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

Policy Brief n° 2

DIGI4FED- (R)évolution numérique dans le gouvernement fédéral belge : Un écosystème de gouvernance ouverte pour le big data, l'intelligence artificielle et la blockchain (DIGI4FED)

DIGI4FED vise à comprendre comment les (big) data peuvent être utilisées dans le système de l'administration fédérale belge pour permettre une meilleure prestation de services publics grâce aux nouvelles technologies, telles que l'intelligence artificielle et la blockchain. En se concentrant sur les conditions techniques, morales, juridiques et organisationnelles au sein des processus décisionnels fédéraux internes et externes, DIGI4FED vise à développer un modèle de gouvernance qui sert les processus administratifs et de service public du gouvernement fédéral belge et utilise pleinement le potentiel offert par le big data et son application via l'intelligence artificielle et la technologie blockchain. DIGI4FED se concentre sur le développement d'une *proof of concept* (PoC) d'un modèle de gouvernance – design artefact – dans deux domaines politiques fédéraux spécifiques : les infractions à la sécurité sociale et les fraudes fiscales.

Partenaires du projet : KU Leuven, UAntwerpen, ULiège, UNamur

Calendrier du projet : 2020-2022

Contexte et question(s) de la recherche

Trois facteurs définissent le contexte dans lequel DIGI4FED est influencé. Le premier facteur est l'attention croissante portée à l'impact du big data (BG) et de l'intelligence artificielle (IA) sur les processus traditionnels d'information du gouvernement. Le second facteur est l'attente croissante de la société vis-à-vis des administrations publiques pour qu'elles adoptent de nouveaux moyens technologiques afin d'avancer vers une gouvernance et une prestation de services publics efficaces et efficientes, tout en veillant à ce que les valeurs démocratiques et morales fondamentales ne soient pas perdues de vue. Le troisième facteur concerne l'administration fédérale belge elle-même. Bien que plusieurs mesures aient été prises en faveur de la transformation numérique de l'Etat fédéral belge par le passé, des défis subsistent.

Le projet DIGI4FED a recherché les conditions dans lesquelles introduire, afin d'améliorer les processus de détection des fraudes dans le domaine de la fiscalité et de la sécurité sociale, de nouvelles technologies numériques, telles que le BG, l'IA et la blockchain. L'objectif ultime du projet DIGI4FED est d'esquisser un modèle de gouvernance d'une plateforme d'échange de données qui tire parti des données gouvernementales ouvertes et des nouvelles technologies numériques, tout en respectant les exigences spécifiques de l'écosystème du gouvernement fédéral belge. Tout au long du projet, l'équipe

DIGI4FED a recueilli des données par divers moyens (par exemple, des expériences, des entretiens, un *living lab*) afin d'identifier les défis à surmonter pour atteindre cet objectif. Les détails de la collecte de données et les processus d'analyse ont été rapportés dans divers livrables produits dans le cadre du projets (voir D.1.3, D.1.4, D.2.2, D.3.2, D.3.3). Pour avoir un meilleur aperçu de ces processus, nous invitons les lecteurs à consulter ces livrables.

Principales observations

La recherche a révélé plusieurs types de défis à l'introduction de nouvelles technologies numériques dans le gouvernement fédéral belge. Nous soulignons ci-dessous les principales conclusions sur la faon de relever les défis dans sept catégories : les défis ayant trait à la confiance, les défis organisationnels, les défis administratifs, les défis techniques, les défis d'acceptation par les utilisateurs, les défis juridiques et les défis politiques.

1. Les défis ayant trait à la confiance :

- La transparence seule peut parfois réduire la confiance des citoyens dans les projets d'IA et les plateformes d'échange de données, en particulier si les informations publiées peuvent être perçues comme menaçantes.
- La combinaison de la transparence et du contrôle des données par les citoyens permet de maintenir la confiance dans les projets d'IA et les plateformes d'échange de données.
- Les citoyens sont prêts à partager leurs données avec le gouvernement fédéral, mais moins avec les entreprises commerciales ou les gouvernements régionaux et locaux.
- La discrimination perçue est significativement liée à la confiance dans les projets d'IA.

2. Défis opérationnels :

- Les administrations belges ne savent pas qui détient quel type de données dans leurs bases de données. Ceci entrave l'utilisation efficace des données dans la lutte contre la fraude et entraine un gaspillage d'efforts et de ressources dans des projets concurrents.
- Il existe un certain manque de volonté de partager les données par crainte de la charge administrative et l'absence d'une vision stratégique et unificatrice à long terme pour encourager l'échange de données.
- Le manque de normes procédurales entre les SPF et les organisations extérieurs entraves les échanges de données pour lutter contre la fraude.

3. Défis administratifs:

- Les risques concernant l'accès aux données sensibles et l'incapacité à contrôler les fournisseurs de services de données obligent les organisations du secteur public à diriger les efforts de gouvernance de la plateforme d'échange de données.
- Cependant, les organisations du secteur public sont désavantagées par rapport aux prestataires de services privés en termes de mobilisation des ressources financières et humaines pour soutenir la gouvernance des plateformes d'échange de données.
- Les solutions développées par les acteurs européens et les solutions *open source* pourraient réduire la dépendance du secteur public vis-à-vis des organisations du secteur privée.

4. Défis techniques:

- Des solutions analytiques plus avancées dans la lutte contre la fraude ravivent les inquiétudes concernant l'explicabilité et l'équité des décisions. L'IAO, les technologies décentralisées et le contrôle des ensembles de données de formation peuvent apporter des solutions, mais l'efficacité de ces solutions reste à prouver.

- L'analyse des fraudes à l'aide des nouvelles technologies numériques doit assurer un équilibre entre l'explicabilité et l'efficacité de la détection des fraudes, mais une période d'adaptation et d'apprentissage serait nécessaire avant d'adopter des solutions technologiques plus avancées.
- Les décisions d'investir dans des technologies centralisées ou décentralisées pour soutenir l'analyse de la fraude sont étroitement liées à l'intérêt public et aux défis administratifs et politiques.

5. Défis d'acceptation par les utilisateurs

- Les choix de conception de la gouvernance nécessitent l'évaluation des implications de l'intérêt public.
- Il existe des contradictions parmi les répondants quant à l'objectif d'un système de détection des fraudes, comme l'efficacité par rapport à la transparence, les processus automatisés par rapport aux processus contrôlés par l'homme, et les processus contrôlés par les citoyens par rapport au principe du "une fois pour toutes".
- La convivialité et la compréhension sont d'autres défis à relever dans les processus de conception. La fracture numérique, l'auto-efficacité technologique des citoyens et les différences régionales dans la volonté de partager les données sont des facteurs sociétaux importants qui peuvent déterminer le succès des solutions technologiques.

6. Défis juridiques :

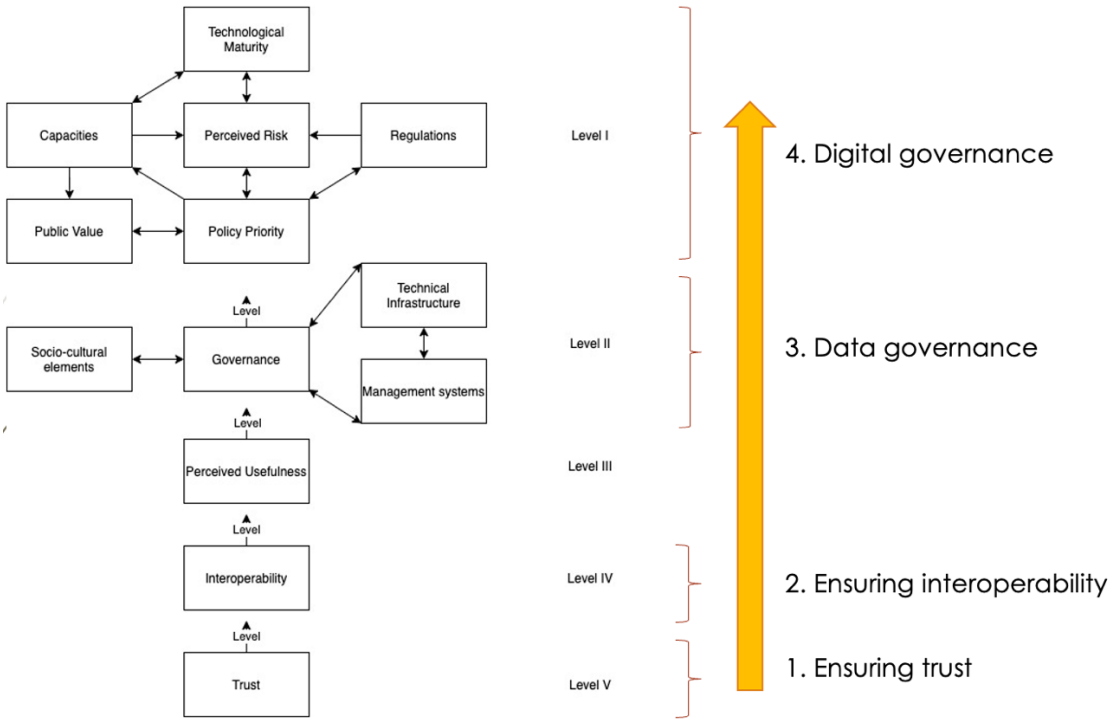
- Le cadre législatif actuel sur les règles de traitement des données limite l'adaptabilité des solutions avancées d'analyse des données dans la lutte contre la fraude. Il existe des interprétations divergentes par les DPOs et des difficultés de coordination et d'échange entre les administrations.
- Le cadre législatif doit être mieux adapté aux nouvelles technologies numériques. Cependant, la manière de réaliser cette adaptation est discutable.
- Les bacs à sable réglementaires et les nouvelles initiatives et législations européennes sur les nouvelles technologies numériques peuvent être une solution, mais des lignes directrices et des règles claires sont nécessaires pour une adoption généralisée.

7. Défis politiques :

- Il existe des opinions divergentes sur l'opportunité de solutions de systèmes décentralisés et centralisés pour la gouvernance de la plateforme d'échange de données.
- La structure de gouvernance des données devrait remédier aux désaccords entre les différents niveaux de gouvernement et poursuivre une vision unificatrice pour faciliter la coordination entre les initiatives européennes, fédérales, régionales et locales en matière d'échanges de données.
- Le rôle des acteurs privés dans la gouvernance des données doit être clairement défini.

Conclusion et recommandations

Les recommandations pour la construction d'un modèle de gouvernance suivront les étapes méthodologiques identifiées par le modèle structurel interprétatif (MSI) présenté dans le délivrable D.3.3. Le MIS explique les interrelations entre les moteurs de la mise en œuvre des nouvelles technologies numériques dans la lutte contre la fraude dans le domaine de la fiscalité et de la sécurité sociale. En conséquence, les résultats de la recherche sont compilés en quatre domaines de recommandation : (1) assurer la confiance, (2) assurer l'interopérabilité, (3) la gouvernance des données, et (4) la gouvernance numérique. Nous présentons ci-dessous les recommandations visant à établir un modèle de gouvernance qui tire parti de l'analytique avancée dans la détection des fraudes.



Problème de gouvernance	**Recommendation politique**
Confiance	**Recommandation politique 1 :** poursuivre la mise en place d'un système d'échange de données transparent qui s'appuie sur des solutions d'identité auto-souveraine (SSI) et permet aux utilisateurs de suivre les transactions de données.
	Recommandation politique 2 : combiner les solutions technologiques avec des efforts pédagogiques / de communication envers les citoyens. Mais attention, la communication elle-même n'est pas une solution miracle.
Interoperabilité	**Recommandation politique 3 :** établir une passerelle unique vers les différents départements, administrations, entreprises et organisations de parties prenantes afin d'explorer les types d'ensembles de données détenus par les différentes administrations.
	Recommandation politique 4 : créer des documents et des règles normalisés pour faciliter l'échange de données par le biais de la passerelle unique.
	Recommandation 5 : intégrer les solutions SSI dans le système d'échange de données en conformité avec les solutions EBSI et ESSIF.
Gouvernance des données	**Recommandation politique 6 :** ne pas construire une nouvelle plateforme d'échange de données pour lutter contre la fraude, mais relever les défis de l'intégration des systèmes entre les organisations publiques et privées concernées et les systèmes de partage de données existants.
	Recommandation politique 7 : Ne pas créer une nouvelle entité pour coordonner l'échange de données pour la lutte contre la fraude. BOSA

	apparaît comme le candidat idéal pour coordonner d'autres acteurs pour la plateforme d'échange de données.
	Recommandation politique 8 : établir un centre de gouvernance des données dirigé par le BOSA, mais auquel participent des représentants des gouvernements régionaux et locaux, ainsi que des entreprises et des organisations de la société civile. Le BOSA doit définir les règles et les directives en matière d'extraction, de partage et d'utilisation des données de la plateforme. Une approche modulaire sur le partage des données et les règles d'utilisation est conseillée.
	Recommandation politique 9 : Gérer le traitement des données dans la lutte contre la fraude de manière décentralisée, où les data scientists sont employés dans les unités respectives des domaines de la sécurité sociale et de la fiscalité, mais soutenus par la gestion de la plateforme en termes de dimensions juridiques et techniques dans la gouvernance des données.
Compétence et expertise numériques	**Recommandation politique 10 :** collaborer avec des organisations du secteur privé pour développer des solutions technologiques dans le domaine de l'analyse avancée, mais privilégier les technologies libres et développer des compétences internes dans le domaine de l'analyse des données et des technologies avancées afin de s'engager avec succès auprès des fournisseurs de technologies.
	Recommandation politique 11 : Investir dans des programmes et activités de formation qui fournissent des compétences numériques avancées dans le secteur public. Des formations interdisciplinaires sont nécessaires pour combiner les compétences informatiques avec les dimensions juridiques et sociales.
	Recommandation politique 12 : fournir aux fonctionnaires de première ligne une formation et un soutien pour atteindre un degré suffisant de maîtrise des données et de connaissance des analyses avancées. Cette formation et ce soutien politique peuvent être assurés par la direction centrale de la plateforme.
Value-based design	**Recommandation politique 13 :** combiner le partage des données contrôlé par les citoyens (c'est-à-dire les SSI) avec des mesures de transparence dans l'utilisation des données afin de maintenir la confiance et l'engagement des citoyens dans la gouvernance numérique.
	Recommandation politique 14 : lorsque l'on soupçonne qu'un outil d'analyse de données particulier peut être perçu comme illégitime ou discriminatoire par certains sous-groupes de la société, mener des recherches sur la manière dont un tel système serait interprété par les membres de ces sous-groupes.
	Recommandation politique 15 : utiliser les exigences juridiques, techniques et éthiques pour concevoir des procédures d'achat éthiques pour les fournisseurs de services du secteur privé dans le domaine de l'analyse avancée.
	Recommandation politique 16 : S'engager dans une communication claire sur le contenu du changement numérique avec les utilisateurs finaux

	au sein de l'administration qui sont les plus touchés par les techniques avancées d'analyse de la fraude. Éviter de combiner l'intégration de l'IA ou d'outils de soutien axés sur les données avec des réductions excessives dans une catégorie spécifique de fonctionnaires de première ligne.
Priorités politiques	**Recommandation politique 17 :** S'assurer que les projets nationaux et régionaux sur les SSI et les portefeuilles numériques sont compatibles avec les solutions de l'UE.
	Recommandation politique 18 : Participer aux *use cases* de l'EBSI sur la fiscalité et la sécurité sociale afin de soutenir l'adoption de ces solutions dans l'écosystème belge.
Gestion du risque	**Recommandation politique 19 :** mener des expériences in vitro pour tester la faisabilité et la compréhension des solutions XAI pour l'analyse prédictive.
	Recommandation politique 20 : mener des expériences contrôlées pour évaluer différentes configurations technologiques dans la gouvernance des données en trouvant un équilibre entre la performance de l'analyse prédictive et la compréhension et la transparence des décisions algorithmiques.
Conformité à la loi	**Recommandation politique 21 :** élaborer des lignes directrices normalisées pour les DPOs et les APD dans la gestion des politiques d'ouverture des données pour l'analyse avancée. Les solutions informatiques développées au niveau de l'UE présentent un avantage certain pour faciliter la tâche des DPOs.
	Recommandation politique 22 : améliorer la fiabilité des solutions informatiques grâce à des bacs à sable réglementaires et à l'analyse comparative.
	Recommandation politique 23 : expérimenter avec des bacs à sable réglementaires pour tester les différents systèmes réglementaires pour l'utilisation des technologies numériques dans la lutte contre la fraude.

Information

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

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