7-328/1

SÉNAT DE BELGIQUE

SESSION DE 2021-2022

23 FÉVRIER 2022

Proposition de résolution relative à la mise en place d'une autorité de contrôle des algorithmes

(Déposée par M. Rik Daems et consorts)

DÉVELOPPEMENTS

I. INTRODUCTION: ALGORITHMES, OÙ EST LE PROBLÈME?

Les algorithmes sont omniprésents sur l'internet. Il s'agit de règles mathématiques qui, dans les coulisses des entreprises de médias sociaux, sont les rouages indispensables de la sélection des contenus qui seront présentés à l'internaute. Ils sont toutefois de plus en plus controversés.

C'est avant tout sur l'internet qu'ils sont présents de manière tangible. Et l'on pense d'abord aux médias sociaux. Les chambres d'écho et les bulles de filtres y sont légion et ont pour but premier de maintenir l'internaute le plus longtemps possible sur le site web en question. Cela a pour effet secondaire de précipiter l'utilisateur dans un piège bien connu où, à la longue, il ne reçoit plus que des messages qui confirment son opinion et qui deviennent de plus en plus radicaux et polarisants.

Les algorithmes se rencontrent cependant aussi en dehors des médias sociaux. On les trouve dans le secteur privé, où ils sont surtout utilisés à des fins de marketing (publicité ciblée), mais on tente également d'introduire ces applications dans le secteur public, avec un succès variable.

Une étude réalisée aux États-Unis a ainsi démontré que les algorithmes utilisés dans les hôpitaux présentaient un biais important qui discriminait systématiquement

BELGISCHE SENAAT

ZITTING 2021-2022

23 FEBRUARI 2022

Voorstel van resolutie met betrekking tot oprichting van een algoritmetoezichthouder

(Ingediend door de heer Rik Daems c.s.)

TOELICHTING

I. INLEIDING: ALGORITMEN, WAT IS HET PROBLEEM?

Algoritmen zijn alomtegenwoordig op het internet. Dit zijn in wezen wiskundige regels die achter de schermen van sociale mediabedrijven de onmisbare tandwielen zijn die de content selecteren en bij de gebruiker aanleveren. Ze staan echter steeds meer ter discussie.

De plaats waar ze in eerste instantie voelbaar zijn, is op het internet. Er wordt dan in hoofdzaak gedacht aan de sociale media. Echokamers en filterbubbels zijn er legio en hebben als primair doel de gebruiker zo lang mogelijk op de website in kwestie te houden. Dit heeft als neveneffect dat de gebruiker in een spreekwoordelijke fuik terechtkomt waarin hij of zij op de lange duur enkel nog bevestigende berichten tegenkomt, die voortdurend feller en polariserender worden.

Algoritmen komen echter ook buiten de sociale media voor. Naast de private sector, waar algoritmen vooral voor marketingdoeleinden worden gebruikt (*targeted ads*), tracht men deze toepassingen met wisselend succes ook te implementeren in de publieke sector.

Zo was er in de Verenigde Staten een studie die aantoonde dat algoritmen die gebruikt werden door ziekenhuizen, een zware bias vertoonde waarbij het zwarte

les personnes noires (1). Ils étaient intégrés dans un programme que les hôpitaux américains utilisaient à grande échelle pour l'attribution des soins aux patients.

L'étude, publiée dans la revue scientifique *Science*, arrivait à la conclusion que sous l'effet de l'algorithme, les noirs, alors qu'ils souffraient d'une maladie de même gravité que les blancs, étaient moins souvent dirigés vers des programmes destinés à améliorer les soins aux patients ayant des besoins médicaux complexes (2).

C'est pour la même raison que le modèle dit de «*predictive policing*» (police prédictive) fait l'objet de critiques aux Pays-Bas. D'aucuns craignent qu'à terme, les algorithmes subissent l'influence de préjugés et de stéréotypes et influencent à leur tour les futurs modèles prédictifs et algorithmes. Cela produirait des résultats discriminatoires se traduisant par des niveaux de risque supérieurs pour certains groupes de la population (3).

Il est nécessaire de paramétrer les algorithmes avec précision, pour pouvoir les utiliser de manière responsable. Les préjugés (tant implicites qu'explicites) des développeurs, le volume de l'*input* et le type d'*input* sont tous lourds de conséquences sur le développement et le paramétrage d'un algorithme. Ces éléments suffisent parfois à faire la différence entre la qualité de «suspect» et la qualité de «non-suspect» et ont donc une importance capitale pour les personnes concernées.

Nous ne pouvons par conséquent plus rester spectateurs et laisser aux fournisseurs de technologies, aux programmeurs et aux développeurs de logiciels le soin de régler ces questions. La numérisation nous concerne tous, que ce soit dans la sphère publique ou dans la sphère privée. Ces algorithmes ont d'importantes répercussions sociales et politiques. Une régulation ou une forme de contrôle est nécessaire.

Les Pays-Bas ont déjà pris des initiatives à cet égard. Lors de l'élaboration de l'accord de gouvernement de 2021, il a été décidé de mettre en place une autorité de contrôle des algorithmes.

(1) *https://www.nature.com/articles/d41586-019-03228-6#ref-CR1.*
(2) Obermeyer, Z., Powers, B., Vogeli, C. et Mullainathan, S., «Dissecting racial bias in an algorithm used to manage the health of populations», in *Science*, vol. 336, nº 6464, 25 octobre 2019, pp. 447-453.
(3) *https://www.amnesty.nl/actueel/nederland-maak-een-einde-aan-gevaarlijke-politie-experimenten-met-massasurveillance.*

mensen systematisch discrimineerde (1). Het maakte deel uit van een programma dat in Amerikaanse ziekenhuizen op grote schaal wordt gebruikt om gezondheidszorg aan patiënten toe te wijzen.

De studie, die in het wetenschappelijk tijdschrift *Science* werd gepubliceerd, concludeerde dat het algoritme zwarten minder vaak dan blanken – die even ziek waren – doorverwees naar programma's die erop gericht zijn de zorg voor patiënten met complexe medische behoeften te verbeteren (2).

Het zogenaamde «*predictive policing*» model in Nederland krijgt om dezelfde reden kritiek. Ook hier is men bezorgd dat op termijn de algoritmen onderworpen worden aan vooroordelen en stereotypen. Dit beïnvloedt op zijn beurt de toekomstige voorspellingsmodellen en algoritmen. Dit leidt tot discriminerende uitkomsten met hogere risicoscores voor bepaalde maatschappelijke bevolkingsgroepen (3).

Algoritmen moeten nauwkeurig afgesteld worden alvorens ze op verantwoorde wijze gebruikt kunnen worden. Vooroordelen (zowel impliciet als expliciet) van de ontwikkelaars, de hoeveelheid input en de soort van input hebben allemaal verregaande gevolgen voor de ontwikkeling en afstelling van een algoritme. Dit kan soms het verschil maken tussen «verdacht» of «niet verdacht», en is dus van zeer groot belang voor de betrokkenen.

We kunnen daarom niet langer toekijken en dit louter aan *techproviders*, programmeurs en softwareontwikkelaars overlaten. De digitalisering treft ons allemaal, zowel in de publieke als in de private sfeer. Deze algoritmen hebben een diepe sociale en politieke impact. Een regulering of vorm van toezicht is noodzakelijk.

In Nederland staat men hier reeds verder mee. In het kader van het regeerakkoord van 2021 besliste men daarom om een algoritmetoezichthouder aan te stellen.

(1) *https://www.nature.com/articles/d41586-019-03228-6#ref-CR1.*
(2) Obermeyer, Z., Powers, B., Vogeli, C. en Mullainathan, S., «Dissecting racial bias in an algorithm used to manage the health of populations», in *Science*, vol. 336, nr. 6464, 25 oktober 2019, blz. 447-453.
(3) *https://www.amnesty.nl/actueel/nederland-maak-een-einde-aan-gevaarlijke-politie-experimenten-met-massasurveillance.*

II. ALGORITHMES ET ENVIRONNEMENT

A. Algorithmes dans le secteur privé

Les algorithmes servent en premier lieu à répondre aux besoins de l'utilisateur. Lorsqu'un consommateur achète un produit dans une boutique en ligne, il se voit souvent proposer des articles apparentés qui sont aussi susceptibles de l'intéresser. Il en va de même dans d'autres domaines, tels que la collecte d'informations.

La numérisation modifie les modes de consommation de l'information, qui sont de plus en plus déterminés par des algorithmes commerciaux. Ceux-ci sont alimentés par des métriques de popularité, les *likes* et les *shares*.

Il n'est donc pas étonnant que les algorithmes fassent la loi sur internet, en particulier sur les réseaux sociaux. L'explosion du nombre d'informations et de désinformations, ainsi que la forte accélération de leur diffusion sont surtout dues aux algorithmes utilisés par les médias sociaux.

Ces formules mathématiques visent en effet à proposer toujours plus de contenu similaire à celui que l'utilisateur consomme. Pour ce faire, on mesure différents paramètres de l'utilisateur: la durée de visionnage d'une vidéo, les clics sur des liens, les *likes* attribués, etc.

Le but est de faire en sorte que l'utilisateur reste le plus longtemps possible sur le site internet, afin qu'il puisse voir un maximum de publicités. Tout le modèle économique de la plupart des sociétés de médias sociaux (comme *Facebook*) repose sur les revenus publicitaires. Il est donc capital que les utilisateurs du site internet restent stimulés, afin qu'ils surfent plus longtemps sur le site et puissent voir davantage de publicités.

Concrètement, l'utilisateur ne voit donc pas l'ensemble du spectre, mais uniquement des messages qui corroborent des opinions précédentes. C'est le fondement de la polarisation et des chambres d'écho.

B. Algorithmes, infox (*fake news*) et chambres d'écho

Le problème des algorithmes sur les réseaux sociaux réside dans le fait qu'ils sont également responsables de la diffusion d'informations. Plus un message ou une information suscite des interactions (*likes*, *upvotes* (votes ascendants), clics, etc.), plus l'algorithme les mettra en avant. Il existe toutefois un déséquilibre dans

II. ALGORITMEN EN OMGEVING

A. Algoritmen in de private sector

Algoritmen dienen er in eerste instantie toe te voorzien in de behoeften van de gebruiker. Wanneer men iets in een webshop koopt, krijgt men vaak aanverwante artikelen te zien die de koper ook kunnen interesseren. Dit geldt ook voor andere domeinen, zoals nieuwsgaring.

Door de digitalisering zien we wijzigingen in de nieuwsconsumptie, die in toenemende mate bepaald wordt door commerciële algoritmen. Die worden gevoed door populariteitsmetrieken, de zogenaamde *likes* en *shares*.

Het is dan ook geen wonder dat algoritmen online de boventoon voeren, in het bijzonder op sociale media. De enorme toename van de omvang en de snelheid van verspreiding van informatie en desinformatie heeft vooral te maken met de algoritmen die sociale media gebruiken.

Met deze wiskundige formules wordt namelijk continu geprobeerd meer van dezelfde inhoud aan te bieden die de gebruiker consumeert. Dit doet men via het meten van verschillende parameters: hoe lang men naar een filmpje kijkt, welke links men aanklikt, welke *likes* er gegeven worden, enz.

Het doel is de gebruiker zo lang mogelijk op de website te houden, zodat hij of zij meer advertenties te zien krijgt. Het hele economische model van de meeste sociale mediabedrijven (zoals dat van *Facebook*) hangt af van advertentie-inkomsten. Het is dus van groot belang dat de gebruikers van de website geprikkeld blijven, zodat ze er langer op blijven en dus meer advertenties kunnen zien.

Dit betekent dus in de praktijk dat de gebruiker niet het volledige plaatje te zien krijgt, maar slechts berichten waarin eerdere meningen worden bevestigd. Dit legt het fundament voor polarisering en echokamers.

B. Algoritmen, *fake news* en echokamers

Het probleem met algoritmen op sociale media is dat ze ook instaan voor de verspreiding van berichten. Hoe meer interactie er is met bepaalde berichten (*likes*, *upvotes*, kliks, enz.), hoe meer het algoritme deze berichten zal bevoordelen. Er bestaat echter een onevenwicht in de platformarchitectuur, want polariserende inhoud krijgt

l'architecture de la plateforme, car un contenu polarisant attire davantage l'attention des utilisateurs qu'un contenu neutre, et il est aussi repéré plus rapidement par les algorithmes.

C'est la raison pour laquelle un contenu hyperpolarisant, qui relève souvent aussi de l'infox, est davantage et plus rapidement partagé que des informations factuelles et neutres.

Les révélations des *Facebook Papers* confirment ce constat. À partir de 2017, l'algorithme de *Facebook* a accordé cinq fois plus d'importance à la réaction par l'émoticône «fâché» qu'à la réaction «j'aime», de sorte que les informations en question apparaissaient plus souvent dans les fils d'actualité des utilisateurs. La théorie était simple: les informations qui généraient de nombreuses réactions par émoticônes impliquaient davantage les utilisateurs, et l'implication permanente des utilisateurs était le but principal de *Facebook* (4). Ce système n'a été modifié que plus tard.

Il en résulte en outre un phénomène de cloisonnement algorithmique, mieux connu sous le nom de «bulle d'information». Une bulle d'information constitue un réseau très homogène dans lequel les utilisateurs suivent principalement des personnes de «leur» bulle et ne sont plus confrontés à d'autres opinions. Cela crée en fin de compte des chambres d'écho, c'est-à-dire des espaces virtuels au sein desquels la conviction personnelle de l'utilisateur est répétée comme un écho par des personnes qui partagent les mêmes idées.

Ce phénomène d'autoconfirmation polarise encore plus la population. On élude les autres opinions et, finalement, de nombreuses personnes sont de moins en moins capables d'accepter des opinions différentes, ce qui ne fait que perpétuer la polarisation.

Les infox en particulier sont le venin qui empoisonne insidieusement la société. Un citoyen d'une société démocratique ne peut pas faire des choix mûrement réfléchis s'il est submergé jour et nuit d'informations erronées et trompeuses. C'est aussi pour cette raison que le Sénat a déjà entrepris des démarches pour tenter d'inverser la tendance par le biais du rapport d'information concernant la nécessaire collaboration entre l'autorité fédérale et les Communautés en matière de lutte contre les infox (*fake news*) (5).

(4) *https://www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm/.*
(5) Doc. Sénat, nº 7-110/1-4.

meer aandacht van gebruikers dan neutrale inhoud. Deze inhoud wordt ook sneller opgepikt door algoritmen.

Dit is de reden waarom hyperpolariserende inhoud, die vaak ook *fake news* is, meer en sneller wordt gedeeld door algoritmen dan feitelijk, neutraal nieuws.

De onthullingen van de *Facebook-papers* bevestigen dit. Vanaf 2017 gaf het algoritme van *Facebook emoji*-reacties zoals «boos» vijf keer zoveel gewicht als «vind ik leuk», waardoor deze berichten een boost kregen in de *feeds* van gebruikers. De theorie was eenvoudig: berichten die veel reactie-*emoji's* uitlokten, maakten gebruikers meer betrokken. Gebruikers betrokken houden was immers *Facebook*'s hoofddoel (4). Pas later werd dit aangepast.

Bovendien leidt het tot algoritmische verzuiling, beter bekend als informatiebubbels. Een informatiebubbel vormt een heel homogeen netwerk waarin gebruikers vooral personen binnen de bubbel volgen en niet meer in contact komen met andere meningen. Dit geeft uiteindelijk echokamers. Deze echokamers zijn virtuele plaatsen waarin de eigen overtuiging als een echo wordt herhaald door mensen die hetzelfde denken.

Dit polariseert de bevolking verder omdat het zelfbevestigend werkt. Het ontwijkt andere meningen en zorgt ervoor dat velen steeds minder in staat zijn om andere meningen te accepteren, wat de polarisering bestendigt.

Fake news in het bijzonder is het sluipende gif in de bloedbaan van de samenleving. Burgers in een democratische samenleving kunnen geen goede, weldoordachte keuzes maken als ze dag en nacht overspoeld worden door foutieve en misleidende informatie. Het is ook daarom dat de Senaat met het informatieverslag over de noodzakelijke samenwerking tussen de federale overheid en de Gemeenschappen inzake de bestrijding van *fake news* reeds stappen heeft gezet om te pogen deze trend te keren (5).

(4) *https://www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm/.*
(5) Doc.Senaat, nr. 7-110/1-4.

Dans cette optique, il est donc important de lutter non seulement contre les infox en tant que telles, mais aussi contre les mécanismes (en l'occurrence, les algorithmes) qui facilitent leur diffusion.

C. Algorithmes dans le secteur public

Outre le secteur privé, qui recherche avant tout le profit commercial, le secteur public recourt de plus en plus aux algorithmes dans le contexte de la numérisation.

Le modèle de la police prédictive (*predictive policing*) est un exemple que l'on cite souvent. Les Pays-Bas sont déjà plus avancés dans ce domaine. En 2016, le Conseil scientifique néerlandais pour la politique gouvernementale a ainsi rédigé un rapport indiquant notamment que les mégadonnées (*big data*) peuvent améliorer la sécurité du pays. La police néerlandaise, par exemple, en fait usage.

La police néerlandaise a réalisé un test d'utilisation des mégadonnées en vue de prédire la survenance de certains délits dans un intervalle de temps déterminé et à un endroit donné. Voilà un bon exemple d'utilisation des mégadonnées par le secteur public pour améliorer son efficacité de manière innovante.

Le fait de prédire où la criminalité aura lieu est aussi désigné par la notion de «police prédictive», un phénomène relativement récent qui est né aux États-Unis en 2008. L'idée de la police prédictive a aussi gagné les Pays-Bas, où la police a commencé à l'appliquer en 2014 à Amsterdam, dans le cadre du programme CAS (*Criminaliteits Anticipatie Systeem* ou Système d'anticipation de la criminalité) (6).

Selon la police néerlandaise, 40 % des cambriolages dans les habitations et 60 % des vols à la tire peuvent être prédits. Le système CAS s'appuie sur de grandes quantités de données provenant de plaintes déposées à la police, de statistiques de criminalité et de la banque de données du Bureau central de la statistique (*Centraal Bureau voor de statistiek* – CBS). Il s'agit concrètement d'informations concernant le nombre d'allocations octroyées par quartier, l'âge, le sexe et la composition de ménage, à partir desquelles les algorithmes déterminent où et quand la police peut s'attendre à un risque de criminalité accru.

(6) van der Eijk, L., *A successful implementation of predictive policing: An analysis of the Dutch police working with CAS*, mémoire de master, faculté *Governance and Global Affairs*, Université de Leyde, 7 janvier 2021.

In het licht hiervan is het dus belangrijk dat men niet enkel *fake news* als zodanig aanpakt maar ook de mechanismen (namelijk de algoritmen), waardoor het gefaciliteerd en verspreid wordt.

C. Algoritmen in de publieke sector

Naast de private sector, waar men vooral naar commercieel gewin kijkt, maakt ook de publieke sector, in het kader van de digitalisering, steeds meer gebruik van algoritmen.

Een veelgenoemd voorbeeld is het zogenaamde «*predictive policing*»-model. In Nederland staat men hierbij reeds verder. In 2016 schreef de Nederlandse Wetenschappelijke Raad voor het regeringsbeleid een rapport waarin stond dat *big data* de veiligheid van het land kan verbeteren. Een voorbeeld hiervan is de Nederlandse politie.

Zij hebben een poging gedaan om *big data* te gebruiken om het voorkomen van bepaalde misdrijven in een bepaald tijdslot en op een bepaalde plaats te voorspellen. Dit is een goed voorbeeld van het gebruik van *big data* door de publieke sector, als innovatie om hun efficiëntie te verbeteren.

Voorspellen waar criminaliteit zal plaatsvinden wordt ook wel *predictive policing* genoemd en is een relatief nieuw fenomeen, met wortels in de Verenigde Staten in 2008. Het idee van *predictive policing* heeft ook Nederland bereikt en de Nederlandse politie is in 2014 begonnen met de implementatie van *predictive policing* in Amsterdam met een programma genaamd het «Criminaliteits Anticipatie Systeem» (CAS) (6).

Volgens de Nederlandse politie kan 40 % van de woninginbraken en 60 % van de straatroven worden voorspeld. Het CAS-systeem gebruikt veel data die voortvloeien uit aangiftes, criminaliteitscijfers en gegevens van het Centraal Bureau voor de statistiek (CBS). Hierbij gaat het concreet om informatie over het aantal uitkeringen per wijk, leeftijden, geslacht en de gezinssamenstellingen. Algoritmen bepalen vervolgens waar en wanneer de politie een verhoogde kans op criminaliteit kan verwachten.

(6) van der Eijk, L., *A successful implementation of predictive policing: An analysis of the Dutch police working with CAS*, master thesis, Faculteit *Governance and Global Affairs*, Universiteit Leiden, 7 januari 2021.

D. Les dangers liés aux algorithmes et prédictions en l'absence de régulation

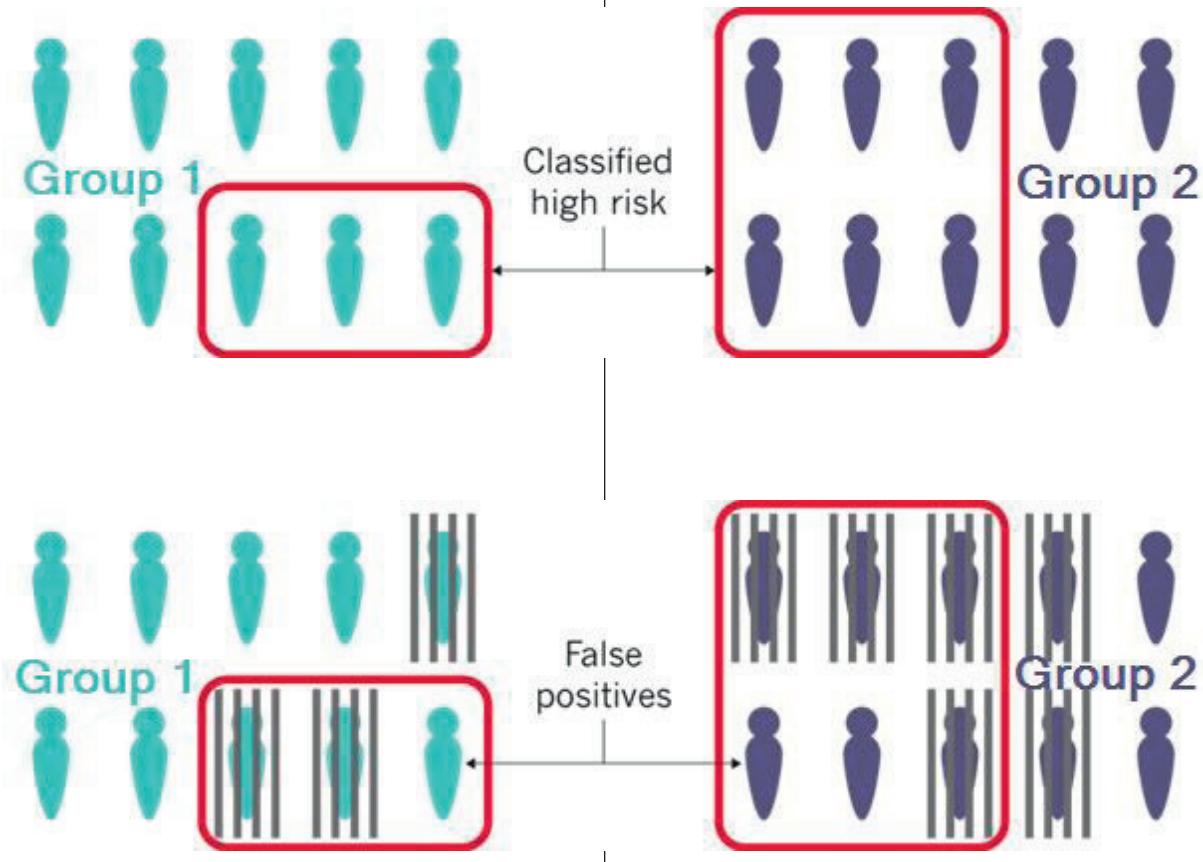
Les algorithmes sont aussi équitables que leurs programmeurs veulent qu'ils le soient. Le risque de biais est donc bien réel.

Imaginons qu'un algorithme utilisé dans le système pénal (comme aux Pays-Bas) attribue des scores à deux groupes de personnes selon le risque qu'elles présentent d'être à nouveau arrêtées. Dans l'exemple illustré ci-dessous, les données historiques indiquent que le groupe 2 présente un taux d'arrestation plus élevé, de sorte que le modèle considérerait davantage de personnes du groupe 2 comme étant à haut risque (7).

D. De gevaren van ongereguleerde algoritmen en voorspellingen

Algoritmen zijn maar zo «*fair*» als de mate waarin ze door programmeurs zo zijn afgesteld. Het gevaar op bias is dus reëel.

Stel dat een algoritme voor gebruik in het strafrechtelijk systeem (zoals in Nederland) scores toekent aan twee groepen voor hun risico om opnieuw te worden gearresteerd. Historische gegevens wijzen in dit voorbeeld erop dat «*group 2*» een hoger arrestatiecijfer heeft, zodat het model meer mensen in «*group 2*» als hoogrisicogroep zou classificeren (7).



Tant que des pourcentages différents de membres du groupe 1 et de membres du groupe 2 seront à nouveau arrêtés, il sera difficile d'atteindre l'équité prédictive et des pourcentages égaux de faux positifs.

D'aucuns pourraient considérer le fait que le groupe 2 présente un taux plus élevé de faux positifs comme de la

Zolang leden van «*group 1*» en «*group 2*» met verschillende percentages opnieuw worden gearresteerd, zal het moeilijk zijn om predictieve gelijkheid en gelijke vals-positieve percentages te bereiken.

Sommigen zouden de hogere fout-positieve percentages voor «*group 2*» als discriminatie zien. Maar andere

(7) *https://www.nature.com/articles/d41586-018-05469-3.*

(7) *https://www.nature.com/articles/d41586-018-05469-3.*

discrimination. D'autres chercheurs affirment toutefois qu'il ne s'agit pas nécessairement là d'une preuve évidente de parti pris dans l'algorithme. Le déséquilibre pourrait s'expliquer par une cause plus profonde: les membres du groupe 2 pourraient avoir été initialement ciblés à tort comme des personnes susceptibles d'être à nouveau arrêtées. En s'appuyant sur des données du passé pour prévoir avec précision que plus de personnes du «groupe 2» feront l'objet d'une nouvelle arrestation, l'algorithme pourrait reproduire voire ancrer un préjugé déjà présent dans la société.

C'est la raison pour laquelle des organisations telles qu'*Amnesty International* s'inquiètent à propos de la police prédictive, telle qu'appliquée par exemple aux Pays-Bas. Les modèles mathématiques qui sous-tendent les algorithmes prédictifs pourraient perpétuer, légitimer voire reproduire les préjugés et la discrimination à l'encontre de certains groupes (les Européens de l'Est, les étrangers, les allochtones, etc.) (8).

Cela nous conforte dans notre demande de mise en place d'une autorité de contrôle des algorithmes.

III. ALGORITHMES ET CONTRÔLE: VERS UNE RÉGULATION DES ALGORITHMES

L'accord de gouvernement conclu lors de la formation de la coalition gouvernementale néerlandaise en 2021 prévoit une intensification des efforts déployés par le pays en matière de numérisation. Outre les déclarations usuelles par lesquelles le gouvernement promet, entre autres, de continuer à réduire le fossé numérique et à renforcer la sécurité sur l'Internet, le texte contient une déclaration concernant la mise en place d'une autorité de contrôle des algorithmes chargée de veiller au respect des règles légales de contrôle des algorithmes en termes de transparence, de discrimination et d'arbitraire (9).

Ce projet n'arrive pas par hasard: le scandale des allocations de garde d'enfants aux Pays-Bas a montré que l'administration fiscale se fiait à des algorithmes qu'elle comprenait à peine et pouvait encore moins expliquer.

Aux États-Unis, où l'usage d'algorithmes au sein du secteur public est déjà beaucoup plus répandu, il est également apparu que plusieurs services concernés ne disposaient pas de suffisamment de moyens pour évaluer les algorithmes qu'ils utilisaient eux-mêmes (10).

(8) *https://www.amnesty.nl/actueel/nederland-maak-een-einde-aan-gevaarlijke-politie-experimenten-met-massasurveillance.*
(9) *https://www.parlement.com/id/vloreou0m8t6/regeerakkoord_2021.*
(10) *https://www.nature.com/articles/d41586-018-05469-3.*

onderzoekers beweren dat dit niet noodzakelijk een duidelijk bewijs is van vooringenomenheid in het algoritme. Er zou een diepere oorzaak voor de onevenwichtigheid kunnen zijn: «*group 2*» zou in de eerste plaats ten onrechte voor arrestatie in aanmerking kunnen zijn gekomen. Door op basis van gegevens uit het verleden nauwkeurig te voorspellen dat meer mensen uit «*group 2*» opnieuw zullen worden gearresteerd, zou het algoritme een reeds bestaand maatschappelijk vooroordeel kunnen herhalen – en misschien verankeren.

Het is daarom dat bepaalde organisaties als *Amnesty International* zich zorgen maken om *predictive policing*, zoals in Nederland. De wiskundige modellen achter de voorspellende algoritmen zouden vooroordelen en discriminatie jegens bepaalde groepen (Oost-Europeanen, buitenlanders, allochtonen, enz.) kunnen bestendigen, legitimeren en zelfs reproduceren (8).

Dit bestendigt onze vraag naar een toezichthouder voor deze algoritmen.

III. ALGORITMEN EN HANDHAVING: NAAR EEN REGULERING VAN ALGORITMEN

Bij de regeringsvorming in Nederland in 2021 werd in de beleidsverklaring van het regeerakkoord gesteld dat het land inzet op meer digitalisering. Naast de gebruikelijke verklaringen, waarbij men onder meer belooft verder in te zetten op de digitale kloof en de veiligheid op het internet, wordt ook vermeld dat men een algoritmetoezichthouder zal aanstellen om wettelijk te regelen «dat algoritmen worden gecontroleerd op transparantie, discriminatie en willekeur» (9).

Deze oproep komt niet toevallig: de Nederlandse toeslagenaffaire liet zien dat de Belastingdienst vertrouwde op algoritmen die ze zelf amper kon begrijpen, laat staan uitleggen.

Ook in de Verenigde Staten, waar algoritmen binnen de openbare sector al veel verder verspreid zijn, bleek dat verschillende van deze diensten over onvoldoende middelen beschikten om de algoritmen te evalueren die ze zelf gebruikten (10).

(8) *https://www.amnesty.nl/actueel/nederland-maak-een-einde-aan-gevaarlijke-politie-experimenten-met-massasurveillance.*
(9) *https://www.parlement.com/id/vloreou0m8t6/regeerakkoord_2021.*
(10) *https://www.nature.com/articles/d41586-018-05469-3.*

Des scientifiques sont confrontés à des questions complexes sur ce que signifie «rendre un algorithme équitable». Les chercheurs qui tentent de développer des logiciels responsables et efficaces en coopération avec des organismes publics doivent se demander comment des instruments automatisés peuvent induire des préjugés ou renforcer des inégalités existantes.

Il est donc crucial que nous mettions en place notre propre autorité de contrôle des algorithmes, à l'instar des Pays-Bas. La technologie évolue de plus en plus vite. Par conséquent, au plus tôt nous intervenons et créons un cadre, au mieux la société peut en recueillir les fruits, avec de moindres risques d'être confrontée à des effets indésirables (imprévus).

Les effets néfastes des algorithmes qui diffusent des infox, par exemple, sont déjà perceptibles dans presque toutes les couches de la société. Il n'est donc jamais trop tôt pour intervenir, bien au contraire.

IV. INSTAURATION D'UNE PROPRE AUTORITÉ DE CONTRÔLE DES ALGORITHMES

Nous proposons tout d'abord que nous nous dotions de notre propre autorité de contrôle des algorithmes, comme l'ont fait les Pays-Bas. Un tel organe est avant tout chargé d'évaluer les algorithmes dans son pays.

Les services publics et services de sécurité qui ont recours à l'intelligence artificielle (AI) prédictive et aux algorithmes doivent relever de cette autorité de contrôle. Comme souligné plus haut, le risque d'une surveillance de masse non autorisée, combinée à des effets indésirables tels qu'un profilage ethnique, est bien réel. En effet, la police prédictive et les systèmes apparentés ont recours à des mégadonnées, ce qui ne peut fonctionner correctement que si l'on collecte un maximum de données.

Une autorité de contrôle est dès lors indispensable.

La police prédictive, par exemple, n'est acceptable qu'à condition d'être clairement encadrée. Elle deviendra en effet de plus en plus spécifique grâce aux évolutions de l'intelligence artificielle, et les frontières entre un comportement individuel punissable et une pensée non punissable seront éprouvées.

Par ailleurs, cette autorité de contrôle des algorithmes, agissant de concert avec ses homologues d'autres pays (européens), pourra inciter les entreprises *Big Tech*, en particulier les plateformes de médias sociaux, qui ne

Wetenschappers worden geconfronteerd met complexe vragen over wat het betekent om een algoritme eerlijk te maken. Onderzoekers die samenwerken met overheidsinstanties om te proberen verantwoorde en doeltreffende software te ontwikkelen, moeten zich afvragen hoe geautomatiseerde instrumenten vooroordelen kunnen introduceren of bestaande ongelijkheden kunnen verankeren.

Het is daarom van groot belang dat we naar Nederlands voorbeeld ook een eigen algoritmetoezichthouder instellen. De technologie evolueert steeds sneller, dus hoe sneller we ingrijpen en hiervoor een kader bouwen, des te beter kan de maatschappij de vruchten ervan plukken en daalt de kans geconfronteerd te worden met (onvoorziene) ongewenste neveneffecten.

De negatieve effecten van algoritmen die bijvoorbeeld *fake news* verspreiden zijn reeds voelbaar in nagenoeg alle geledingen van de maatschappij. Ingrijpen is dus nooit te vroeg, maar altijd te laat.

IV. OPRICHTING VAN EEN EIGEN ALGORITMETOEZICHTHOUDER

Vooreerst stellen we voor dat naar Nederlands model er een eigen algoritmetoezichthouder wordt aangesteld. Dit orgaan heeft in eerste instantie als taak de algoritmen in eigen land te evalueren.

Overheidsdiensten en veiligheidsdiensten die gebruik maken van voorspellende artificiële intelligentie (AI) en algoritmen dienen onder de controlebevoegdheid van deze toezichthouder te vallen. Zoals hierboven reeds aangegeven, is de kans op ongeoorloofde massasurveillance, gecombineerd met ongewenste neveneffecten zoals etnische profilering reëel. *Predictive policing* en aanverwante systemen maken namelijk gebruik van *big data*, wat enkel naar behoren kan functioneren indien men zoveel mogelijk data verzamelt.

Een toezichthouder is daarom onontbeerlijk.

Predictive policing kan bijvoorbeeld alleen maar wanneer dit duidelijk omkaderd is. *Predictive policing* zal door de ontwikkelingen inzake artificiële intelligentie immers steeds specifieker worden en aldus zullen de grenzen worden afgetast tussen individueel strafbaar gedrag en een niet-strafbare gedachte.

Verder kan deze toezichthouder, samen met soortgelijke toezichthouders van andere (Europese) landen de *Big Tech*-bedrijven, met name socialemediaplatformen, die op dit ogenblik nog onvoldoende maatregelen treffen om

prennent pas encore suffisamment de mesures pour endiguer leur flux d'infox, à intensifier leurs efforts dans ce domaine.

Eu égard aux matières traitées (technologies de l'information et de la communication (TIC), sciences, respect de la vie privée et numérisation), il est question en l'espèce d'une matière transversale qui relève à la fois de la compétence de l'autorité fédérale et de celle des Communautés.

*
* *

hun stroom aan *fake news* in te dijken, ertoe aansporen meer hiertegen te doen.

Gelet op de behandelde materies (informatie- en communicatietechnologie (ICT), wetenschap, privacy en digitalisering) gaat het hier om een transversale aangelegenheid die de federale overheid deelt met de Gemeenschappen.

*
* *

PROPOSITION DE RÉSOLUTION

Le Sénat,

A. considérant que la numérisation continue est une réalité et qu'elle doit être sans cesse soutenue;

B. considérant que les algorithmes sont omniprésents en ligne et y jouent un rôle déterminant;

C. considérant que, dans le secteur privé, les algorithmes sont surtout utilisés en ligne pour garantir l'engagement client;

D. considérant que, dans les médias sociaux, les algorithmes déterminent dans une très large mesure les messages qui seront ou non présentés à l'internaute;

E. considérant que, dans les médias sociaux, les algorithmes peuvent alimenter les chambres d'écho et la polarisation;

F. considérant que les algorithmes favorisent généralement les contenus polarisants;

G. considérant que le secteur public recourt lui aussi de plus en plus aux algorithmes;

H. considérant que la police prédictive est un exemple de l'innovation et de l'amélioration de l'efficacité que peuvent apporter les mégadonnées et les algorithmes;

I. considérant que l'utilisation d'algorithmes, comme dans la police prédictive, risque d'induire un profilage ethnique et peut favoriser les stéréotypes et la discrimination;

J. considérant que les mégadonnées et les algorithmes ont besoin du plus grand volume de données possible pour fonctionner, ce qui risque de mettre en péril le respect général de la vie privée;

K. considérant que les Pays-Bas vont mettre en place une autorité de contrôle des algorithmes, laquelle sera chargée de vérifier le degré de transparence, de discrimination et d'arbitraire des algorithmes;

L. considérant que l'on constate, aux États-Unis, que divers services publics ne disposent pas de moyens suffisants pour évaluer les algorithmes qu'ils utilisent eux-mêmes,

VOORSTEL VAN RESOLUTIE

De Senaat,

A. overwegende dat de continue digitalisering een feit is en blijvend moet worden ondersteund;

B. overwegende dat algoritmen online alomtegenwoordig zijn en er een doorslaggevende functie hebben;

C. overwegende dat algoritmen in de private sector online vooral gebruikt worden om *user-engagement* te garanderen;

D. overwegende dat op sociale media algoritmen in verregaande mate sturen welke berichten de gebruiker al dan niet te zien krijgt;

E. overwegende dat de algoritmen op sociale media echokamers en polarisatie kunnen bestendigen;

F. overwegende dat algoritmen polariserende inhoud veeleer promoten;

G. overwegende dat ook in de openbare sector steeds meer van algoritmen gebruik wordt gemaakt;

H. overwegende dat *predictive policing* een voorbeeld is van innovatie en van hoe *big data* en algoritmen tot een verbetering van de efficiëntie kunnen leiden;

I. overwegende dat door het gebruik van algoritmen, zoals bij *predictive policing*, het gevaar van etnische profilering dreigt en stereotypering en discriminatie in de hand kunnen worden gewerkt;

J. overwegende dat *big data* en algoritmen zoveel mogelijk data nodig hebben om te functioneren, wat de algemene privacy mogelijk in het gedrang brengt;

K. overwegende dat men in Nederland een algoritmetoezichthouder zal aanstellen die zal toezien op transparantie, discriminatie en willekeur bij algoritmen;

L. overwegende dat men in de Verenigde Staten vaststelt dat verschillende openbare diensten over onvoldoende middelen beschikken om de algoritmen te evalueren die ze zelf gebruiken,

Demande à tous les gouvernements:

1) de s'employer à mettre en place une autorité de contrôle des algorithmes, en tant qu'instance indépendante;

2) de placer sous la surveillance de cette autorité les institutions publiques qui recourent déjà à des algorithmes, à l'intelligence artificielle (IA) et aux mégadonnées;

3) d'éviter, par l'intermédiaire de l'autorité de contrôle des algorithmes, qu'en utilisant leurs propres algorithmes, les pouvoirs publics ne favorisent les préjugés, la discrimination ou les stéréotypes;

4) d'éviter que les algorithmes utilisés par les pouvoirs publics ne deviennent une «boîte noire»;

5) de munir leurs propres services d'outils leur permettant d'évaluer leurs propres algorithmes et, si nécessaire, de les adapter;

6) de charger l'autorité de contrôle des algorithmes, en collaboration avec l'Autorité de protection des données, de veiller à ce que les mégadonnées et algorithmes ne portent pas atteinte à la protection générale de nos données à caractère personnel;

7) d'éviter que les pouvoirs publics ne collectent plus de données de citoyens que nécessaire;

8) de développer pour le secteur public un ensemble spécifique de règles d'éthique des données qui garantissent le respect de la vie privée du citoyen et l'utilisation correcte des mégadonnées et algorithmes;

9) de faire en sorte que cette autorité de contrôle des algorithmes unisse ses forces à celles des autorités homologues des pays voisins de l'Union européenne pour inciter les entreprises *Big Tech* (principalement celles des médias sociaux) à prendre des mesures contre les infox et la désinformation sur leurs plateformes.

Le 21 janvier 2022.

Vraagt aan alle regeringen om:

1) werk te maken van de oprichting van een algoritmetoezichthouder als onafhankelijke instantie;

2) openbare instellingen die reeds met algoritmen, artificiële intelligentie (AI) en *big data* werken onder het toezicht van deze algoritmetoezichthouder te plaatsen;

3) via de algoritmetoezichthouder te voorkomen dat de overheid bij gebruik van eigen algoritmen vooroordelen, discriminatie of stereotypering in de hand werkt;

4) te voorkomen dat de door de overheid gebruikte algoritmen een *black box* zouden worden;

5) aan de eigen diensten tools aan te reiken die hen in staat stellen de eigen algoritmen te evalueren en waar nodig aan te passen;

6) in samenwerking met de Gegevensbeschermingsautoriteit, de algoritmetoezichthouder erover te doen waken dat *big data* en algoritmen niet onze algemene privacy aantasten;

7) te voorkomen dat de overheid meer data van de burgers verzamelt dan nodig;

8) voor de publieke sector een eigen set van data-ethiek regels te ontwikkelen, die de privacy van de burger en het correcte gebruik van *big data* en algoritmen moeten verzekeren;

9) ervoor te zorgen dat deze algoritmetoezichthouder de krachten bundelt met andere soortgelijke toezichthouders uit de omringende landen van de Europese Unie om zo de grote *Big Tech* bedrijven (voornamelijk die van de sociale media) ertoe aan te zetten iets te doen tegen *fake news* en desinformatie op hun platformen.

21 januari 2022.

Rik DAEMS.
Fatima AHALLOUCH.
Véronique DURENNE.
Katia SEGERS.
Bert ANCIAUX.

Imprimerie centrale – Centrale drukkerij