling voor fraudebestrijding te coördineren. BOSA lijkt de ideale kandidaat om andere actoren voor het gegevensuitwisselingsplatform te coördineren.
	Beleidsaanbeveling 8: Zet een hub op omtrent data governance onder leiding van BOSA, maar waaraan wordt deelgenomen door vertegenwoordigers van regionale en lokale overheden, het bedrijfsleven en maatschappelijke organisaties. Het doel moet zijn om de regels en richtlijnen vast te stellen voor het verwerven, delen en gebruiken van platformgegevens. Een modulaire aanpak van de regels voor het delen van gegevens en het gebruik ervan is aan te bevelen.
	Beleidsaanbeveling 9: Beheer gegevensverwerking in de strijd tegen fraude op een gedecentraliseerde manier, waarbij eenheden van datawetenschappers worden ingezet in de sociale en fiscale domeinen, maar waarbij ze ondersteund worden door de platformbeheerder omtrent de juridische en technische dimensies van data governance.
Digitale Vaardigheden & Expertise	**Beleidsaanbeveling 10:** Werk samen met organisaties uit de particuliere sector bij de ontwikkeling van technologische oplossingen op het gebied van geavanceerde data-analyses, maar kies voor opensourcetechnologie en bouw interne competenties op inzake

	gegevensanalyse en geavanceerde technologieën om succesvol te kunnen samenwerken met technologieverkopers.
	Beleidsaanbeveling 11: Investeer in opleidingsprogramma's en -activiteiten die geavanceerde digitale vaardigheden in de overheidssector aanleren. Er is een nood aan interdisciplinaire opleidingen die computervaardigheden combineren met de relevante juridische en sociaalwetenschappelijke dimensies.
	Beleidsaanbeveling 12: Bied eerstelijnsambtenaren opleidingen en ondersteuning aan om voldoende kennis over databeheer en geavanceerde data-analyses te verwerven. Opleidingen en beleidsondersteuning kunnen worden verstrekt door het centrale management van het platform.
Value-based Design	**Beleidsaanbeveling 13:** Combineer citizen-controlled data sharing (d.w.z. SSI) met transparantiemaatregelen bij het gebruik van data om het vertrouwen in en betrokkenheid van burgers bij digital governance te behouden.
	Beleidsaanbeveling 14: Wanneer het vermoeden bestaat dat een bepaald instrument voor data-analyse door sommige groepen als onwettig of discriminerend kan worden ervaren, moet worden onderzocht hoe een dergelijk systeem door leden van deze groepen geïnterpreteerd kan worden.
	Beleidsaanbeveling 15: Hanteer juridische, technische en ethische vereisten om ethische aanbestedingsprocedures te ontwerpen voor dienstverleners van geavanceerde data-analyses uit de particuliere sector.
	Beleidsaanbeveling 16: Zorg voor duidelijke communicatie over de inhoud van digitale veranderingen met de eindgebruikers binnen de administratie die het meest te maken krijgt met geavanceerde technieken voor fraudeanalyse. Vermijd dat de integratie van AI- of datagestuurde ondersteuningsinstrumenten gepaard gaat met een buitensporige inkrimping van een specifieke categorie van eerstelijnsambtenaren.
Beleidsprioriteiten	**Beleidsaanbeveling 17:** Zorg ervoor dat nationale en regionale projecten omtrent SSI en digitale portemonnees compatibel zijn met EU-oplossingen.
	Beleidsaanbeveling 18: Neem deel aan de EBSI use cases betreffende belastingen en sociale zekerheid om de toepassing van deze oplossingen in het Belgische ecosysteem te ondersteunen.
Risicomanagement	**Beleidsaanbeveling 19:** Voer in-vitro-experimenten uit om de haalbaarheid en begrijpelijkheid van XAI-oplossingen voor voorspellende analyses te testen.
	Beleidsaanbeveling 20: Voer gecontroleerde experimenten uit om verschillende technologische configuraties in gegevensbeheer te beoordelen bij het vinden van een evenwicht tussen de prestaties van voorspellende analyses en de begrijpelijkheid en transparantie van algoritmische besluiten.
Naleving Van De Wettelijke Voorschriften	**Beleidsaanbeveling 21:** Ontwikkel gestandaardiseerde richtlijnen voor de functionarissen voor gegevensbescherming en de gegevensbeschermingsautoriteiten voor het beheer van een open databeleid voor geavanceerde analyses. IT-oplossingen die op EU-niveau zijn ontwikkeld, hebben een duidelijk voordeel bij het vergemakkelijken van de taken van functionarissen voor gegevensbescherming.
	Beleidsaanbeveling 22: Verbeter de betrouwbaarheid van IT-oplossingen door middel van regulatory sandboxes en benchmarking.
	Beleidsaanbeveling 23: Zet een proefproject op met regulatory sandboxes om verschillende regelgevingssystemen voor het gebruik van digitale technologieën bij fraudebestrijding te evalueren.

Gegevens

Contact
Tan, Evrim
KU Leuven Public Governance Institute
Evrim.tan@kuleuven.be

Crompvoets, Joep
KU Leuven Public Governance Institute
Joep.crompvoets@kuleuven.be

BRAIN-be 2.0 : *Sinds 2012 voert de POD Wetenschapsbeleid (BELSPO) een recurrent onderzoeksprogramma uit dat erop gericht is de wetenschappelijke basis van het federale overheidsbeleid en de strategie en het potentieel van de federale wetenschappelijke instellingen (FWI) te versterken. Meer: www.belspo.be/brain-be*