Study on Potential Policy Measures to Promote the Uptake and Use of AI in Belgium in Specific Economic Domains

Summary – Samenvatting – Résumé – Zusammenfassung

economie

FPS Economy, S.M.E.s, Self-employed and Energy

.be

FPS Economy, S.M.E.s, Self-employed and Energy

Rue du Progrès 50
1210 Brussels
N° d'entreprise : 0314.595.348

0800 120 33 (free call)

facebook.com/SPFEco

@SPFEconomie

linkedin.com/company/fod-economie

instagram.com/spfeco

youtube.com/user/SPFEconomie

https://economie.fgov.be

Responsible publisher:
Séverine Waterbley
Chair of the Board of Directors
Rue du Progrès 50
1210 Brussels

Internet version

SUMMARY (EN)

Artificial intelligence (AI) and robots are becoming increasingly important in our daily lives. AI systems are already used for a variety of purposes and deployed in many sectors such as traffic, health, (personalised) marketing, manufacturing, fraud detection, content recommendation, etc. The rise of AI is no surprise considering the many benefits. AI systems process information faster than humans. Consequently, they may perform many tasks 'better' than their human counterparts, thereby improving productivity and competitiveness. AI systems can also have advantages for the specific sector in which they are used, including for the purposes of safety. They can for example be used to detect manufacturing defects or to reduce traffic accidents and enable increased mobility for those who are not capable of operating a vehicle. Nonetheless, the use of AI systems also comes with many ethical and legal challenges. The commercialisation of AI will pose several challenges from a legal and regulatory point of view as it affects nearly all legal domains.

In this study, we examined the impact of AI systems on the legal domains for which the Federal Public Service (FPS) Economy, S.M.E.s, Self-Employed and Energy is competent. In a first report, we assessed the impact of AI on several legal domains that are relevant to the FPS (gap analysis). In the second report, we conducted a legal comparative analysis of the policy initiatives regarding AI in four jurisdictions: France, the Netherlands, the United Kingdom and Germany. We based our analysis on a standardised questionnaire. In a final report, we formulated recommendations that can be relied upon by the FPS for the development of their (future) AI policy. This was based on a standardised questionnaire as well. The summary of our findings are listed below.

- **Intellectual Property and Trade Secrets (WP 2)**

One of the topics investigated in this study is the interaction between intellectual property (IP) law and AI. The requirements for IP protection (including copyright and patent law) often contain references to human actors which render it difficult to apply the relevant concepts to AI-supported creations. A crucial step in that regard is to distinguish AI-assisted creations (protectable) from AI-generated creations (unprotectable), whereby the latter refer to entirely autonomous creations by AI-systems without significant relevant human intervention. Other issues also arise with regard to the practical impact that AI may have on our current IP system (e.g. sufficiency of disclosure) and the risk of international regulatory competition with regard to the protection of AI-generated creations. Taking into account these various issues, a list of proposals has been formulated that should strengthen the existing IP framework while also supporting the promotion of the development, uptake and the use of AI-technology in Belgium and the European Union (EU).

- **Consumer and Market (WP 3)**

  - **Competition Law (WP 3.1.)**

The currently applicable legal framework does not address new digital infringement of competition law such as collusion by algorithms and price discrimination. When anticompetitive behaviour is caused through the functioning of algorithms without any human intervention, it should constitute an infringement of competition law. Once a violation is committed by using algorithms, it must also be ensured that it is possible for authorities to hold an actor liable. This problem can only be solved by qualifying algorithmic collusion and price discrimination by algorithms as anti-competitive behaviour at the EU level.

  - **Consumer Protection (WP 3.2.)**

The focus of this part was to analyse the adequacy of consumer protection rules when AI systems are being deployed. To do so, the study considered existing and future legal rules on warranty,

information obligations, liability for defective products, unfair commercial practices, requirements for consent and the use of automated means for prospection. As the analysis identified several gaps in this legal framework for the fields included in this study, several policy recommendations were formulated that could be implemented at the Belgian level to make consumer protection fit for AI.

- **Telecommunication and Information Society (WP4)**

  - **AI Safety and Security (WP 4.1.)**

The focus of this part was to map the different regulatory regimes that serve to mitigate harm caused by and to AI systems. An important finding is that the regulatory framework is a patchwork of different types of legislation and regimes (e.g. contract law, tort law, product safety laws, data protection laws, cybersecurity laws, both general and sectoral). These regimes all have different scopes and cover specific types of harm. A common thread is that they tend to combine open standards of care with a reference to standardisation as a way to operationalise open behavioural norms into (presumed) best practices. Many of these rules, such as the product safety framework, the GDPR and cybersecurity laws are regulated at EU level. This patchwork, as well as the absence and slow development of concrete standards concerning AI safety, are a cause of concern, as they allow risk coverage gaps to occur and redouble work at the same time. Convergence of these regimes as well as clear standardisation is thus required. To be clear, the EU legislator and international standardisation organisations are already working on this. Therefore, the focus of Belgium should be on supporting these rules and on awareness campaigns to ensure their use by the wider public. Several proposals to address the (regulatory) gaps were formulated in the third report.

  - **Data Economy (WP 4.2.)**

The focus of this part was to analyse the adequacy of data economy rules when AI systems are in use. To do so, the study considered existing and future rules (and to some extent soft law as well) on personal and non-personal data portability, re-use of public sector information, data sharing between businesses and between businesses and the public sector. Considering that the report identified gaps and issues in this legal framework for the fields included in this study, several policy recommendations were formulated that could be implemented at the Belgian level to make the data economy fit for AI.

  - **Electronic Identification and Trust Services for Electronic Authentication (eIDAS) (WP 4.3.)**

No gaps were identified regarding the use of AI in the field of electronic identification. In order to improve the legal certainty, the scope of some guiding principles (e.g. freedom to use electronics, functional equivalency, non-discrimination and technological neutrality) included in the eIDAS Regulation may be expressly extended to AI.

  - **E-Commerce (WP 4.4.)**

Automated systems are used to detect and react to illegal content online and prevent the (re-)upload of the illegal content. However, the current state of AI technologies does not guarantee an infallible result. For that reason, the use of AI by intermediaries must be subject to legal regulations establishing appropriate safeguards, which the E-commerce Directive did not contain.

The identified gaps are addressed in the Proposal of a Digital Service Act (DSA Proposal) and the Proposal for a Regulation on AI (AI Act Proposal). Indeed, the DSA Proposal and the AI Act Proposal provide for information, transparency and reporting obligations. Besides, when machine learning models or algorithms make a decision about the legality of a content, there is a real risk of blocking lawful content and unduly restricting freedom of expression. The DSA Proposal

provides for a defined notice and action mechanism, appeal procedure and also a right to require that the decision made by AI technologies be reassessed by a human. Both Proposals provide for such a human-in-the-loop safeguard. However, their scope of application is too narrow as is Article 22 of the GDPR, which also requires the intervention of a human to challenge an automated decision. This human-in-the-loop guarantee should be a general guarantee to counter the risks created by automated and autonomous tools. Finally, the DSA proposal states that platforms will not lose their exemption from liability if they take active steps to prevent the (re-)uploading of illegal content to counter the reluctance of internet service providers to indulge in voluntary monitoring out of fear of losing the benefit of the liability exemption. In any case, as explained in the study, the Belgian legislator cannot intervene on a national level up until the European Regulations has been adopted.

- **Insurance (WP5)**

The use of AI by insurance companies might have multiple benefits to insurance companies as well as to insureds/beneficiaries and third parties but, at the same time, also raises various concerns and points for consideration (i.e. discrimination, exclusions, …). Although most of these concerns are not new nor AI-specific and thus well-known in insurance, close further monitoring will be necessary to determine whether and to what extent these concerns might be heightened by the use of AI. While some AI concerns are already covered by horizontal regulations (e.g. the GDPR and the AI Act Proposal), this part evaluated their application to the insurance sector, considering the sector's particularities. Moreover, account should be taken of the fact that the European insurance sector is already highly regulated by sector-specific instruments (e.g. Solvency II and IDD). Therefore, potential overlap with the existing regulatory framework is identified to avoid excessive regulatory burdens on innovation where possible. As far as we could ascertain, the level of penetration of AI systems in the Belgian insurance sector is currently still growing. Therefore, the proposals, inspired by initiatives taken in four neighbouring countries (NL, DE, FR, UK), also aim to be as technology-neutral and future-proof as possible.

SAMENVATTING (NL)

Artificiële intelligentie (AI) en robots worden steeds belangrijker in ons dagelijks leven. AI-systemen worden al voor allerlei doeleinden gebruikt en ingezet in tal van sectoren, zoals verkeer, gezondheidszorg, (gepersonaliseerde) marketing, bouw, fraudedetectie, inhoudsaanbeveling, het optimaliseren van bedrijfsprocessen, enz.

De opkomst van AI is geen verrassing gezien de vele voordelen die het biedt. Bedrijven uit verschillende sectoren vertrouwen bijvoorbeeld reeds op AI om kosten te verlagen, inkomsten te genereren, de productkwaliteit te verbeteren en hun concurrentievermogen te verhogen.

AI-gedreven applicaties hebben toegang tot veel meer gegevens om beslissingen te nemen en zijn ook nauwkeuriger en efficiënter omdat zij informatie sneller verwerken dan mensen. Als gevolg daarvan kunnen ze verschillende taken "beter" uitvoeren dan hun menselijke tegenhangers. AI biedt ook voordelen die eigen zijn aan de specifieke sectoren waarin ze kunnen worden aangewend. Autonome motorvoertuigen stellen bijvoorbeeld personen die zich voorheen niet met de wagen konden verplaatsen, in staat om toch zelfstandig aan het verkeer deel te nemen. Autonome motorrijtuigen zouden eveneens het aantal verkeersongevallen drastisch kunnen doen dalen. Het gebruik van AI zorgt echter ook voor heel wat ethische en juridische uitdagingen aangezien het gevolgen heeft voor bijna alle juridische domeinen.

In deze studie onderzochten we de impact van AI op een aantal juridische domeinen die onder de bevoegdheid vallen van de Federale Overheidsdienst (FOD) Economie, K.M.O., Middenstand en Energie.

In een eerste rapport beoordeelden we de impact van AI op verschillende juridische kaders die relevant zijn voor de FOD Economie (cf. analyse van mogelijk hiaten in regelgevende kaders).

In het tweede rapport voerden we een rechtsvergelijkende analyse uit van het beleid met betrekking tot AI in vier naburige landen: Frankrijk, Nederland, het Verenigd Koninkrijk en Duitsland. We gebruikten daarvoor een gestandaardiseerde vragenlijst.

In het laatste rapport formuleerden we een aantal concrete aanbevelingen waarop de FOD zich bij de uitwerking van het (toekomstig) AI-beleid kan baseren. Ook dat gebeurde op basis van een gestandaardiseerde vragenlijst. De samenvatting van onze bevindingen worden hieronder kort toegelicht.

- **Intellectuele eigendom en bedrijfsgeheimen(WP 2)**

Een van de onderwerpen die in deze studie worden bestudeerd, is de interactie tussen het intellectuele eigendomsrecht (IE) en AI. De vereisten voor IE-bescherming (met inbegrip van het auteurs- en octrooirecht) bevatten vaak verwijzingen naar menselijke actoren, waardoor het moeilijk is de relevante concepten toe te passen op creaties die tot stand komen met behulp van AI. Een cruciale stap in dat verband is het onderscheid te maken tussen door AI-ondersteunde creaties (beschermbaar) en door AI-gegenereerde creaties (niet-beschermbaar). De laatste categorie verwijst naar volledig autonome creaties door AI-systemen zonder significante relevante menselijke tussenkomst. Verder rijzen er ook vragen in verband met de praktische gevolgen die AI kan hebben voor ons huidige IE-stelsel (bv. voldoende openbaarmaking) en het risico op internationale regelgevende concurrentie voor de bescherming van door AI-gegenereerde creaties. Rekening houdend met die verschillende vraagstukken werd een lijst van voorstellen geformuleerd die het bestaande IE-kader moet versterken en tezelfdertijd de ontwikkeling, de introductie en het gebruik van AI-technologie in België en de Europese Unie (EU) moet bevorderen.

- **Consument en markt (WP 3)**

  - **Mededingingsrecht (WP 3.1.)**

Het huidige juridisch kader biedt geen bescherming tegen nieuwe digitale inbreuken op het mededingingsrecht, zoals collusie via algoritmen en prijsdiscriminatie. Indien anticompetitief

gedrag wordt uitgelokt door de werking van algoritmen zonder enige menselijke tussenkomst, zou ook dit als een inbreuk op het mededingingsrecht moeten worden

gekwalificeerd. Eens een schending met behulp van algoritmen wordt begaan, moet ook worden verzekerd dat de autoriteiten een actor aansprakelijk kunnen stellen. Dat probleem kan alleen op het EU-niveau worden opgelost door algoritmische collusie en prijsdiscriminatie door algoritmen als anticompetitief gedrag te kwalificeren.

- **Consumentenbescherming (WP 3.2.)**

De opzet van dit deel was om de effectiviteit van het consumentenbeschermingsrecht te analyseren als AI-systemen zijn ingevoerd. Hiervoor analyseerde de studie de huidige en toekomstige rechtsregels inzake garantie, informatieverplichtingen, aansprakelijkheid voor gebrekkige producten, oneerlijke marktpraktijken, toestemmingsvereisten en het gebruik van automatische middelen voor prospectie. Omdat de analyse verschillende leemten aan het licht bracht in het huidige wettelijke kader over de gebieden waarop deze studie betrekking heeft, werden verschillende aanbevelingen geformuleerd die op Belgisch niveau kunnen worden uitgevoerd om de consumentenbescherming geschikt te maken voor AI.

- **<u>Telecommunicatie en informatiemaatschappij (WP 4)</u>**

- **AI-veiligheid en cybersecurity (WP 4.1.)**

De focus van dit deel was om de verschillende regelgevende regimes in kaart te brengen die dienen om de schade veroorzaakt aan en door AI-systemen te beperken. Een belangrijke bevinding is dat het regelgevend kader een lappendeken is van verschillende soorten regelgevende regimes (bijv. contractenrecht, buitencontractueel aansprakelijkheidsrecht, productveiligheidswetgeving, gegevensbescherming, cybersecurity, en dat zowel algemeen als sectoraal). Die regimes verschillen allemaal qua toepassingsgebied en dekken elk specifieke risico's. Een gemeenschappelijk rode draad is dat zij open gedragsnormen combineren met een verwijzing naar technische normering om die open gedragsnormen in (vermoede) *best practices* om te zetten. Veel van die regels, zoals de wetgeving over productveiligheid, de AVG (Algemene Verordening Gegevensbescherming) en de wetten i.v.m. cybersecurity, vinden hun grondslag in EU-regulering. Dat lappendeken, alsook de afwezigheid en trage ontwikkeling van concrete standaarden voor AI-veiligheid, zijn een reden tot zorgen, aangezien zij lacunes in de risicodekking laten ontstaan en tegelijk zorgen voor een overlapping van risicomatigingstaken. Een convergentie van die regimes, alsook een duidelijke standaardisering is dus vereist. De EU-wetgever en internationale organisaties zijn al bezig met de ontwikkeling van dergelijke regulering. Daarom moet de Belgische wetgever zich (vooral) richten op de ondersteuning van die beleidsinitiatieven, alsook op een toenemende bewustmaking van de bevolking om hun toepassing te stimuleren. In het derde deel van de studie werden verschillende voorstellen gedaan om voornoemde lacunes op te vullen.

- **Data-economie (WP 4.2.)**

Dit deel richtte zich op een analyse van de toereikendheid van de regels in verband met de data-economie bij gebruik van AI-systemen. De analyse omvatte de huidige en toekomstige regels (en in zekere mate eveneens *soft law*) rond de overdraagbaarheid van persoons- en niet-persoonlijke gegevens, het hergebruik van informatie door de publieke sector, alsook het delen van data tussen ondernemingen onderling en tussen ondernemingen en de publieke sector. Gezien de studie verschillende lacunes en problemen aan het juridisch kader identificeerde, formuleerden we meerdere beleidsvoorstellen die op Belgisch niveau kunnen worden ingevoerd om de data-economie aan te passen aan AI.

- **Elektronische identificatie en vertrouwensdiensten voor elektronische authenticatie (eIDAS) (WP 4.3.)**

Geen lacunes werden geïdentificeerd betreffende het gebruik van AI voor elektronische identificatie. Om de rechtszekerheid te verbeteren, zou de reikwijdte van bepaalde principes (bijv. de vrijheid om elektronica te gebruiken, functionele equivalentie, niet-discriminatie en technologieneutraliteit) uit de eIDAS-Verordening uitdrukkelijk naar AI-systemen kunnen worden

uitgebreid.

- **Elektronische handel (WP 4.4.)**

Automatische systemen worden gebruikt om illegale content te detecteren en erop te reageren, alsook om de her-upload van digitale inhoud te verhinderen. De huidige staat van AI-technologie verzekert echter geen feilloos resultaat. Om die reden moet het gebruik van AI door tussenpersonen onderworpen worden aan rechtsregels die passende waarborgen bieden. Die waarborgen worden niet geboden door de richtlijn elektronische handel.

De geïdentificeerde lacunes worden ondervangen in het voorstel van een *Digital Services Act* (DSA-voorstel) en het voorstel voor een verordening over AI (Voorstel AI-Verordening). Het DSA-voorstel en het voorstel AI-verordening voorzien inderdaad in informatie-, transparantie- en rapporteringsverplichtingen. Wanneer modellen op grond van *machine learning* of andere algoritmen worden gebruikt om een beslissing te maken over de rechtmatigheid van content, is er ook een reëel risico dat rechtmatige inhoud wordt geblokkeerd en de vrijheid van meningsuiting op onrechtmatige wijze wordt ingeperkt. Het DSA-voorstel voorziet daarom in een vooraf bepaald mechanisme voor melding en actie, een beroepsprocedure en een recht om te vereisen dat een beslissing die AI-technologieën hebben gemaakt opnieuw door een mens wordt beoordeeld. Hun toepassingsgebied is echter te nauw, net zoals dat van artikel 22 AVG, dat ook een menselijke interventie vereist om een automatische beslissing aan te vechten. Die waarborg van een *human-in-the-loop* zou een algemene waarborg moeten bieden om de risico's van automatische en autonome tools te bestrijden. Ten slotte bepaalt het DSA-voorstel dat platformen hun aansprakelijkheidsbeperking niet zullen verliezen indien zij actieve stappen ondernemen om de (her)upload van illegale inhoud te verhinderen. Dat dient om de weigerachtigheid te bestrijden van internetdienstenleveranciers (ISPs) om op vrijwillige basis hun platformen te monitoren, uit vrees dat zij het voordeel van de aansprakelijkheidsbeperking zouden verliezen. In elk geval, en zoals uitgelegd in de studie, kan de Belgische wetgever niet op een nationaal niveau tussenkomen tot op het moment dat de Europese voorstellen werd aangenomen.

- **<u>Verzekeringen (WP 5)</u>**

Het gebruik van AI door verzekeringsondernemingen biedt verschillende voordelen voor zowel verzekeringsondernemingen als verzekerden/begunstigden en derde partijen, maar brengt ook diverse problemen en aandachtspunten met zich mee (bv. discriminatie, uitsluitingen, …). Hoewel die bezorgdheden niet nieuw zijn, noch specifiek voor AI zijn, en dus gekend zijn in de verzekeringssector, moet nader worden opgevolgd of en in hoeverre ze zouden kunnen toenemen door het gebruik van AI. Sommige van die bezorgdheden zijn reeds door horizontale wetgeving gereguleerd (zoals de AVG en het voorstel van een AI-verordening). Deze studie evalueert hun toepassing op de verzekeringssector, rekening houdend met zijn bijzondere kenmerken. Bovendien is de Europese verzekeringssector al in hoge mate gereglementeerd door sectorspecifieke instrumenten (e.g. Solvabiliteit II en IDD). Daarom worden potentiële overlappingen met het bestaande wetgevend kader geïdentificeerd om overregulering op innovatie te voorkomen waar mogelijk. Voor zover kon worden nagaan, is het gebruik van AI-systemen in de Belgische verzekeringssector nog volop in ontwikkeling. Bijgevolg beogen de voorstellen, die geïnspireerd zijn door initiatieven genomen in een aantal buurlanden (NL, DE, FR, UK), zo technologieneutraal en toekomstbestendig mogelijk te zijn.

RÉSUMÉ (FR)

L'intelligence artificielle (IA) et les robots occupent une place de plus en plus importante dans notre vie quotidienne. Les systèmes d'IA sont déjà utilisés à des fins diverses et sont déployés dans de nombreux secteurs tels que le trafic, la santé, le marketing (personnalisé), la fabrication, la détection des fraudes, la recommandation de contenu, etc.

L'essor de l'IA n'est pas une surprise compte tenu de ses nombreux avantages. Les systèmes d'IA traitent les informations plus rapidement que les humains. Par conséquent, ils peuvent effectuer de nombreuses tâches « mieux » que leurs homologues humains, améliorant ainsi la productivité et la compétitivité. Les systèmes d'IA peuvent également présenter des avantages pour le secteur spécifique dans lequel ils sont utilisés, notamment pour améliorer la sécurité. Les systèmes d'IA peuvent par exemple être utilisés pour détecter les défauts de fabrication ou pour réduire les accidents de la route et permettre une mobilité accrue pour les personnes qui ne sont pas capables de conduire un véhicule. Néanmoins, l'utilisation des systèmes d'IA implique également de nombreux défis éthiques et juridiques. La commercialisation de l'IA posera plusieurs défis d'un point de vue juridique et réglementaire car elle affecte presque toutes les matières du droit.

Dans cette étude, nous avons examiné l'impact des systèmes d'IA sur les domaines juridiques pour lesquels le Service public fédéral Economie, P.M.E., Classes moyennes et Energie (SPF) est compétent.

Dans un premier rapport, nous avons évalué l'impact de l'IA sur plusieurs domaines juridiques pertinents pour le SPF (analyse des gaps).

Dans le second rapport, nous avons effectué une analyse de droit comparé des initiatives concernant l'IA dans quatre juridictions : France, Pays-Bas, Royaume-Uni et Allemagne. Nous avons basé notre analyse sur un questionnaire standardisé.

Dans un dernier rapport, nous avons formulé des recommandations sur lesquelles le SPF peut s'appuyer pour le développement de sa (future) politique en matière d'IA. Pour cela, nous nous sommes à nouveau basés sur un questionnaire standardisé. Le résumé de nos conclusions est présenté ci-dessous.

- **Propriété intellectuelle et secrets d'affaire (WP 2)**

L'un des sujets étudiés dans cette étude est l'interaction entre le droit de la propriété intellectuelle (PI) et l'IA. Les exigences en matière de protection de la PI (y compris le droit d'auteur et le droit des brevets) contiennent souvent des références aux acteurs humains, ce qui rend difficile l'application des concepts pertinents aux créations générées en tout ou en partie par l'IA. Une étape cruciale à cet égard consiste à faire la distinction entre les créations assistées par l'IA (protégeables) des créations générées par l'IA (non protégeables), ces dernières faisant référence à des créations réalisées par des systèmes d'IA entièrement autonomes ne nécessitant aucune intervention humaine significative. D'autres questions se posent également en ce qui concerne l'impact pratique que l'IA peut avoir sur notre système actuel de propriété intellectuelle (par exemple, en termes de divulgation) et le risque de concurrence réglementaire internationale en matière de protection des créations générées par l'IA. En tenant compte de ces différentes questions, une liste de propositions a été formulée qui devrait renforcer le cadre actuel de la PI tout en soutenant la promotion du développement, de l'adoption et de l'utilisation de la technologie de l'IA en Belgique et dans l'Union européenne (UE).

- **Consommateur et marché (WP 3)**

  - **Droit de la concurrence (WP 3.1.)**

Le cadre juridique actuellement applicable en matière de concurrence n'aborde pas les nouvelles infractions numériques au droit de la concurrence, telles que la collusion par les algorithmes et la discrimination par les prix. Lorsque le comportement anticoncurrentiel est causé par le

fonctionnement d'algorithmes sans intervention humaine, il devrait constituer une infraction au droit de la concurrence. Une fois qu'une violation est commise par l'utilisation d'algorithmes, il faut également s'assurer qu'il est possible pour les autorités compétentes de tenir un acteur pour responsable. Ce problème ne peut être résolu au niveau de l'UE qu'en qualifiant la collusion algorithmique et la discrimination des prix par les algorithmes de comportement anticoncurrentiel.

- **Protection des consommateurs (WP 3.2.)**

L'objectif de cette partie était d'analyser l'adéquation des règles de protection des consommateurs lorsque des systèmes d'IA sont déployés. Pour ce faire, l'étude a pris en compte les règles juridiques existantes et futures relatives à la garantie, l'obligation d'information, la responsabilité pour les produits défectueux, les pratiques commerciales déloyales, les exigences en matière de consentement et l'utilisation de moyens automatisés pour la prospection. Dès lors que l'analyse a identifié plusieurs lacunes du cadre juridique actuel relatives aux domaines concernés par cette étude, plusieurs recommandations ont été formulées qui pourraient être mises en œuvre au niveau belge pour rendre la protection des consommateurs adaptée à l'IA.

- **<u>Télécommunication et société de l'information (WP4)</u>**

- **Sécurité de l'IA et cybersécurité (WP 4.1.)**

L'objectif de cette partie était de cartographier les différents régimes réglementaires en place qui atténuent les préjudices causés par et aux systèmes d'IA. Une constatation importante est que le cadre réglementaire est un patchwork de différents types de législations et règlementations tant générales que sectorielles (par exemple, le droit des contrats, le droit de la responsabilité civile, les lois sur la sécurité des produits, les lois sur la protection des données, les lois sur la cybersécurité). Ces régimes ont tous des champs d'application différents et couvrent des types de préjudices spécifiques. Leur point commun est qu'ils tendent à combiner des standards ouverts en matière de diligence avec une référence à la normalisation comme moyen d'opérationnaliser les normes comportementales ouvertes en pratiques (présumées) exemplaires. Un grand nombre de ces règles, telles que les règles applicables à la sécurité des produits, le RGPD et les lois sur la cybersécurité, sont réglementées au niveau de l'UE. Ce patchwork, ainsi que l'absence et la lenteur du développement de normes concrètes concernant la sécurité de l'IA, sont préoccupants. En effet, ils permettent de créer des brèches dans la couverture des risques et de doubler le travail en même temps. Une convergence de ces régimes ainsi qu'une normalisation claire sont donc nécessaires. Pour être clair, le législateur européen et les organisations internationales de normalisation y travaillent déjà. La Belgique devrait donc se concentrer sur le développement de ces règles et sur l'intensification des campagnes de sensibilisation afin de garantir l'utilisation de ces règles par le grand public. Plusieurs propositions visant à combler les lacunes réglementaires ont été formulées dans le troisième rapport.

- **Économie des données (WP 4.2.)**

L'objectif de cette partie était d'analyser l'adéquation des règles relatives à l'économie des données avec l'utilisation de systèmes d'IA. Pour ce faire, l'étude a examiné les règles existantes et futures (ainsi que, dans une certaine mesure, les règles non contraignantes) sur la portabilité des données personnelles et non personnelles, la réutilisation des informations du secteur public, le partage des données entre entreprises et entre les entreprises et le secteur public. Le rapport ayant identifié des lacunes et des problèmes dans ce cadre juridique pour les domaines concernés par cette étude, plusieurs recommandations politiques ont été formulées qui pourraient être mises en œuvre au niveau belge pour adapter l'économie des données à l'IA.

- **Identification électronique et services de confiance pour les transactions électronique (eIDAS) (WP 4.3.)**

Aucune lacune n'a été identifiée concernant l'utilisation de l'IA dans le domaine de l'identification électronique. Afin d'améliorer la sécurité juridique, le champ d'application de certains principes directeurs inclus dans le règlement eIDAS (par exemple, la liberté d'utiliser l'électronique, l'équivalence fonctionnelle, la non-discrimination et la neutralité technologique) pourrait être expressément étendu à l'IA.

- **Commerce électronique (WP 4.4.)**

Les systèmes automatisés sont utilisés pour détecter et réagir aux contenus illégaux en ligne et empêcher le (re)chargement de ces contenus sur internet. Cependant, l'état actuel des technologies d'IA ne garantit pas un résultat infaillible. C'est pourquoi l'utilisation de l'IA par les intermédiaires doit être soumise à des règles juridiques établissant des garanties appropriées, ce que la directive sur le commerce électronique ne contenait pas.

Les lacunes identifiées sont traitées dans la proposition de règlement sur les services numériques (DSA) et la proposition de règlement sur l'IA (AI Act). En effet, la proposition de DSA et la proposition de règlement sur l'IA prévoient des obligations d'information, de transparence et de signalement. Par ailleurs, lorsque des modèles d'apprentissage automatique ou des algorithmes prennent une décision concernant la légalité d'un contenu en ligne, il existe un réel risque de bloquer des contenus légaux et de restreindre indûment la liberté d'expression. La proposition de DSA prévoit un mécanisme de notification et action défini, une procédure de recours ainsi que le droit d'exiger que la décision prise par les technologies d'IA soit réévaluée par un humain. En réalité, les deux propositions européennes prévoient une telle intervention humaine (« human-in-the-loop »). Toutefois, leur champ d'application est trop étroit, comme l'est l'article 22 du RGPD, qui exige également l'intervention d'un humain pour contester une décision automatisée. Cette garantie devrait être une garantie générale pour contrer les risques créés par les outils automatisés et autonomes. Pour finir, la proposition de DSA stipule que les plateformes ne perdront pas leur exemption de responsabilité si elles prennent des mesures actives pour empêcher le (re)chargement de contenu illégal, afin de contrer la réticence des fournisseurs de services internet à se livrer à une surveillance volontaire par crainte de perdre le bénéfice de l'exemption de responsabilité. En tout état de cause, comme expliqué dans l'étude, le législateur belge ne peut intervenir au niveau national tant que les règlementations européennes n'ont pas été adoptées.

- **Assurance (WP5)**

L'utilisation de l'IA par les entreprises d'assurances pourrait présenter de multiples avantages pour les entreprises d'assurances ainsi que pour les assurés/bénéficiaires et les tiers mais, dans le même temps, elle soulève également diverses préoccupations (à savoir la discrimination, les exclusions, etc.). Bien que la plupart de ces préoccupations ne soient ni nouvelles ni spécifiques à l'IA et donc bien connues dans le domaine de l'assurance, une surveillance étroite sera nécessaire pour déterminer si, et dans quelle mesure, ces préoccupations pourraient être amplifiées par l'utilisation de l'IA. Cette partie de l'étude a évalué l'application des réglementations horizontales (par exemple, le RGPD et la proposition de règlementation sur l'IA) au secteur de l'assurance, compte tenu des particularités du secteur. En outre, il convient de tenir compte du fait que le secteur européen de l'assurance est déjà fortement réglementé par des instruments sectoriels (par exemple, Solvabilité II et DDA). Par conséquent, les chevauchements potentiels avec le cadre réglementaire existant sont identifiés afin d'éviter, dans la mesure du possible, des charges réglementaires excessives pesant sur l'innovation. D'après ce que nous avons pu vérifier, le niveau de pénétration des systèmes d'IA dans le secteur belge de l'assurance est actuellement en pleine croissance. Par conséquent, les propositions, inspirées par les initiatives prises dans quatre pays voisins, visent également à être aussi neutres que possible sur le plan technologique et à l'épreuve du futur.

ZUSAMMENFASSUNG (DE)

Künstliche Intelligenz (KI) und Roboter werden in unserem täglichen Leben immer wichtiger. KI-Systeme werden bereits für eine Vielzahl von Zwecken genutzt und in vielen Bereichen wie Verkehr, Gesundheit, (personalisiertes) Marketing, Produktion, Betrugserkennung, Content-Empfehlungen usw. eingesetzt. Der Vormarsch von KI ist angesichts der vielen Vorteile keine Überraschung. KI-Systeme verarbeiten Informationen schneller als Menschen. Folglich können sie viele Aufgaben „besser" als ihre menschlichen Pendants erledigen und so können sie die Produktivität und Wettbewerbsfähigkeit verbessern. KI-Systeme können auch für den jeweiligen Sektor, in dem sie eingesetzt werden, Vorteile bringen, auch im Hinblick auf Sicherheit. KI-Systeme können beispielsweise zur Erkennung von Produktionsfehlern oder zur Verringerung von Verkehrsunfällen eingesetzt werden und ermöglichen eine erhöhte Mobilität für Personen, die nicht in der Lage sind, selbst ein Fahrzeug zu bedienen. Der Einsatz von KI-Systemen ist allerdings auch mit vielen ethischen und rechtlichen Herausforderungen verbunden. Die Kommerzialisierung von KI wird aus rechtlicher und regulatorischer Sicht einige Herausforderungen mit sich bringen, da sie nahezu alle Rechtsbereiche betrifft.

In dieser Studie haben wir die Auswirkungen von KI-Systemen auf die Rechtsbereiche untersucht, für den Föderalen Öffentlichen Dienst (FÖD) Wirtschaft, KMB, Mittelstand und Energie zuständig ist. In einem ersten Bericht bewerteten wir die Auswirkungen von KI auf verschiedene Rechtsbereiche, die für den FÖD relevant sind (Analyse der rechtlichen Lücken). Im zweiten Bericht haben wir eine rechtsvergleichende Analyse der politischen Initiativen zu KI in vier Ländern durchgeführt: Frankreich, die Niederlande, das Vereinigte Königreich und Deutschland. Wir stützten unsere Analyse auf einen standardisierten Fragebogen. In einem abschließenden Bericht haben wir Empfehlungen formuliert, auf die sich den FÖD bei der Entwicklung ihrer (zukünftigen) KI-Politik stützen können. Auch dieser Bericht basierte auf einem standardisierten Fragebogen. DieZusammenfassung unserer Ergebnisse ist im Folgenden aufgeführt.

- **Geistiges Eigentum und Geschäftsgeheimnisse (WP 2)**

Eines der in dieser Studie untersuchten Themen ist die Interaktion zwischen dem geistigen Eigentum (IP) und KI. Die Anforderungen an den Schutz des geistigen Eigentums (einschließlich des Urheberrechts und des Patentrechts) enthalten häufig Verweise auf menschliche Akteure, die es schwierig machen, die entsprechenden Konzepte auf KI-gestützte Werke anzuwenden. Ein entscheidender Schritt in dieser Hinsicht ist der Unterschied zwischen KI-unterstützten Werken (schutzfähig) und KI-generierten Werken (nicht schutzfähig), die sich auf völlig autonome Werke von KI-Systemen ohne signifikante menschliche Intervention beziehen. Weitere Fragen ergeben sich im Hinblick auf die praktischen Auswirkungen, die KI auf unser derzeitiges System des geistigen Eigentums haben kann (z. B. ausreichende Offenlegung), und das Risiko eines internationalen Regulierungswettbewerbs im Hinblick auf den Schutz von KI-generierten Werken. Unter Berücksichtigung dieser verschiedenen Fragen wurde eine Liste von Vorschlägen formuliert, die den bestehenden Rahmen für geistiges Eigentum stärken und gleichzeitig die Entwicklung, Einführung und Nutzung der KI-Technologie in Belgien und der Europäischen Union (EU) fördern sollen.

- **Verbraucher und Markt (WP 3)**

  - **Wettbewerbsrecht (WP 3.1.)**

Der derzeit geltende Rechtsrahmen berücksichtigt nicht die neuen digitalen Verstöße gegen das Wettbewerbsrecht wie etwa Absprachen durch Algorithmen und Preisdiskriminierung. Wenn das wettbewerbswidrige Verhalten durch das Zusammenspiel von Algorithmen ohne menschliches Zutun verursacht wird, sollte diese Handlung einen Verstoß gegen das Wettbewerbsrecht darstellen. Sobald ein Verstoß durch den Einsatz von Algorithmen begangen wird, muss auch

sichergestellt werden, dass die Behörden einen Akteur zur Verantwortung ziehen können. Dieses Problem kann auf EU-Ebene nur gelöst werden, indem algorithmische Absprachen und Preisdiskriminierung durch Algorithmen als wettbewerbswidriges Verhalten eingestuft werden.

- **Verbraucherschutz (WP 3.2.)**

Der Schwerpunkt dieses Teils lag auf der Analyse der Angemessenheit der Verbraucherschutzvorschriften beim Einsatz von KI-Systemen. Zu diesem Zweck wurden in der Studie bestehende und künftige Rechtsvorschriften über Gewährleistung, Informationspflichten, Haftung für fehlerhafte Produkte, unlautere Geschäftspraktiken, Anforderungen an die Einwilligung und den Einsatz automatisierter Mittel zur Prospektion untersucht. Da die Analyse mehrere Lücken in dem rechtlichen Rahmen für die in dieser Studie berücksichtigten Bereiche aufzeigte, wurden mehrere Handlungsempfehlungen, die von belgischer Seite umgesetzt werden könnten, formuliert, um den Verbraucherschutz für KI tauglich zu machen.

- **Telekommunikation und Informationsgesellschaft (WP4)**

  - **KI-Sicherheit und Schutz (WP 4.1.)**

Der Schwerpunkt dieses Teils lag auf der Darstellung der verschiedenen Regulierungssysteme, die dazu dienen, die von und durch KI-Systeme verursachten Schäden zu verringern. Eine wichtige Erkenntnis ist, dass der Rechtsrahmen ein Geflecht aus verschiedenen Gesetzen und Regelungen ist (z. B. Vertragsrecht, Schadensersatzrecht, Produktsicherheitsgesetze, Datenschutzgesetze, Cybersicherheitsgesetze, welche sowohl allgemein als auch sektoral bestehen). Diese Regelungen haben alle einen unterschiedlichen Anwendungsbereich und decken bestimmte Arten von Schäden ab. Ein gemeinsamer Nenner ist, dass sie dazu neigen, offene Sorgfaltsnormen mit einem Verweis auf die Standardisierung zu kombinieren, um offene Verhaltensnormen in (mutmaßlich) beste Verfahren zu operationalisieren. Viele dieser Vorschriften, wie z. B. der Produktsicherheitsrahmen, die DSGVO und die Cybersicherheitsgesetze, sind auf EU-Ebene geregelt. Dieses regulatorische Geflecht sowie das Fehlen und die langsame Entwicklung konkreter Normen für die KI-Sicherheit sind besorgniserregend, da sie Lücken in der Risikodeckung entstehen lassen und gleichzeitig die Arbeit verdoppeln. Eine Konvergenz dieser Regelungen sowie eine klare Standardisierung sind daher erforderlich. Der EU-Gesetzgeber und die internationalen Standardisierungsorganisationen arbeiten bereits an diesem Thema. Daher sollte der Schwerpunkt in Belgien auf der Unterstützung dieser Regeln und auf der Verstärkung von Sensibilisierungskampagnen liegen, um ihre Verwendung durch die breite Öffentlichkeit sicherzustellen. Im dritten Bericht wurden bereits mehrere Vorschläge zur Behebung der (regulatorischen) Lücken erarbeitet.

  - **Datenökonomie (WP 4.2.)**

Der Schwerpunkt dieses Teils lag auf der Analyse der Angemessenheit der Regeln für die Datenwirtschaft beim Einsatz von KI-Systemen. Zu diesem Zweck wurden in der Studie bestehende und künftige Vorschriften (und in gewissem Umfang auch „Soft Law") über die Portabilität personenbezogener und nicht-personenbezogener Daten, die Weiterverwendung von Informationen des öffentlichen Sektors, den Datenaustausch zwischen Unternehmen sowie zwischen Unternehmen und dem öffentlichen Sektor untersucht. In Anbetracht der Tatsache, dass der Bericht Lücken und Probleme in diesem Gesetzesrahmen für die in dieser Studie berücksichtigten Bereiche aufzeigte, wurden mehrere politische Empfehlungen formuliert, die vom belgischen Gesetzgeber umgesetzt werden könnten, um die Datenwirtschaft tauglich für KI zu machen.

  - **Elektronische Identifizierung und Vertrauensdienste für die elektronische Authentifizierung (eIDAS) (WP 4.3.)**

Es wurden in Bezug auf die Nutzung von KI im Bereich der elektronischen Identifizierung keine Lücken festgestellt. Um die Rechtssicherheit zu verbessern, könnte der Geltungsbereich einiger in der eIDAS-Verordnung enthaltener Leitprinzipien (z. B. Freiheit der Nutzung von Elektronik, funktionale Gleichwertigkeit, Nichtdiskriminierung und technologische Neutralität) ausdrücklich auf KI ausgeweitet werden.

- **E-Commerce (WP 4.4.)**

Automatisierte Systeme werden eingesetzt, um illegale Inhalte im Internet aufzuspüren, zu intervenieren und das (erneute) Hochladen von illegalen Inhalten zu verhindern. Der derzeitige Stand der KI-Technologien garantiert jedoch kein unfehlbares Resultat. Aus diesem Grund muss die Nutzung von KI durch Vermittler gesetzlichen Regelungen unterliegen, die angemessene Schutzmaßnahmen vorsehen, was in der E-Commerce-Richtlinie nicht der Fall war.

Die festgestellten Regelungslücken werden in dem Vorschlag einen Digital Service Act (DSA-Vorschlag) und dem Vorschlag für eine Verordnung über KI (KI-Regelungsvorschlag) aufgegriffen. Der DSA-Vorschlag und der Vorschlag für eine KI-Verordnung sehen nämlich Informations-, Transparenz- und Berichtspflichten vor. Wenn maschinelle Lernmodelle oder Algorithmen eine Entscheidung über die Rechtmäßigkeit eines Inhalts treffen, besteht außerdem die Gefahr, dass rechtmäßige Inhalte blockiert und die Meinungsfreiheit unangemessen beschränkt wird. Der DSA-Vorschlag sieht einen definierten Benachrichtigungs- und Klagemechanismus, ein Rechtsmittelverfahren und auch das Recht vor, die Überprüfung der von KI-Technologien getroffenen Entscheidung durch einen Menschen zu verlangen. Beide Vorschläge sehen einen solchen Schutz vor, bei dem der Mensch im Mittelpunkt steht. Jedoch ist der Anwendungsbereich zu eng, ebenso wie der von Artikel 22 der DSGVO, der ebenfalls das Eingreifen eines Menschen erfordert, um eine automatisierte Entscheidung anzugreifen. Diese „Human-in-the-Loop"-Garantie sollte eine umfassende Garantie sein, um den Risiken zu begegnen, die durch automatisierte und autonome Instrumente entstehen. Schließlich sieht der DSA-Vorschlag vor, dass Plattformen ihre Haftungsbefreiung nicht verlieren, wenn sie aktive Schritte unternehmen, um das (erneute) Hochladen illegaler Inhalte zu verhindern, um der fehlenden Bereitschaft von Internetdienstanbietern entgegenzuwirken, welche aus Angst, den Vorteil der Haftungsbefreiung zu verlieren, eine freiwillige Überwachung vorzunehmen. In jedem Fall kann der belgische Gesetzgeber, wie in der Studie erläutert, bis zur Verabschiedung der DSA nicht auf nationaler Ebene intervenieren.

- **<u>Versicherungen (WP5)</u>**

Der Einsatz von KI durch Versicherungsunternehmen kann sowohl für die Versicherungsunternehmen als auch für die Versicherten/Begünstigten und Dritte zahlreiche Vorteile mit sich bringen, wirft aber gleichzeitig auch verschiedene Bedenken und Überlegungen auf (z. B. Diskriminierung, Ausschlüsse, ...). Obwohl die meisten dieser Bedenken weder neu noch KI-spezifisch und daher im Versicherungswesen bekannt sind, ist eine genaue weitere Beobachtung erforderlich, um festzustellen, ob und inwieweit diese Bedenken durch den Einsatz von KI noch verstärkt werden könnten. Während einige KI-Bedenken bereits durch horizontale Vorschriften abgedeckt sind (z. B. die DSGVO und der Vorschlag für ein KI-Gesetz), wurde in diesem Teil ihre Anwendung auf den Versicherungssektor unter Berücksichtigung der Besonderheiten dieses Sektors bewertet. Außerdem sollte berücksichtigt werden, dass der europäische Versicherungssektor bereits durch sektorspezifische Instrumente (z. B. Solvency II und IDD) stark reguliert ist. Daher werden potenzielle Überschneidungen mit dem bestehenden Rechtsrahmen ermittelt, um übermäßige regulatorische Belastungen für Innovationen nach Möglichkeit zu vermeiden. Soweit wir feststellen konnten, ist derzeit der Grad der Verbreitung von KI-Systemen im belgischen Versicherungssektor noch wachsend. Daher zielen die Vorschläge, die sich an Initiativen in vier Nachbarländern orientieren, auch darauf ab, so technologieneutral und zukunftssicher wie möglich zu sein.